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

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
IT Security (Russia)

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

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

С момента основания в 1994 году (свидетельство о регистрации в Государственном комитете Российской Федерации по печати № 017789) и до настоящего времени учредителем журнала является федеральное государственное автономное образовательное учреждение высшего образования Национальный исследовательский ядерный университет «МИФИ» (НИЯУ МИФИ).

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 National Research Nuclear University, "MEPhI" (Moscow Engineering Physics Institute).

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
2. 3.5 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей (технические науки),
2.3.6 – Методы и системы защиты информации, информационная безопасность (технические науки), по которым журнал входит в этот перечень.

The journal is included in the List of the Higher Attestation Commission of the leading peer-reviewed scientific journals and publications in which the main scientific results of dissertations for the degree of doctor and candidate of sciences in the branches of science and a group of specialties of researchers should be published
2.3.5 - Mathematical and software of computers, complexes and computer networks (technical sciences),
2.3.6 - Methods and systems of information protection, information security (technical sciences), for which the journal is included in this list.

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;*
- *Оценка и обеспечение доверенности аппаратной части средств защиты информации;*
- *Методы и средства тестирования стойкости электронной компонентной базы к внешним воздействиям и атакам;*
- *Развитие нормативной базы регулирования жизненного цикла доверенной электронной компонентной базы;*
- *Проектирование и сертификация микроэлектроники специального назначения.*

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;*
- *Evaluation and provision of power of attorney for the hardware of information security tools;*
- *Methods and means of testing the resistance of the electronic component base to external influences and attacks;*
- *Development of the regulatory framework for regulating the life cycle of a trusted electronic component base;*
- *Design and certification of special-purpose microelectronics.*

Журналом приветствуются статьи на русском и английском языках

Papers in Russian and English are equally welcome

СОДЕРЖАНИЕ

CONTENT

КОЛОНКА ГЛАВНОГО РЕДАКТОРА

Уважаемые коллеги!

А все-таки жаль, что кончилось лето! А вместе с ним и наши надежды, что штормовая погода вот-вот завершится и наша жизнь вернется в спокойное русло. А никто и не обещал, что будет легко, покой нам только снится!

Во исполнение ранее опубликованных Указов Президента России (см. колонку главного редактора в нашем журнале том 29 №2 (2022) Правительство Российской Федерации утвердило соответствующие постановления, краткий реферат которых представлен ниже.

Постановление от 15.07.2022 № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)» утвердило соответствующие положения.

Первое из двух утвержденных типовых положений определяет полномочия, права и обязанности заместителя руководителя федерального органа исполнительной власти (ФОИВ), других государственных органов и организаций, стратегического предприятия и системообразующей организации российской экономики, юридического лица, являющегося субъектом критической информационной инфраструктуры – КИИ РФ (далее – орган, организация), ответственного за обеспечение информационной безопасности, в т.ч. за обнаружение, предупреждение и ликвидацию последствий компьютерных атак и реагирование на компьютерные инциденты (далее – ответственное лицо).

Установлено, что ответственное лицо должно иметь высшее образование (не ниже уровня специалитета, магистратуры) по направлению обеспечения информационной безопасности (ИБ) или пройти обучение по программе профессиональной переподготовки по направлению «Информационная безопасность». Перечислены знания, умения и профессиональные компетенции ответственного лица. Установлены трудовые (должностные) обязанности, права и ответственность ответственного лица.

Второе из утвержденных типовых положений определяет цели, задачи, функции, права, взаимоотношения и связи, показатели эффективности и результативности структурного подразделения органа (организации), обеспечивающего его информационную безопасность.

Очевиден рост спроса на специалистов в области ИБ, с другой стороны - еще в мае этого года ряд экспертов констатировали дефицит таких сотрудников на уровне 30% от числа вакансий. Обе тенденции сложились и позволяют прогнозировать высокую нагрузку на ВУЗы и учебные центры по соответствующим образовательным программам. Например, этим летом в НИЯУ МИФИ на направления в области ИБ поступило максимальное число магистров за последние 5 лет, а также дополнительно открыта первая программа профессиональной переподготовки «Информационная безопасность. Обеспечение безопасности значимых объектов критической информационной инфраструктуры».

Постановление от 22 августа № 1478 с нелаконичным названием (воспроизвожу с сокращениями): «Об утверждении требований к программному обеспечению, в том числе в составе программно-аппаратных комплексов, используемому органами государственной власти, заказчиками, осуществляющими закупки а соответствие с Федеральным законом «О закупках товаров, работ, услуг отдельными видами юридических лиц (…) на принадлежащих им значимым объектах КИИ РФ, Правил согласования закупок иностранного программного обеспечения, …, а также закупок услуг, необходимых для использования этого программного обеспечения на таких объектах, и Правил перехода на

преимущественное использование российского программного обеспечения, …». Здесь определены ФОИВ, осуществляющие согласование иностранного программного обеспечения (ПО) и/или услуг, необходимых для использования этого ПО на значимых объектах КИИ РФ в различных областях. В частности, соответствующее согласование в области ракетно-космической и оборонной промышленности возложено на Министерство промышленности и торговли Российской Федерации. Отмечена возможность привлечения отраслевых центров компетенций по импортозамещению ПО, в том числе на базе подведомственных учреждений. Контроль за соблюдением правил закупки иностранного ПО и услуг по его использованию, а также за соблюдением запрета на его использование возложен на Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (далее – Минцифры РФ). Для этого Минцифры РФ может привлекать экспертную организацию в порядке, предусмотренном законодательством РФ. Кроме того, Минцифры РФ поручено в двухмесячный срок утвердить методические рекомендации по переходу на использование российского ПО, в том числе на значимых объектах КИИ РФ.

В утвержденных требованиях к ПО на объектах КИИ отмечено, что данное ПО должно быть включено в единый реестр российских программ для электронных вычислительных машин и баз данных. ПО, предназначенное для обеспечения безопасности значимых объектах КИИ РФ, а также ПО, предназначенное для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты и (или) обмена информацией о таких инцидентах на объектах КИИ должны соответствовать требованиям ФСТЭК России и ФСБ России в пределах их полномочий, что должно быть подтверждено соответствующим документом (сертификатом).

В утвержденных правилах согласования закупок иностранного ПО в целях его использования на значимых объектах КИИ, а также закупок соответствующих услуг отмечено что заявка на закупку с ценой договора 100 млн.рублей и более подлежит рассмотрению специальной комиссией, формируемой Минцифры РФ, в состав которой входят представители уполномоченных органов, иных ФОИВ, а также организаций. Минцифры РФ утверждает Положение о комиссии и ее состав. Указаны основания для принятия решения комиссии об отказе в одобрении закупки или решения уполномоченного органа об отказе в согласовании покупки.

В утвержденных правилах перехода на преимущественное использование российского ПО на объектах КИИ предписана необходимость разработки, указаны содержание и сроки плана перехода на отечественное ПО, составленного на период до 1 января 2025 г. (с разбивкой по годам).

К большому сожалению, принятое Постановление ограничилось регламентацией порядка приобретения и использования только ПО и не затронула аппаратную часть – РЭА и ЭКБ для комплектования радиоэлектронных систем и комплексов объектов КИИ.

Далее – анонс информационных событий по тематике нашего журнала. Важнейшим из них является Российский Форум «Микроэлектроника 2022» (далее – Форум»), который состоится со 2 по 8 октября 2022 г. в Розе Хутор (Сочи). Наш журнал является доверенным информационным партнером Форума.

Одной из центральных тематических линий Форума в этом году является обеспечение доверенности ЭКБ и РЭА, как важнейшего составного элемента конкурентоспособности электронных изделий.

Под доверенностью (в смысле предсказуемости, соответствия ожиданиям) далее понимается подтвержденное свойство изделия или процесса удовлетворять потребности в соответствие с назначением в течение срока и в условиях эксплуатации, верифицируемости,

тестопригодности и соответствия документации, санкционной стойкости, а также отсутствие недекларируемых включений, коррекций и возможностей управления и считывания информации, признаков фальсификата и контрафактного происхождения. В таком контексте информационная безопасность (состояние защищенности данных, при котором обеспечены их конфиденциальность, доступность и целостность) является лишь составной частью доверенности – важной, но не самой приоритетной для многих гражданских систем.

В оборонной технике нормированы основные требования к изделиям, по сути, формирующие свойства доверенности – это качество, надежность, стойкость к внешним воздействующим факторам, информационная безопасность. Но для гражданской продукции данные требования практически не отражены в нормативных документах. В гражданских системах до последнего времени применялись почти исключительно иностранные ЭКБ и электронные блоки, соответствие которых требованиям назначения сводилась к их формальной сертификации, проводившейся в основном по наличию поставочной документации. Такие изделия можно было считать условно доверенными при легальной закупке продукции известных брендов, предоставляющих потребителю подробную документацию, эффективную систему технической поддержки и гарантийного обслуживания. В существующих реалиях потребовалась смена поставщиков и логистических цепочек. Потребители лишились технической поддержки и гарантий изготовителя. Отсутствует техническая информация о проектных решениях и базовых техпроцессах ЭКБ, о методических подходах и условиях проведения испытаний – по сути компоненты стали «черными ящиками». В этих условиях требуется обеспечить полный и информативный входной контроль работоспособности изделий у квалифицированного поставщика и/или потребителя с проверкой соответствия требованиям назначения с учетом сроков и условий эксплуатации. Понятие контрафакта требует юридической переквалификации в реалиях параллельного импорта. Максимальную актуальность и остроту приобрело требование обеспечения технологической независимости – по сути, санкционной стойкости. В целом, во весь рост встал вопрос выбора пути (стратегии) обеспечения комплектования аппаратуры: (1) путем поэлементной замены всей номенклатуры недружественного на дружественный импорт; (2) путем поэлементной замены всей номенклатуры ЭКБ ИП на отечественные аналоги; (3) путем переработки целых узлов и блоков РЭА на системно-ориентированные блоки в микроэлектронном исполнении в виде систем-на-кристалле и систем-в-корпусе, (4) или еще как-то? Очевидно, что на практике потребуется разумное сочетание всех перечисленных подходов, но для рационального выбора необходим всесторонний анализ выполнимости и технико-экономической эффективности каждого из них. Данная ситуация характерна не столько для узкого круга специальных ЭКБ, сколько для широчайшей номенклатуры электронной продукции для аппаратуры связи, навигации, цифровой идентификации, интернета вещей, транспорта (в том числе беспилотного), больших данных, коммунального хозяйства, охранных и многочисленных других классов гражданских электронных систем. Методы обеспечения и оценки доверенности должны развиваться и применяться на этапах проектирования, изготовления, верификации, тестирования и испытаний изделий – для всей гражданской продукции это важнейшая новая комплексная задача, в решение которой должны внести свой вклад и дизайн-центры, и предприятия – контрактные изготовители ЭКБ, и испытательные центры и предприятия-потребители ЭКБ и РЭА. Именно поэтому тема доверенности ЭКБ и РЭА обоснованно оказалась в центре научной проблематики Форума.

Наиболее интересным мероприятием из уже состоявшихся событий в рамках Форума за текущий период считаю предконференцию «Доверенные и экстремальные

электронные системы», которая прошла с 12 по 14 сентября 2022 г. в Москве на базе одноименного консорциума НИЯУ МИФИ и АО «ЭНПО СПЭЛС».

В жестком рабочем режиме – ежедневно с 9.00 до 19.00 – по 8 часов интересных докладов, жарких дискуссий по наиболее актуальным темам развития отечественной электроники и полезных экскурсий по лабораториям (в том числе мастер-класс по лазерному экспресс-удалению маркировки с кристаллов микросхем). 82 доклада, более 100 участников ежедневно, из них треть очно и две трети онлайн. Рекорд по числу слушателей зафиксирован у доклада Филаретова А.Г. (АО «Светлана-Рост») «Место и роль A_3B_5 СВЧ технологий в процессах разработки и производства радиотехнических систем». Приз зрительских симпатий у эмоционального доклада Безродного Б.Ф. (ФГУП «НИИАС») «Проблемы ЭКБ при обеспечении кибербезопасности систем железнодорожной автоматики и телемеханики». Приз координатора предконференции (Ваш покорный слуга) за запоминающийся доклад поделили – Горбунов М.С. (НИЯУ МИФИ – АО «ЭНПО СПЭЛС») «Какой могла бы быть программа создания отечественных САПР» и Чистов А.С. (ООО «НПП «ИТЭЛМА») «Требования к электронным компонентам для доверенных блоков управления автотранспортом».

Вопросы обеспечения и оценки доверенности ЭКБ и РЭА при их разработке, изготовлении и эксплуатации были рассмотрены на обзорном заседании в рамках блока «Доверенная электроника» Предконференции, которое состоялось 14 сентября 2022 г. в Москве. Было представлено 23 доклада, значимая часть времени уделена ярким и интересным дискуссиям о соотношении доверенности и информационной безопасности, особенностям задания требований доверенности и методов оценки соответствия этим требования изделий, предназначенных для комплектования как объектов КИИ, так и широкого круга гражданских систем.

В процессе подготовки данного номера появилась инициатива ввести в порядке эксперимента в нашем журнале новую рубрику «Есть мнение», в которой авторы будут выступать с оперативными откликами и мнениями по актуальным проблемам, мероприятиям и документам.

Продолжим анонс – теперь уже предстоящих событий Форума по тематике нашего журнала.

Проблемная ситуация в области обеспечения технологической независимости, безопасности критической информационной инфраструктуры и доверенности комплектующих ЭКБ и РЭА будет рассмотрена на пленарном заседании Форума «**Доверенность ЭКБ и РЭА – тема для спекуляций или объективный вызов?**», которое состоится 4 октября 2022 г., с 15.00 до 18.30 (Роза-холл). В программе запланированы выступления представителей государственного регулятора – Лютикова В.С. (ФСТЭК России), головной Госкорпорации – Шевченко А.Б. (ГК «Росатом») и научно-академического сообщества – Зегжды Д.П. (Институт кибербезопасности и защиты информации СПбПУ). Подходы к созданию гражданской продукции в новых реалиях представят руководители предприятий-разработчиков радиоэлектронных систем – Анцев И.Г (АО «Радар-ММС») и Бутко А.Б. (АО «РАСУ»). В завершение Тихонов А.И. (Ассоциация «Доверенная платформа») обобщит системные аспекты обеспечения технологической независимости и безопасности критической информационной инфраструктуры. В ходе дискуссии будут подведены итоги заседания.

Анализ и обсуждение различных аспектов обеспечения и оценки доверенности ЭКБ и РЭА будут продолжены в ходе трека обзорно-дискуссионных заседаний «**Развитие экосистемы создания доверенной ЭКБ и РЭА в условиях турбулентности**» 5 и 6 октября 2022 г. с 10.00 до 18.30 (Роза Холл).

КОЛОНКА ГЛАВНОГО РЕДАКТОРА

На заседании «Проблемная ситуация по комплектованию аппаратуры в новых реалиях» 5 октября 2022 г. 10.15–11.30 особенности комплектования радиоэлектронных комплексов будут рассмотрены в выступлениях Краснова М.И. (АО «Российские космические системы») – применительно к космическим системам, и Чистова А.С. (ООО «НПП «ИТЭЛМА») – применительно к автоэлектронике. Подход к формированию сквозных проектов развития ЭКБ и РЭА представит Заблоцкий А.В. (ФПИ). В выступлении Одинокова А.В. (ООО «СБИС Технологии») будет дан обзор зарубежной практики государственной поддержки развития национальной электронной промышленности.

На заседании «Системный подход к разработке и комплектованию ЭКБ доверенной аппаратуры приемо-передающих радиоэлектронных комплексов связи и передачи данных» 5 октября 2022 г. 12.00–13.30 рассмотрим современное состояние и тенденции развития ЭКБ аппаратуры комплексов связи и передачи данных, которые составляют подавляющую долю рынка современной радиоэлектроники. На примере сетей 5-го и 6-го поколений и интернета вещей обсудим вопросы: развивать унифицированную или системно-ориентированную номенклатуру ЭКБ; какие технологические процессы и инфраструктура приоритетно необходимы для изготовления ЭКБ; какой маршрут разработки предпочтительнее – сосредоточенный или распределенный и нужна ли синхронизация маршрутов разработки РЭА и ЭКБ. В выступлении Будякова А.С. (ООО «ИнноЦентр ВАО») будут рассмотрены состояние и перспективы развития отечественных микроэлектронных программно-конфигурируемых радиосистем для комплексов связи 5G и 6G. Доценко В.В. (АО «НПП «Радар-ММС») проанализирует новые вызовы и решения в области ЭКБ аппаратуры перспективных сетей связи и передачи данных. В докладе Матвеева М.Ю. (ПАО «МТС») будут представлены доверенные устройства и решения интернета вещей и номенклатура ЭКБ для их реализации. В дискуссии примут участие эксперты – Монастырев Е.А. (АО «НИИПП») и Зайцев А.В. (АО «НПЦ «Элвис»).

На заседании «Потребности и возможности создания новых технологий и доверенных контрактных производств микро-, нано-, и СВЧ-электроники» 5 октября 2022 г. 15.00–16.30 рассмотрим состояние и перспективы отечественных контрактных производств ЭКБ микро- и СВЧ-электроники по кремниевым и А3В5 технологиям для систем связи и передачи данных. Шелепин Н.А. (ИНМЭ РАН) обобщит отечественный опыт контрактного производства КМОП СБИС. Состояние и перспективы развития отечественных контрактных производств твердотельной СВЧ электроники представят Чалый В.П. (АО «Светлана-Рост») и Щербаков С.В. (АО «НПП «Исток» им. Шокина»). Особенности и примеры характеризации базовых техпроцессов контрактных производств СВЧ ЭКБ в своих содокладах озвучат Бабак Л.И. (ТУСУР) и Усачев Н.А. (НИЯУ МИФИ).

Завершающее заседание первого дня трека «Обеспечение и контроль функционирования ЭКБ в экстремальных условиях изменения Климата (было «-7», а стало «-8»)…» 5 октября 2022 г. 17.00–18.30 посвящено вопросам радиационной стойкости ЭКБ.

Сначала Селецкий А.В. (АО «НИИМЭ»), Шелепин Н.А. (ИНМЭ РАН) и Новоселов А.Ю. («Миландр-ЭК)» обсудят задачу создания технологической платформы разработки радиационно-стойких схем на базе отечественного КМОП производства. Далее Пармон П.Л. (АО «НИИЭТ») и Чуков Г.В. (АО «ЭНПО СПЭЛС») проанализируют опыт использования лазерного и рентгеновского испытательных комплексов на предприятии для оперативных оценок и контроля радиационной стойкости изделий и процессов разработки и производства ЭКБ. В завершение выступит Уланова А.В. (НИЯУ МИФИ) с анализом методических особенностей оценки радиационной стойкости ЭКБ по новому комплексу стандартов. В дискуссии примут участие эксперты – Щепанов А.Н. (АО «НИИП») и Чубунов П.А. (АО «НИИКП»).

КОЛОНКА ГЛАВНОГО РЕДАКТОРА

Следующий день работы трека откроется заседанием «Развитие доверенной инфраструктуры для проектирования компонентов и СФ блоков микро-, нано- и СВЧ-электроники: проблемы и пути их решения» 6 октября 2022 г. 10.00–11.30. Рассмотрим обеспечение инфраструктуры разработки ЭКБ и РЭА средствами автоматизированного проектирования. Обсудим вопросы разработки отечественных САПР и использования иностранного программного обеспечения (ПО), рассмотрим особенности открытого ПО. Горбунов М.С. (НИЯУ МИФИ – АО «ЭНПО СПЭЛС») представит свой взгляд на облик программы создания отечественных САПР. Елизаров С.Г. (ООО «Мальт Систем») выскажется о перспективах использования открытого ПО и IP для разработки микросхем. Далее Плаксин А.А. (ЭРЕМЕКС) рассмотрит новые и старые вызовы для отечественного разработчика САПР электроники. И в завершение Бабак Л.И. (ТУСУР) расскажет о создании отечественных САПР для проектирования СВЧ устройств и полупроводниковых ИС. В дискуссии примет участие в качестве эксперта Старилов М.В. (ЗАО «СКАН»).

На следующем заседании «Микропроцессорные платформы в новых реалиях» 6 октября 2022 г. 12.00–13.30 рассмотрим вопросы выживания и развития микропроцессорных платформ в условиях турбулентности, включая перспективы RISC-V, ARM и Эльбрус, обсудим наши возможности участвовать в развитии RISC-V или создания его отечественной версии. Доклад Трушкина К.А. (АО «МЦСТ») представит развитие архитектуры «Эльбрус» в обострившейся конкурентной борьбе с RISC-V. Редькин А.Н. (ООО «СИНТАКОР») выскажет мнение о наличии альтернативы у RISC-V. Козлов А.В. (ООО «Клаудбеар») расскажет об отечественных RISC-V ядрах в сопоставлении с ядрами ARM. В завершение заседания Хренов Г.Ю. (Байкал Электроникс) подведет его итоги и выскажется по перспективе.

Завершающее заседание трека «Обеспечение и оценка соответствия ЭКБ требованиям доверенности» 6 октября 2022 г. 15.00–16.30 рассмотрит практические аспекты системы обеспечения и оценки доверенности, необходимые нормативные документы и новые вызовы в обеспечение доверенности в условиях параллельного импорта ЭКБ, а также задачи защиты РЭА от реинжиниринга. Откроет заседание Кессаринский Л.Н. (НИЯУ МИФИ) с докладом по облику системы обеспечения и оценки доверенности на всех этапах жизненного цикла ЭКБ. Титаренко А.А. (ГК «Росатом») представит подход к заданию и реализации требований доверенности к ЭКБ и радиоэлектронным комплексам критической инфраструктуры. Далее Боярков В.С. (18 ЦНИИ) опишет задачу и методику удаления маркировки корпусов ЭКБ для применения в доверенной РЭА. И, наконец, Горный С.Г. (ООО «Лазерный Центр») расскажет об идентификации, контроле оборота и защиты от подделки лазерными штриховыми кодами высокой плотности. В завершение работы трека состоится общая дискуссия и подведение его итогов.

Учитывая, что все мероприятия будут транслироваться онлайн, приглашаем всех заинтересованных специалистов зарегистрироваться для участия в Форуме и принять участие в заседаниях. Ждем вас на Форуме, Роза Хутор 2–8.10.2022.

Искренне ваш,

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

ЕСТЬ МНЕНИЕ

Максим С. Горбунов, Игорь А. Данилов

КАКОЙ МОГЛА БЫ БЫТЬ ПРОГРАММА СОЗДАНИЯ ОТЕЧЕСТВЕННЫХ САПР?

Уважаемые коллеги!

Как уже было анонсировано мы открываем новую регулярную рубрику «Есть мнение», и в качестве первого опыта мы пригласили Горбунова Максима Сергеевича, к.т.н., доцента НИЯУ МИФИ, который в соавторстве с к.т.н. Даниловым Игорем Александровичем выскажет мнение на тему «Какой могла бы быть программа создания отечественных САПР?». Это авторский взгляд, основанный на опыте разработки сложнофункциональных блоков по актуальным отечественным и зарубежным КМОП технологиям, а также программных инструментов для моделирования радиационных эффектов в стандартном маршруте проектирования. Кроме того, М.С. Горбунов принимал активное участие в подготовке программ и подпрограмм создания отечественных САПР, которые, к сожалению, по разным причинам не стартовали. Учитывая актуальность этой проблемы для разработки широкой номенклатуры отечественной ЭКБ, включая доверенную, мы полагаем, что взгляд на организацию таких работ, по крайней мере, небезынтересен.

Главный редактор,
доктор технических наук, профессор
Александр Ю. Никифоров

МНЕНИЕ: «Какой могла бы быть программа создания отечественных САПР?»

DOI: http://dx.doi.org/10.26583/bit.2022.3.01

Обсуждая задачу создания отечественных САПР, прежде всего следует установить целеполагание. Учитывая необходимость колоссальных финансовых, человеческих и временных затрат – зачем нужны такие отечественные системы? На этот вопрос есть несколько вариантов ответов: кто-то скажет, что российские САПР обеспечат доверенность создаваемой ЭКБ, другой отметит необходимость иметь доступные средства проектирования, свободные от санкционных рисков, третий, говоря об отечественных разработчиках, сделает акцент на необходимости сохранения существующих команд и развития их компетенций. Обобщая, можно сказать, что российские САПР нужны главным образом для поддержки дорожной карты развития полупроводниковых производств в России. В отсутствие такой дорожной карты и системного подхода к её реализации все остальные аргументы довольно слабы.

За прошедшие 5 лет было, по крайней мере, две крупных попытки запустить создание полноценных отечественных систем автоматизированного проектирования электронной компонентной базы: «Программа-710» (подпрограмма № 6) Минпромторга РФ и комплексный научно-технический проект полного цикла «Комплексное развитие разработки российских систем автоматизированного проектирования в целях дальнейшего производства на их базе приоритетных видов микроэлектроники» (КНТП САПР), который представляли ФГУ ФНЦ НИИСИ РАН, АО «НИИМА «Прогресс», АО ЦНИИ «Электроника», ЗАО «СКАН» и другие компании. Обе программы так и не были запущены, несмотря на прохождение нескольких этапов экспертизы. Проект «Программы-710», по меткому сравнению Ю.В. Завалина (АО «НИИМА «Прогресс»), вынашивался, как ребёнок, 9 месяцев, за которые удалось выделить основные команды разработчиков из разных отечественных компаний (как государственных, так и частных, включая предприятия малого и среднего бизнеса), которые имеют наработки в области инструментов создания цифровой, аналого-цифровой и СВЧ ЭКБ. В результате выполнения Программы эти

наработки должны были быть доведены до уровня прототипа или, в идеале, коммерческого продукта. К сожалению, Программа не предусматривала создания единого программного комплекса и, следовательно, не предъявляла единых требований к разрабатываемым инструментам. Разработчики КНТП САПР взяли за основу наработки «Программы-710», но дополнительно предложили строить систему на основе трёх направлений маршрутов проектирования: цифровой, аналого-цифровой и СВЧ ЭКБ – так, чтобы разработчики электронных компонентов получили единую «бесшовную» среду, близкую к тем промышленным стандартам де-факто, что предоставляются «большой тройкой», т.е. компаниями Cadence, Synopsys и Mentor Graphics (ставшей позднее Siemens EDA). Близкую если не по эффективности (осознавая колоссальный временной и финансовый отрыв от существующих коммерческих продуктов), то по крайней мере идеологически. Проект системы, или платформы, ориентировался прежде всего на существующие в России фабрики и на перспективную линию 28 нм. Реализация КНТП САПР требовала наличия единого «мозгового центра», координирующего разрозненные группы разработчиков, и, к сожалению, не опиралась на какое-либо достаточно крупное ИТ-предприятие, способное не только создать прототип системы, но и заниматься её развитием и технической поддержкой.

Но вернёмся к сегодняшнему дню. Конкурентоспособность САПР, как на внутреннем, так и на внешнем рынке, складывается из экономической эффективности, технических преимуществ и удобства использования для разработчика ЭКБ. Говоря об удобстве, следует отметить:

– комфортную (иначе говоря, привычную) среду разработки, прививаемую, вообще говоря, со студенческой скамьи;

– совместимость с актуальными маршрутами проектирования, то есть поддержку методологии проектирования и правил верификации на соответствующем уровне технологий;

– бесшовность, то есть отсутствие необходимости применения дополнительных программных средств, скриптов для преобразования форматов между стадиями маршрута или для «склейки» результатов разных стадий;

– грамотную техническую поддержку;

– наличие базы знаний и комплектов для освоения маршрутов (rapid adoption kits, RAK)[1].

Что касается технических преимуществ и экономической эффективности, то, во-первых, эти показатели могут быть достигнуты благодаря развитию собственных алгоритмов за счёт (всё ещё) сильной математической школы. Во-вторых, не имеет смысла создавать САПР саму по себе и сравнивать её с заведомо более эффективными конкурентами от «большой тройки» – однако в увязке с дорожной картой развития российских полупроводниковых технологий становится очевидна роль САПР для обеспечения проектирования, не только доступного отечественным компаниям и дизайн-центрам (включая малые предприятия и стартапы), но и лежащего в основе программ подготовки инженерных кадров, математиков и программистов. В-третьих, следует продавать не только лицензии на САПР, а инфраструктуру на основе отечественных операционных систем и вычислителей. Такая инфраструктура схематически представлена на рис. 1.

[1]URL: https://www.cadence.com/content/cadence-www/global/en_US/home/multimedia.html/content/dam/cadence-www/global/en_US/videos/services/rak-faqs-main-final-full-hd-25mbps (дата обращения: 09.09.2022).

Рис. 1. Схематическое изображение программно-аппаратной Платформы в виде инфраструктуры проектирования

Важно отметить, что рыночный потенциал такой инфраструктуры гораздо выше, чем каждого из компонентов в отдельности. Так, для типового дизайн-центра стоимость лицензий на САПР для маршрутов проектирования на основе «зрелых» технологий (к которым относится как уровень 65 нм, так и 28 нм) составляет порядка 1 млн дол. США и может быть кратно выше для маршрутов, ориентированных на передовые технологии. Для отечественных САПР стоимость коммерческих лицензий для внутреннего рынка не сможет быть существенно меньше, особенно в первые 5–10 лет, из-за необходимости развития продукта и обеспечения техподдержки, что означает необходимость софинансирования государством лицензий для дизайн-центров. Серверное оборудование, необходимое для обеспечения проектирования, стоит порядка десятков тысяч долларов США, а с учётом отечественной элементной базы и необходимости затрат на поддержку стоимость можно оценить по порядку величины в 100 тыс. дол. США, т.е. около 10% стоимости лицензии на САПР. Техническое преимущество серверов на отечественной элементной базе может быть достигнуто за счёт оптимизации архитектуры вычислителей и компиляторов не под синтетические тесты, демонстрирующие потенциальные возможности тех или иных архитектур и их микроархитектурных реализаций, а под конкретные задачи, связанные с многоуровневым моделированием, синтезом и верификацией. Иными словами, эксплуатируя концепцию «встречной оптимизации»[2] аппаратной и программной частей. Тогда сочетание уникальных алгоритмов, лежащих в основе САПР, с оптимизированным «железом» может дать значимое преимущество отечественной инфраструктуры перед аналогичными комплексами сравнимой стоимости на базе ЭКБ иностранного производства. Способность российских команд провести такую оптимизацию на базе «Эльбрусов» или серверных микропроцессоров АО «Байкал Электроникс» не вызывает сомнений. Разумеется, в условиях острого дефицита отечественных электронных компонентов и ограничений доступа к кремниевым фабрикам такая концепция нереализуема и разумно начать развитие инфраструктуры на доступных компонентах. Однако отсутствие требований совместимости отечественного ПО с отечественными же архитектурами в обозримом будущем неизбежно приведёт к вымиранию последних и полной утрате соответствующих компетенций, что, несомненно, противоречит концепции технологического суверенитета. И это одна из причин, по которой создание САПР должно быть встроено в дорожную карту развития отечественной полупроводниковой промышленности.

[2]Бетелин В.Б. Отечественные суперкомпьютерные технологии экзафлопсного класса – необходимое условие обеспечения технологической конкурентоспособности России в XXI веке. Программные продукты и системы. 2013, № 4. URL: https://cyberleninka.ru/article/n/otechestvennye-superkompyuternye-tehnologii-ekzaflopsnogo-klassa-neobhodimoe-uslovie-obespecheniya-tehnologicheskoy (дата обращения: 09.09.2022).

Отметим, что одним из направлений бизнеса компании Cadence Design Systems является поставка ускорителей эмуляции Palladium (для быстрой отладки оборудования) и прототипирования Protium (для проверки программного обеспечения)[3]. К сожалению, в России пока нет элементной базы для создания подобного класса аппаратуры, однако отечественные серверные решения, в том числе на основе удалённого доступа и облачных вычислений, могли бы быть интересны разработчикам ЭКБ по всему миру.

Возвращаясь к вопросу создания непосредственно отечественных САПР, можно выделить три основных стратегии:

– реализация полного маршрута проектирования только на отечественном ПО;

– реализация на отечественном ПО только тех стадий маршрута проектирования, в которых у российских компаний есть существенный задел, остальное обеспечивать открытым ПО (open source) с необходимой доработкой;

– разработка ПО только для тех стадий маршрута проектирования, которые являются критичными, например, с точки зрения обеспечения доверенности.

Рассмотрим преимущества и недостатки этих стратегий по критериям, указанным в табл. 1. Оценки по 3-балльной шкале приведены экспертно от 0 до 2, где 0 – низкая степень, 2 – высокая. В качестве маршрута выберем цифровой (RTL-to-GDSII[4]) как наиболее показательный и трудоёмкий, но, как можно будет убедиться далее, результаты анализа в полной мере переносимы в аналого-цифровой и СВЧ маршруты.

Таблица 1. Сравнительные характеристики стратегий реализаций САПР

	Полный маршрут	Полный маршрут с open source	Только критичные стадии
Трудоёмкость	2	1	0
Доверенность	2	0...2	1...2
Бесшовность	2	0...2	1...2
Профанируемость разработчиком САПР	0	0...1	1...2
Профанируемость пользователем	0...1	0...2	2

Реализация полного маршрута, очевидно, является наиболее трудоёмкой стратегией, особенно с учётом того, что у российских разработчиков нет значимых компетенций в части реализации этапов физического синтеза и верификации – наиболее трудоёмких и критичных с точки зрения обеспечения доверенности. Продукты с открытым кодом облегчают задачу в целом, но также не закрывают упомянутые критичные этапы. Наконец, создание компонентов САПР, обеспечивающих реализацию только критичных стадий, – задача высокой сложности, однако с наименьшей трудоёмкостью из трёх стратегий.

В отсутствие соответствующей нормативной базы, расставить трём стратегиям баллы по доверенности затруднительно, тем не менее, полный маршрут получит наивысший балл по этому критерию, как бы ни были сформулированы требования по доверенности в стандартах. Стратегия, использующая компоненты с открытым исходным кодом, может дать любой результат: от наименьшей доверенности (при безответственном и неконтролируемом использовании стороннего кода) до наибольшей (при тщательном

[3]URL: https://www.shunlongwei.com/ru/cadence-unveils-next-generation-palladium-z2-and-protium-x2-systems/ (дата обращения: 09.09.2022).
[4]URL: https://www.cadence.com/en_US/home/training/all-courses/86136.html (дата обращения: 09.09.2022).

анализе и сертификации заимствованного кода). Наконец, реализация только критичных стадий, по определению, должна обеспечить наивысшую доверенность, однако отсутствуют не только требования по полноте и глубине проверок, но в ряде случаев – понимание того, каких проверок будет достаточно. Особенно высока эта неопределённость для современных маршрутов с нормами менее 65 нм.

Все три стратегии могут дать наилучший результат с точки зрения бесшовности. Однако при ненадлежащем внимании к этому критерию возможно ухудшение качества, особенно в стратегии с открытым кодом.

Следующие два критерия наиболее субъективны, однако могут стать причиной, по которой отечественные САПР окажутся совершенно не эффективными и в конечном счёте невостребованными. Под профанируемостью (со стороны разработчика и пользователя САПР) будем понимать способность свести на нет эффективность использования САПР, при соблюдении формальностей и выполнении вероятных требований контролирующих органов (как внешних по отношению к предприятию-разработчику, так и внутренних – таких как служба главного конструктора или иная служба обеспечения качества по ОСТ 11 0999). Со стороны разработчика САПР наименее «профанируемой» является стратегия реализации полного маршрута, наиболее – реализация только критичных стадий, главным образом, из-за вышеупомянутой неопределённости относительно полноты и глубины требуемых проверок в разных маршрутах. Со стороны пользователя САПР наиболее профанируемой, каким бы странным это ни показалось на первый взгляд, является стратегия реализации только критичных стадий: даже при идеально полных и глубоких проверках, реализованных в САПР, разработчик ЭКБ может продолжить пользоваться привычными САПР «большой тройки», а контролирующим структурам предоставлять специально сформированные протоколы проверок, лог-файлы и т.п. Исключить такое поведение разработчика ЭКБ полностью, к сожалению, невозможно, даже при высоком качестве и удобстве отечественных САПР, поскольку нельзя недооценивать силу привычки и других человеческих факторов. Таким образом, профанируемость также должна учитываться при выборе стратегии создания отечественных САПР.

На рис. 2 показана предлагаемая трёхкомпонентная структура организации разработки САПР. В центре структуры видится организация, осуществляющая научно-методическое руководство и создающая консорциум разработчиков в среде компаний, имеющих тот или иной задел. Такой организацией (экспертным центром) могло бы стать создаваемое в соответствии с Указом Президента РФ от 30.03.2022 № 166 научно-производственное объединение, специализирующееся на разработке, производстве, технической поддержке и сервисном обслуживании доверенных программно-аппаратных комплексов для критической информационной инфраструктуры (КИИ). Учитывая колоссальную сложность создания программной платформы САПР, необходимо привлечение опытных программистов и специалистов по поддержке и продвижению продукта на рынке, поэтому успешное создание отечественной платформы САПР зависит от возможности привлечения к работе крупной ИТ-компании («Яндекс», «Лаборатория Касперского», «ВК» или др.). Эта компания может осуществлять и разработку, и реализацию платформы САПР отечественным и зарубежным дизайн-центрам, на рис. 2 обозначенным буквами кириллицы «А...Я» и латиницы «A…Z». Референсные проекты, на первых этапах выполняемые на зарубежных промышленных САПР и служащих для отработки маршрутов проектирования на отечественной платформе, должны разрабатываться в рамках межуниверситетской кооперации. Эти же университеты будут готовить необходимые кадры и выполнять научно-исследовательские и поисковые работы в сотрудничестве с профильными академическими институтами.

Рис. 2. Предлагаемая трёхкомпонентная структура организации разработки отечественных САПР

Необходимым условием успешного продвижения отечественных САПР на рынках является защита интеллектуальной собственности патентами как на внутреннем рынке, так и на перспективных внешних рынках. Права на отечественную САПР должны быть переданы от государства ИТ-компании, с обязательными и законодательно обоснованными выплатами лицензионных вознаграждений разработчикам – членам консорциума.

Важно отметить, что главным показателем качества разрабатываемой платформы САПР должна быть не выручка от реализации лицензий, а успешная разработка проектов, их изготовление на отечественных и зарубежных фабриках и последующие успешные испытания. В предлагаемой модели структуры разработки отечественной платформы САПР дизайн-центры не должны выполнять роль исключительно потребителей – они могут предложить технические требования на тестовые проекты электронных компонентов (рис. 3). Сложность таких проектов должна быть не хуже 32-разрядного конвейерного микропроцессора с подсистемой памяти.

Все технические требования должны поступать в межуниверситетский центр, который осуществляет их первичную обработку, заключающуюся, в том числе, в обезличивании проектов (например, путём исключения указаний конкретных отечественных архитектур или уникальных IP-блоков высокоскоростных каналов, по которым можно было бы «вычислить» авторов), и направляет в экспертный центр проекты технических заданий. Экспертный центр дорабатывает проекты технических заданий и выдаёт их дизайн-центрам. Таким образом, реализуется аналог «двойного слепого» выполнения заданий: дизайн-центры не знают, чей проект они выполняют, а экспертный центр распределяет проекты также вслепую. Межуниверситетский центр может осуществлять параллельную разработку по данным техническим заданиям, результаты которой послужат референсом. Такой подход исключит подмену новых результатов готовыми топологическими проектами GDSII[5] и подмену разработки на отечественной платформе разработкой на зарубежных САПР. При этом можно будет максимально объективно выявить достоинства и недостатки программного обеспечения.

[5]URL: https://www.layouteditor.org/layout/file-formats/gdsii (дата обращения: 09.09.2022).

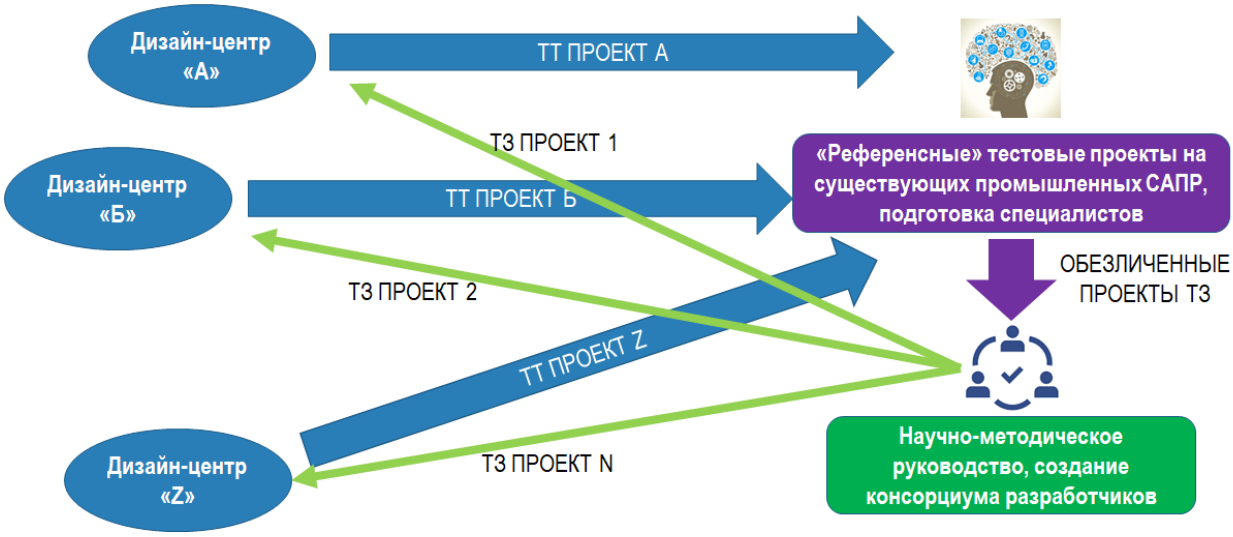

Рис. 3. Взаимодействие дизайн-центров с экспертной организацией и межуниверситетским центром

Как видно из сказанного, разработка отечественных САПР должна быть встроена в дорожную карту развития отечественных полупроводниковых технологий и поддержана отечественной вычислительной инфраструктурой. Отсюда видны ключевые риски выполнения предлагаемого проекта программы: отсутствие доступа к современным технологическим процессам; дефицит отечественных вычислителей. Кроме того, необходимо не только привлечь, но и удержать участников разработки от перехода в компании-конкуренты или в другие отрасли. Это можно сделать как материальными средствами (заработной платой выше рыночной), так и нематериальными – например, если участники будут осознавать, что решается не частная коммерческая задача, а составная часть большой задачи по обеспечению технологического суверенитета и развития страны.

Горбунов Максим Сергеевич
кандидат технических наук
Национальный исследовательский ядерный университет «МИФИ», доцент
Каширское ш., 31, Москва, 115409, Россия
АО «ЭНПО СПЭЛС», ведущий научный сотрудник
Каширское ш., 31, Москва, 115409, Россия
e-mail: msgorbunov@mephi.ru, https://orcid.org/0000-0002-4017-7033

Данилов Игорь Александрович
кандидат технических наук
Национальный исследовательский ядерный университет «МИФИ», инженер-исследователь
Каширское ш., 31, Москва, 115409, Россия
АО «ЭНПО СПЭЛС», старший научный сотрудник
Каширское ш., 31, Москва, 115409, Россия
e-mail: iadanilov@mephi.ru, https://orcid.org/0000-0001-7952-5392

Анатолий А. Малюк
Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
e-mail: AAMalyuk@mephi.ru, http://orcid.org/0000-0002-5746-1508

СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКИЕ ПРИЕМЫ ИНФОРМАЦИОННОЙ ВОЙНЫ

DOI: http://dx.doi.org/10.26583/bit.2022.3.02

Аннотация. С конца XX века информационные технологии начали активную экспансию во все сферы жизни общества, что привело его к новому этапу развития, получившему название «информационного». В новом обществе главным элементом существования людей стала информация. По этой причине они очень часто попадают под влияние лиц, заинтересованных в решении различного рода политических проблем в нужном им ключе, что является ничем иным, как «информационным оружием». Сегодня в мире можно наблюдать такие яркие результаты его применения, как ненависть между гражданами различных государств, дезинтеграция общества и создание образа врага. Успешное ведение информационной войны на международной арене может обеспечить огромное влияние на мнение мировой общественности. По своей сути информационная война уже стала разновидностью военного межгосударственного противостояния. В развитии такого рода конфликтов важнейшим элементом является информационно-психологическое подавление противника, заключающееся в том, чтобы напугать и эмоционально подавить оппонента. В этих условиях знание форм и методов такой информационной войны позволит не только ослабить и минимизировать ее накал, но и обезопасит людей, предоставляя им возможность обеспечить как общую, так и информационную безопасность. В связи с этим данная статья посвящена исследованию проблемы классификации различных приемов информационно-психологического воздействия на личность и общество и особенностей их применения для реализации тех или иных целей вероятного противника.

Ключевые слова: информационное общество, информационная война, информационно-психологическое воздействие на личность и общество, демагогические приемы информационного противоборства.

Для цитирования: МАЛЮК, Анатолий А. СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКИЕ ПРИЕМЫ ИНФОРМАЦИОННОЙ ВОЙНЫ. Безопасность информационных технологий, [S.l.], т. 29, № 3, с. 18–37, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1431. DOI: http://dx.doi.org/10.26583/bit.2022.3.02.

Anatoly A. Malyuk
National Nuclear Research University MEPHI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31, Moscow, 115409, Russia
e-mail: AAMalyuk@mephi.ru, http://orcid.org/0000-0002-5746-1508

Socio-psychological techniques of information warfare

DOI: http://dx.doi.org/10.26583/bit.2022.3.02

Abstract. Since the end of the XX century, information technologies have begun to actively penetrate into all spheres of society, which led it to a new stage, so-called "informational". In the new society, information has become the main element of people's existence. For this reason, they very often fall under the influence of persons interested in solving various kinds of political problems in the way they need, which is nothing else than an "information weapon». In the world today one can observe such vivid results of its application as hatred between citizens of different states, the disintegration of society and the creation of the image of an enemy. The successful conduct of an information war in the international arena can provide a huge impact on the opinion of the world community. At its core, the information war has already become a kind of military interstate confrontation. In the development of such conflicts, the most important element is the informational and psychological suppression of the enemy, which consists

in frightening and emotionally suppressing the opponent. In these sense, the knowledge of forms and methods of such information warfare will not only weaken and minimize its effect, but also protect people, giving them the opportunity to ensure both general and information security. This paper is devoted to the problem of classifying of various methods of informational and psychological impact on the individual and society and the features of their application for the realization of certain goals of a potential enemy.

Keywords: information society, information war, information and psychological impact on the individual and society, demagogic techniques of information warfare.

For citation: MALYUK, Anatoly A. Socio-psychological techniques of information warfare. IT Security (Russia), [S.l.], v. 29, no. 3, p. 18–37, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1431. DOI: http://dx.doi.org/10.26583/bit.2022.3.02.

1. Информационная война как средство военно-силового противоборства

В настоящее время мы являемся свидетелями бурно развивающегося целенаправленного использования информационных средств и современных информационных технологий для ведения вооруженной борьбы на межгосударственном уровне (хотя, заметим в скобках, эти средства активно применяются и во внутриполитической борьбе). Анализ тенденций в развитии военно-силового противоборства ясно показывает, что «кибервойны», или в более широком смысле «информационные войны», превращаются в основное средство борьбы в XXI веке [1, 2]. Исторический экскурс приводит нас к следующей картине (рис. 1).

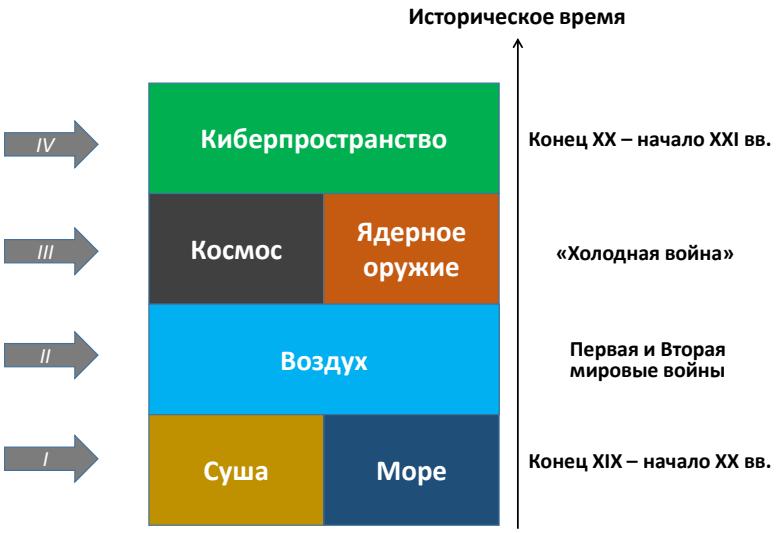

Рис. 1. Пространство военно-силового противоборства
Fig. 1. The space of military-power confrontation

В конце XIX века пространством военно-силового противоборства являлись суша и море, именно там был основной театр военных действий. Далее, Первая и Вторая мировые войны расширили это пространство, подключив сюда воздух. В период «холодной войны» соперничество переместилось в космос и в область создания и развития ядерного оружия. Наконец, в конце XX – начале XXI века война все активнее перемещается в киберпространство. В переживаемую нами сегодня информационную эпоху чрезвычайно высокой становится информационная зависимость всех сфер жизнедеятельности современного общества от информационных технологий. Это делает информационную

войну очень эффективным средством нанесения непоправимого ущерба «противнику», а «информационное оружие» представляет серьезную военную угрозу [3–6].

В подтверждение этого можно привести оценку американских экспертов, утверждающих, что нарушение работы компьютерных сетей, используемых в системах управления государственными и банковскими структурами США, путем вывода из строя вычислительных и связных средств или уничтожения хранящейся в сетях информации способно нанести экономике страны настолько серьезный ущерб, что его можно сравнивать с ущербом от применения против США ядерного оружия[1].

В профессиональных кругах сегодня существует мнение, что суть информационной войны состоит в достижении какой-либо страной (или группой стран) подавляющего преимущества в информационной области, позволяющего с достаточно высокой степенью достоверности моделировать поведение «противника» и оказывать на него в явной или скрытой форме выгодное для себя влияние. Таким образом, можно предположить, что страны, проигравшие информационную войну, проигрываю ее «навсегда», поскольку их возможные шаги по изменению ситуации, которые сами по себе требуют колоссальных материальных и интеллектуальных затрат, будут контролироваться победившей стороной [7].

Анализ многочисленных публикаций и информации, циркулирующей в сети Интернет (в том числе, данных, опубликованных ЦРУ США), приводит к выводу, что сегодня число стран, разрабатывающих информационное оружие (в основном, использующее Интернет, в том числе социальные сети), превышает 120 (для сравнения, число стран, разрабатывающих оружие массового уничтожения, составляет по различным данным, опубликованным в открытой печати, 30), и рано или поздно они получат возможность вести информационные войны. Основными задачами в них, очевидно, будут дезорганизация функционирования критически важных военных, промышленных, административных объектов и систем «противника», а также информационно-психологическое воздействие на военно-политическое руководство, войска и население [8].

Известно, что в США на сегодня уже создана система ведения информационных войн (*Information operations*) технической и психологической направленности. Причем, мы каждый день наблюдаем постоянное усиление Западной экспансии, направленной на противодействие развивающемуся евроазиатскому сотрудничеству в политической, экономической и идеологической сферах.

Итак, попробуем четко сформулировать основные цели информационной войны. Из предыдущего изложения напрашивается заключение, что этими целями могут быть:

- дезорганизация деятельности управленческих структур, транспортных потоков и средств коммуникации;
- блокирование деятельности отдельных предприятий и банков, а также целых отраслей промышленности путем нарушения многозвенных технологических связей и системы взаиморасчетов, проведения валютно-финансовых махинаций и т.п.;
- инициирование крупных техногенных катастроф на территории «противника» в результате нарушения штатного управления технологическими процессами и объектами, имеющими дело с большими количествами опасных веществ и высокими концентрациями энергии;
- массовое распространение и внедрение в сознание людей определенных представлений, привычек и поведенческих стереотипов;
- вызов недовольства или паники среди населения, а также провоцирование деструктивных действий различных социальных групп.

[1]По материалам средств массовой информации.

При этом объектом информационного противоборства может явиться любой объект, в отношении которого возможно осуществление информационного воздействия, результатом которого будет модификация его свойств как информационной системы. Исходя из этого, в качестве таких объектов можно рассматривать и системы социальных, политических и психологических отношений информационного общества [9, 10]. Таким образом, объектом информационного противоборства может стать любой сегмент информационно-психологического пространства, в том числе массовое и индивидуальное сознание граждан, социально-политические системы и процессы, информационная инфраструктура, информационные и психологические ресурсы. Очень красноречиво в этом смысле высказался известный ученый С.П. Расторгуев [11]: «… черепаха не знала и уже никогда не узнает, что информационная война – это целенаправленное обучение врага тому, как снимать панцирь с самого себя …».

Отметим здесь, что информационное противоборство в области социально-политических отношений явление не новое и имеет глубокие исторические корни. Примеры использования такого рода информационного оружия и борьбы с ним (защиты от информации) мы можем найти и в нашей истории. Возьмем, например, документ, относящийся к XVIII веку. Это Указ Императрицы Елизаветы Петровны[2], приведенный на рис. 2.

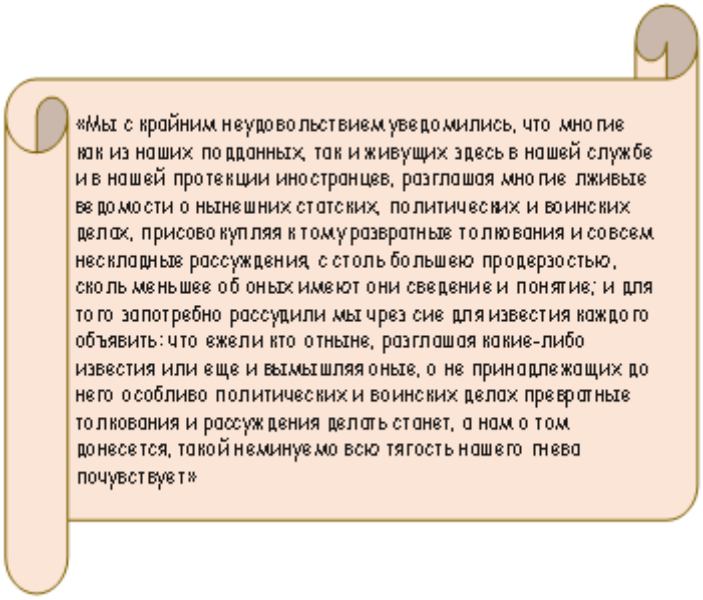
«Мы с крайним неудовольствием уведомились, что многие как из наших подданных, так и живущих здесь в нашей службе и в нашей протекции иностранцев, разглашая многие лживые ведомости о нынешних статских, политических и воинских делах, присовокупляя к тому развратные толкования и совсем нескладные рассуждения, с столь большею продерзостью, сколь меньшее об оных имеют они сведение и понятие; и для того запотребно рассудили мы чрез сие для известия каждого объявить: что ежели кто отныне, разглашая какие-либо известия или еще и вымышляя оные, о не принадлежащих до него особливо политических и воинских делах превратные толкования и рассуждения делать станет, а нам о том донесется, такой неминуемо всю тягость нашего гнева почувствует»

Рис. 2. Указ Императрицы Елизаветы Петровны (1750 г.)
Fig. 2. Decree of Empress Elizabeth Petrovna (1750)

Завершая этот раздел статьи, попробуем четко определить объекты и субъекты информационного противоборства. Итак, основными объектами применения информационного оружия в современных условиях будут являться:

- компьютерные и связные системы, используемые государственными и правительственными организациями при выполнении своих управленческих функций;
- военная информационная инфраструктура, решающая задачи управления войсками и боевыми средствами, сбора и обработки информации в интересах вооруженных сил;

[2]Газета «С. Петербургские ведомости», 1750 г., № 46.

- информационные и управленческие структуры банков, транспортных и промышленных предприятий;
- средства массовой информации, в первую очередь электронные (радио, телевидение, Интернет и т.д.);
- психологические ресурсы общества (система ценностей, индивидуальное и массовое сознание граждан, их психическое здоровье).

К субъектам, которые могут применять информационное оружие, надо отнести:

- государства, их союзы и коалиции;
- международные организации;
- негосударственные незаконные вооруженные формирования и организации террористической, экстремистской, радикальной политической и религиозной направленности;
- транснациональные корпорации;
- виртуальные социальные сообщества;
- медиа-корпорации;
- виртуальные коалиции.

Особо надо выделить роль в информационно-психологической борьбе сетевых корпораций. Во-первых, в глобальном информационном обществе они практически обладают всеми признаками суверенного государства – территорией, определяемой ареалом распространения их сетевой инфраструктуры, стратегическими ресурсами (информационными потоками в их информационных и телекоммуникационных системах), «населением» (штатом сотрудников) и относительно полным суверенитетом. Во-вторых, транснациональные корпорации, разрабатывая новые информационно-коммуникационные технологии, развивая свои информационные и телекоммуникационные системы и сети, контролируя циркулирующие по ним потоки, создают театр военных действий, на котором затем будут разворачиваться боевые действия между участниками информационно-психологического противоборства.

2. Негативный контент как инструмент информационно-психологического воздействия

Сосредоточимся теперь на основной проблеме данной статьи – воздействии информационного оружия на психологические ресурсы общества [12, 13], под которыми мы понимаем систему ценностей, индивидуальное и массовое сознание граждан, их психическое здоровье.

Для начала приведем цитату из одного из выступлений Патриарха Московского и Всея Руси Кирилла, на наш взгляд, как нельзя лучше иллюстрирующую обозначенную проблему: «Если в старые времена круг влияния на человека был очень ограничен, то сегодня каждый, кто публикует свои мысли и слова в Интернете, становится в ряд тех, кто может оказать страшное, разрушительное воздействие на человеческую природу. Мы знаем, что тысячи и миллионы сегодня влияют на наше сознание, на наш разум, на наши чувства».

Очень красноречиво о характере и задачах такого воздействия в 1945 г. высказался бывший директор ЦРУ США А. Даллес[3]. Дословно он говорил: «Мы найдем своих единомышленников, своих помощников и союзников в самой России. Эпизод за эпизодом будет разыгрываться грандиозная трагедия гибели самого непокорного на земле народа,

[3]США уничтожает Россию-План Алена Даллеса -"ГАРВАРДСКИЙ ПРОЕКТ"- "ХЬЮСТОНСКИЙ ПРОЕКТ". URL: https://russiasila.livejournal.com/2516.html. 25 апреля, 2011 (дата обращения: 10.06.2022).

окончательного угасания его самосознания. Литература, театр, кино – все будет изображать и прославлять самые низменные человеческие чувства. Мы будем всячески поддерживать и поднимать, так называемых, художников, которые станут насаждать и вдалбливать в сознание культ секса, насилия, садизма, предательства – словом, всякой безнравственности. Хамство и наглость, ложь и обман, пьянство и наркоманию, животный страх и вражду народов, прежде всего, вражду и ненависть к русскому народу – все это мы будем незаметно культивировать. Мы будем расшатывать таким образом поколение за поколением… Мы будем драться за людей с детских, юношеских лет, будем всегда главную ставку делать на молодежь, станем разлагать, развращать, растлевать ее. Мы сделаем из них космополитов».

Рассмотрим далее возможности использования в обозначенных целях негативного контента, циркулирующего в СМИ и в Интернете (прежде всего в социальных сетях) [14–16]. В соответствии с устоявшимися понятиями, под негативным контентом будем понимать информацию, оказывающую деструктивное воздействие на психику человека или общественное сознание. Сюда могут быть отнесены различные по виду материалы – тексты, картинки, аудио- и видеофайлы, ссылки на сторонние ресурсы. Все эти материалы в той или иной форме могут быть расценены как информационное оружие.

Остановимся на некоторых демагогических приемах, манипуляциях и подтасовках, использующихся сегодня для решения задач информационного противоборства. Отметим здесь, что очень многие риторические приемы, широко используемые сегодня в информационном противоборстве, были отражены еще в книге Карела Чапека[4]. В расширенном виде их можно представить в виде следующих ниже трех классов[5].

3. Опровержение аргументации

- *Прямые бездоказательные утверждения.*

Сюда могут быть отнесены выражения типа «наш продукт – номер один на рынке …». Множество примеров этого подхода можно увидеть в разыгравшейся информационной войне Запада по поводу специальной операции России на Украине. Вот только некоторые из них, взятые из различных выступлений Президента США Дж. Байдена[6]:

– «Мы – Соединенные штаты, непреодолимы, и мы владеем финишной чертой».
– «Свобода – это подавляющее американское понятие».
– «XXI век будет веком Америки».

- *Ссылка на стереотипы.*

Если взять пример такого подхода из часто употребляющихся выражений в обычной жизни, то это может быть, например, такая фраза: «естественно, все женщины хотят детей». Но такой подход может быть и эффективным приемом информационного противоборства. За примерами далеко ходить не надо. США постоянно подчеркивают, что являются оплотом демократии (естественно США – это демократия). Однако еще 8 января 1918 г. Вашингтон фактически установил новый мировой порядок. «14 пунктов Вильсона» можно считать прямым заявлением Америки на мировое господство. Очень красноречиво об этом в свое время высказался И.В. Сталин: «Я всегда думал, что

[4]Карел Чапек. Двенадцать приемов литературной полемики или Пособие по газетным дискуссиям. URL: lib.ru/SOCFANT/CHAPEK/gazeta.txt (дата обращения: 10.06.2022).
[5]Нестеренко Ю.Л. Демагогия. URL: https://wikilivres.ru/Демагогия_(Нестеренко) (дата обращения: 10.06.2022).
[6]80 лучших фраз Джо Байдена. URL: https://ru1.warbletoncouncil.org/frases-joe-biden-399 (дата обращения: 10.06.2022).

демократия – это власть народа, но вот товарищ Рузвельт мне доходчиво объяснил, что демократия – ЭТО ВЛАСТЬ АМЕРИКАНСКОГО НАРОДА»[7].

- *Использование неявных умолчаний.*

Например, такое умозаключение – «стремиться к богатству бессмысленно, ведь его не возьмешь на тот свет». Данный прием может эффективно использоваться для манипуляции общественным мнением в целях внедрения в сознание под видом объективной информации неявного, но желательного для определенных групп содержания, для воздействия на болевые точки общественного сознания, возбуждающего страх, тревогу, ненависть и т.п. С помощью этого приема возможна также реализация замыслов и скрываемых целей, достижение которых одна из сторон противоборства связывает с поддержкой общественным мнением своей позиции. Пример последнего времени – постоянная пропаганда наращивания санкций против России за «агрессию» против Украины, с раздуванием того вреда, который они наносят ее экономике. При этом умалчивается вред, наносимый тем странам, которые принимают подобные решения.

- *Ссылки на недостоверные источники.*

В обыденной жизни примером может быть выражение: «у моего соседа друг лично видел …». К этому демагогическому приему может быть отнесено получившее в последнее время чрезвычайно широкое распространение использование фейковых новостей [17], особенно в связи со специальной военной операцией России на Украине. Вот только некоторые примеры такого рода фейков, в разное время появившихся в зарубежных СМИ: о тактике российских военных; об артиллерии российских войск во дворах; о блокировке техники Apple на территории России; об отказе военных из Чеченской республики и Дагестана; о том, что в Белгороде не хватает донорской крови – и т.д., и т.п.

- *Выдача желаемого за действительное.*

Например, выражения такого рода: «Смерть навсегда несправедлива, поэтому ее не может быть». Примеры такого приема легко найти во всякого рода политических заявлениях. Например, предвыборное утверждение партии «Яблоко», представляющее то, чего очень хочется автору, как объективную реальность. Дословно это звучит следующим образом: «… в парламенте нужна настоящая оппозиция – такая, как «Яблоко»; только такая оппозиция остановит произвол власти, только такая оппозиция помешает разворовывать миллиарды рублей…».

- *Некорректные аналогии.*

Примером может являться следующее выражение: «сомневающийся подобен слепцу». Другой пример. В истории денежной единицы США, например, было установлено, что доллар неплохо обращается в Америке, Европе, Азии и Австралии. Учитывая, что это части света, можно прийти к популярному умозаключению, что «доллар – он и в Африке доллар». Как яркий пример такого приема в информационной войне можно привести еще активно продвигаемую в связи со специальной военной операцией России на Украине аналогию с действиями США в конфликтах в Ираке, Сирии, Афганистане, Югославии и др. Как же можно действовать по-другому, ведь аналогичное уже имело место?

- *Корректные аналогии.*

Сюда могут быть отнесены выражения типа «такие налоги – это просто грабеж». В этом ключе сформулированы и многие тезисы в западных СМИ, посвященные уже упоминавшейся нами специальной военной операции России на Украине. Звучат они

[7]Ироничная цитата Сталина о демократии, которая восхищает до сих пор. URL: https://za-dergavy.livejournal.com/260137.html (дата обращения: 10.06.2022).

примерно так: «российская специальная операция – это захват территории и уничтожение мирного населения Украины». Видим, что это яркий пример информационного противоборства.

- *Количественно-качественные подмены.*

Смысл такой демагогии может быть проиллюстрирован, например, следующим умозаключением: «нет разницы, умрет один человек или десять, ведь в любом случае погибнут люди». В этом смысле довольно часто в сфере информационного противоборства можно встретить попытки оправдать терроризм с помощью подмены такого рода: «Террористы убили только одного, а спецназовцы – десять!». Демагогию этого вида особенно охотно используют всевозможные «правозащитники».

- *Некорректное следствие.*

В литературе, посвященной исследованию демагогических приемов, довольно часто можно встретить следующее высказывание: «Сумасшедшие никогда не признают, что они сумасшедшие. Все, кто не признались в безумии – сумасшедшие». Некорректное следствие очень часто используется в тактике информационной войны и применяется, когда одна из сторон отрицает предъявленное ей обвинение. Самый простой вариант некорректного следствия – это конструкция «если А, то Б», в которой на самом деле Б вовсе не следует из А. Особенно часто такого рода прием используется для оправдания терроризма [18]. Примером может служить муссируемое в последнее время обвинение России в спонсировании терроризма: «вы поддерживаете Донбасс, когда Украина проводит антитеррористическую операцию». Более сложный вариант – логически ошибочная конструкция «если из А следует Б, то из Б следует А». Здесь можно привести такой популярный фейк: «Россия напала на Украину, что привело к огромным жертвам среди мирного населения». Это вполне соответствует приведенному выше демагогическому приему. Здесь имеется прямая ссылка на ложный стереотип.

- *Выдача следствия за причину.*

Снова возьмем пример из обыденной жизни: «Большинство невротиков когда-либо обращались к психологу. От психологов один вред». Суть использования такого приема в целях информационного противоборства заключается в выворачивании причинно-следственной связи наоборот, что позволяет исказить картину до полной противоположности. Например, такая фраза: «Все беды современной Украины вызваны стремлением Путина восстановить Советский Союз». На самом же деле именно распад Советского Союза вызвал целый поток негативных явлений на всем постсоветском пространстве.

- *Выдача корреляции за причину.*

Корреляция между событиями или явлениями никоим образом не свидетельствует о наличии между ними причинно-следственной связи. Такая корреляция может быть простым совпадением. Классический пример: «все умершие от рака до этого пили воду». Примером использования этого приема в информационном противоборстве может служить утверждение, что переселение граждан Украины в европейские страны вызвано специальной военной операцией России. Хотя известно, что такой отток существовал всегда с момента распада СССР и особенно усилился в 2014 г. после подписания Соглашения об ассоциации между Украиной и ЕС. На рис. 3 приведен еще очень характерный пример этого приема – «доказательство» того, что глобальное потепление вызвано снижением количества пиратов[8].

[8]Основы статистических методов обработки медико-биологических данных – презентация. URL: www.myshared.ru/slide/543451/ (дата обращения: 10.06.2022).

Рис. 3. Пример выдачи корреляции за причину
Fig. 3. An example of the issue of correlation for the cause

- *Порочный круг.*

Очень красноречивый пример демагогии такого рода выглядит следующим образом: «лидер не может лгать, ведь он говорит, что его слова – правда». Именно такой подход очень часто используется при формировании различного рода фейков, как бы опирающихся на мнения признанных авторитетов (как правило, государственных и общественных деятелей). Но здесь будет полезным привести мнение доктора политических наук Ирины Василенко, которая в статье «Информационная война как фактор мировой политики»[9] дословно отмечает: «В эпоху информационных войн порочный круг замыкается: те, кто занимаются информационными манипуляциями, становятся первыми жертвами этих бескровных операций и вскоре уже не в состоянии отличить вымысел от реальности, поскольку лжец должен верить в созданный им вымысел».

- *Некорректная дихотомия.*

Например, такая дилемма: «или анархия, или тирания». Как видим, этот прием заключается в упущении иных возможностей, кроме некоторых двух рассматриваемых. Как правило, одна из возможностей отметается как ложная или неприемлемая, после чего оставшаяся принимается за истинную (приемлемую), в пользу которой и делается выбор. Некорректная дихотомия особенно любима политиками, например, такое актуальное сегодня противопоставление – «или западная (американская) демократия, или российская (путинская) диктатура».

- *Некорректное использование квантора всеобщности.*

Как считает Ю.Л. Нестеренко[5] данный демагогический прием, состоящий в том, что некоторое свойство (как правило, характерное для большинства объектов некоторого класса) безосновательно приписывается всем объектам этого класса (а иногда еще и других классов). Как пример можно привести расхожее мнение: «все русские любят выпить». Если вспомнить о ведущейся на протяжении уже нескольких десятилетий и особенно обострившейся после 2010 г. войне с российским спортом, то можно привести

[9]Василенко И. Информационная война как фактор мировой политики. Государственная служба. 2009, № 3. URL: https://cyberleninka.ru/article/n/informatsionnaya-voyna-kak-faktor-mirovoy-politiki (дата обращения: 10.06.2022).

пример живущего с 1995 г. в Швейцарии писателя Михаила Шишкина[10], который заявил в интервью *Tages-Anzeiger* накануне ЧМ-2018 по футболу: «В России спорт понимается только как продолжение войны, как попытка уничтожить врагов в спорте, коль скоро мы не можем уничтожить их на войне…»

- *Неявное задание множества.*

Пример подобной демагогии – метод «настоящего шотландца». Основной прием использования этого подхода в информационном противоборстве – это выбрать, например, неудачное высказывание какого-либо представителя противника, которое является, как правило, частным мнением, и выдать его за основное кредо действий всей противостоящей стороны.

- *Темпоральная индукция.*

Снова сошлемся на Ю.Л. Нестеренко[5], который определяет темпоральную индукцию как применение неполной индукции ко времени: «такого сейчас нет и никогда не было – значит, и не будет». Демагог, таким образом, исключает из рассмотрения развитие и саму возможность такового. Такой прием особенно эффективен в политической борьбе и активно используется разного рода ретроградами и врагами прогресса (например, внутриполитическая борьба демократов и республиканцев в США).

- *Отождествление части и целого.*

Этот прием основан на игнорировании того факта, что свойства системы в целом несводимы к свойствам ее элементов. В информационной войне этот подход может применяться как в одну сторону (например, можно приписать какому-то человеку свойства некоторого социального института – «посмотрите, этот человек родился в городе, где процветает наркомания»), так и в другую (приписывание системе свойств элементов, в частности, личных свойств социуму – «филиппинцы обиделись …»).

- *Теоретический формализм.*

Отметим, что это самый хитрый из приемов рассматриваемого нами класса, поскольку формально применяющий его демагог оказывается прав. Что можно возразить, например, на такое изречение: «отсутствие доказательств бытия не есть доказательство небытия»? Посмотрим, как это можно применить в качестве средства информационно-психологического воздействия. Воспользуемся здесь примером, приводимым Ю.Л. Нестеренко[5]. Кто-то утверждает, что некто глуп, и доказывает это утверждением, что за всю свою жизнь он не совершил ни одного умного поступка, зато сделал такие-то и такие-то глупости. Здесь, вообще говоря, мы имеем дело с некорректным следствием. Действительно, из того, что всякий дурак ведет себя глупо, еще не следует, что всякий, ведущий себя глупо – дурак. Более того, можно даже привести примеры, когда умник в определенной ситуации притворяется дураком. Однако с практической точки зрения, как подчеркивает упоминавшийся Ю.Л. Нестеренко, очевидно, что если некто не проявляет определенное свойство никогда, даже в ситуациях, когда это было бы для него явно выгодно, то с вероятностью, стремящейся к единице, он им просто не обладает. Этот прием часто сочетается с инверсией презумпции (о которой речь пойдет ниже) и используется, в частности, ревнителями «политкорректности», доказывающими, например, что представители ЛГБТ-сообщества ничем не отличаются от других членов общества.

[10]URL: https://palm.newsru.com/cinema/09jun2018/schischkin.html Писатель Михаил Шишкин призвал Швейцарию и другие страны "не лизать сапоги Путину" и бойкотировать ЧМ-2018, 09 июня 2018 г. (дата обращения: 10.06.2022).

4. Игнорирование аргументации

- *Прямое игнорирование.*

Если одна из сторон информационного противоборства чувствует, что не может ничего возразить по существу, то может попытаться просто проигнорировать неудобные для нее аргументы. Самым простым вариантом такого приема является прямое игнорирование. При этом сторона, применяющая этот прием, ведет себя так, словно доводов противоположной стороны вообще не было. Этот нехитрый прием лучше всего срабатывает в интеллектуально непритязательной среде, в особенности сочувствующей отстаиваемой при этом позиции. Как пример можно привести поведение представителей Германии, Франции и Украины в рамках Нормандского формата, которые как бы не слышали утверждений представителей России о разворачивающемся геноциде русских в Донбассе и полном невыполнении украинской стороной Минских соглашений, упорно проводя свою линию о суверенитете Украины и необходимости оказания ей всесторонней помощи и поддержки.

- *Простой увод.*

Развитием приема прямого игнорирования является увод от дискуссии – одна из сторон не просто игнорирует тезисы другой стороны, а, начав отвечать вроде бы на них, по возможности незаметно уводит дискуссию в сторону. В обыденной жизни такой простой увод называют «переводом стрелок». Поскольку в большинстве проблем, которые становятся предметом дискуссии, всегда есть доля вины каждой из сторон, то всегда можно перенести акцент как бы «с больной головы на здоровую». Этим активно пользуются всякого рода манипуляторы, перекладывая ответственность в нужную сторону.

- *Ответ вопросом на вопрос.*

Фактически такой прием является ничем иным, как переводом стрелок на противника в информационном противоборстве. Хрестоматийный пример: вопрос – «что вы делали вчера вечером?», ответ – «а вы где тогда были?». Дискуссия подобного рода предоставляет довольно широкие возможности для ведения информационной войны. Можно привести пример с уточняющими вопросами, такого рода вопросы, как правило, предполагают ответ «да» или «нет». Однако, если дать развернутый ответ, то можно, например, получить дополнительную информацию о «противнике». Для этого подходят такие вопросы:

- «Правильно ли я понимаю, что …»;
- «Почему?» (это один из лучших уточняющих вопросов, решающих сформулированную нами задачу);
- «То есть, вы говорите, что …»;
- «Если я вас правильно понял, то …»;
- «Я могу ошибаться, но, по-моему, вы сказали …».

- *Увод на верхний уровень.*

Суть этого приема заключается в следующем. Одна из сторон противоборства заявляет, что поднятый вопрос – частный случай более общего. Далее переводит рассуждения на этот «более общий вопрос» и пускает в ход еще целый набор демагогических приемов – некорректную индукцию, отождествление части и целого, некорректную дедукцию и т.д. Как пример, приведем фразу, которая в тех или иных формах использовалась (да и сейчас еще используется) как демагогия в условиях пока продолжающейся пандемии «*Covid-19*»: «болезнь – просто частный случай неблагополучия, поговорим о неблагополучии в общественной жизни».

- *Концентрация на частностях.*

Смысл этого приема – выбрать в аргументах противника какую-нибудь малозначимую частность и постараться сосредоточить всю дискуссию на ней. В обыденной жизни можно встретить, например, такую фразу: «О чем можно говорить с человеком, неверно расставляющим запятые?». Аналогичный пример из политической жизни: «О какой демократии можно говорить с Россией, если там убивают неугодных государственных и общественных деятелей» (реакция на убийство Б. Немцова в 2015 г.).

- *Некорректная терминология.*

К этому типу можно отнести, например, такое высказывание: «казнь – это убийство». Отметим, что манипуляции с терминами довольно часто применяются в информационном противоборстве. При этом одна из сторон стремится использовать некоторый термин в ином значении, нежели противник. Характерный прием здесь – вместо ответа противнику по существу начать придираться к используемой им терминологии. Например, в споре о преступлениях украинских нацистов начать яростно доказывать, что на Украине нет никакого нацизма, а есть защита национальных интересов.

- *Передергивание и доведение до абсурда.*

Под этот прием вполне подпадает, например, такая фраза: «Забыл? А голову ты не забыл?» (часто используется учителями, когда ученик говорит, что что-то забыл). Смысл такого приема заключается в передергивании, которое, как правило, сочетается с некорректной дискретизацией. При этом одна из сторон информационного противоборства, доведя тезис противника до абсурдной крайности, игнорирует, что помимо этой крайности есть и более разумные и взвешенные варианты. Этим приемом наиболее часто пользуются политики либерального толка, которые на любые предложения в области контроля и регулирования (например, Интернета) дословно заявляют: «Ну конечно! Давайте всех загоним в тюрьмы, давайте вернемся в 1937 г.». Или другой пример. Во время кампании по выборам мэра одна из партий, пытаясь нагнетать ксенофобские настроения среди избирателей, направленные против одного из кандидатов, занялась размещением постов, в которых этот кандидат загодя обвинялся в том, что, после того как он станет мэром, все ключевые должности в городской администрации будут «заняты его единоверцами», которые разворуют бюджет, приватизируют всю собственность и обложат данью «простого русского труженика».

- *Инверсия презумпции.*

Термин «презумпция» определяет, какой из противоположных тезисов считается верным по умолчанию, а какой надлежит доказывать. Таким образом, инверсия презумпции состоит в том, что одна из сторон противоборства вместо того, чтобы доказать свой тезис, требует (вопреки принятой презумпции), чтобы противник доказывал обратный. Например, такой тезис – «Почему это мы должны доказывать, что наше лечение помогает? Все видно и так, это вы докажите, что оно вредно». Отметим, что сегодняшнее противостояние России и объединенного Запада на Украине дает нам огромное множество примеров такого приема в информационной войне. Приведем только один из них. Это полемика вокруг массового убийства мирных граждан в г. Буче, совершенного в марте 2022 г. Запад выносит следующую презумпцию: «вторжение российских войск на Украину имеет признаки военных преступлений и преступлений против человечества, примером чего являются события в Буче». Доказательств этого объективно нет, но Россия, как противник в информационной войне, вынуждена доказывать обратное.

- *Выдвижение несимметричных условий.*

Этот прием, как правило, носит ультимативный характер. Например, такое выражение – «я очень занятой человек; если вы считаете, что эволюция существует, докажите мне просто и ясно, в одном абзаце». При использовании этого приема в информационной войне, если такого рода условия, выдвинутые одной из противоборствующих сторон, принимаются, то эта сторона получает преимущество, если отвергаются, то она заявляет, что дискуссия сорвана ее противником, который «побоялся» предоставить ей «нормальные» условия. Примеров использования описываемого подхода можно привести очень много из истории проведения различного рода международных переговоров, в частности, продолжающееся уже не один десяток лет противоборство, связанное с расширением блока НАТО.

- *Размен тезисами.*

Размен тезисами, как правило, апеллирует к вежливости: «я согласился с вами, теперь и вы меня уважьте». Здесь можно привести массу примеров, относящихся к развернутой сегодня Украиной дискуссии из области ее истории. Например, такая демагогия: «Я согласен с утверждением, что Киев – мать городов русских, но согласитесь и вы с тем, что из этого следует, что Россия фактически является дочерью Украины».

- *Излишний релятивизм.*

Если одна из сторон понимает, что ей нечего возразить по существу аргументов противника, то она может пуститься в разглагольствования в духе «все относительно», «абсолютной истины не существует», «каждый по-своему прав» и т.п. Можно привести такой пример: «Он совершил множество преступлений? Ну и что? Никто из нас не был в его ситуации, и кто мы, чтобы осуждать других людей …». Если говорить об информационном противоборстве, то вот пример такой демагогии[11]: «Было время, когда однополые отношения считались персоной нон грата. Сейчас такие виды отношений вполне приемлемы и даже поощряются. Есть те, кто все еще настаивает на том, что эта практика не должна быть разрешена, но их голоса заглушаются теми, кто считает, что она должна быть разрешена».

5. Отрицание логики

- *Прямая дискредитация тезиса.*

Дискредитация тезиса в соответствии с классификацией демагогических приемов, предложенной уже неоднократно упоминавшимся нами выше Ю.Л. Нестеренко[12] (кстати, на наш взгляд, это очень продуманный подход, позволяющий принимать обоснованные решения по противодействию этой демагогии), имеет цель «доказать», что тезис плох, вместо того, чтобы разбирать, истинен он или ложен. Таким образом, прямая дискредитация даже не содержит попыток доказательства, а прямо декларирует негодность тезиса. Например, такое выражение: «Даже если это правда, говорить так все равно нельзя. Это мерзко». На высказываниях такого рода целиком построено такое явление, как «политкорректность». Как один из последних примеров рассматриваемого приема можно привести высказывание канцлера ФРГ О. Шольца на Мюнхенской конференции по безопасности (19.02.2022), где он дословно сказал: «На Донбассе происходит геноцид – это, конечно, смешно».

[11]Каковы некоторые примеры релятивизма? – Quora. URL: https://www.quora.com/What-are-some-examples-of-relativism (дата обращения: 10.06.2022).
[12]Нестеренко Ю.Л. Демагогия. URL: https://www fan.lib.ru/n/nesterenko_j_l/text_0610.shtml#:~:text= Прямая дискретизация тезиса даже не может обвинить оппонента в демагогии (дата обращения: 10.06.2022).

- *Прямая апелляция к эмоциям.*

Подобного рода приемы напрямую утверждают, что согласиться с аргументами противоборствующей стороны нельзя по чисто эмоциональным причинам. Например, «разве какие-то сухие рациональные выкладки могут заставить нас отказаться от …». Из актуальных сегодня примеров такого информационного противоборства можно привести аргументацию противников вакцинации от «*Covid-19*»: «Вакцины – это настолько неестественно. Отвратительно, что люди соглашаются запускать себе в тело нечто подобное».

- *Объективно-субъективная подмена.*

Данный прием является фактически частным случаем прямой апелляции к эмоциям и заключается в подмене объективной картины, специально подобранной по признаку наибольшей неблагоприятности субъективной, в надежде, что последняя окажется эмоционально неприемлемой для противной стороны. Схема этого приема выглядит следующим образом: «Да, ошибки крайне редки. Но хотели бы вы сами стать жертвой такой вот ошибки?». Как пример, можно привести полемику между сторонниками и противниками смертной казни.

- *Использование эмоционально окрашенных терминов.*

Данный прием имеет широкое распространение в наблюдаемых нами в последнее время развязанных Западом информационных войнах против России. Заключается он в том, чтобы создать предвзятое мнение о доводах противника. Например, такие выражения – «вам диверсанты, нам партизаны» или «вам мятежники, нам повстанцы». Наверное, у всех у нас на слуху такие перлы западной пропаганды, как «аннексия Крыма», а не присоединение его в результате легитимного референдума, или «патриоты Украины», а не нацистские формирования. Этот перечень можно продолжать довольно долго.

- *Апелляция к морали.*

Апелляция к морали уместна лишь в споре, целью которого собственно и является попытка дать моральную оценку. Как пример, можно привести такой довод: «использование арбалетов аморально, так как они слишком смертоносны». Следует, однако, отметить, что ссылки на мораль (аморальность тезисов одной из сторон информационного противоборства или высокую моральность противоположной стороны) являются довольно грубым демагогическим приемом. Тем не менее, мы являемся свидетелями достаточно широкого его использования. Ярким примером этого является морализаторство по поводу предвоенной политики СССР в отношении Польши и Прибалтики. Типичная оценка событий того времени, часто используемая современными западными СМИ, выглядит следующим образом. «Аннексию Советским Союзом прибалтийских государств в 1940 г. нельзя считать просто «мерами по укреплению обороны» или «переустройства границ». Это был настоящий акт международного разбоя, в результате которого три суверенных государства потеряли не только независимость, но и четверть населения. Всему этому способствовало заключение нацистско-советского пакта, который дал Сталину и Гитлеру право на бандитизм в собственных «сферах влияния». При этом заметьте, что заключение «нацистско-демократического» сговора в Мюнхене не удостаивается такого осуждения. Он расценивается не как ошибка, а как мудрый стратегический маневр. Таким образом делается вывод о том, что «пакт Молотова-Риббентропа – однозначно преступление перед Польшей, Прибалтикой, Западом, Востоком, Севером, Югом, человечеством и человечностью».

- *Ссылки на нечто осуждаемое.*

Этот прием основан на том, что оспариваемый тезис объявляется частью некоей негативно воспринимаемой концепции. Другой вариант – в число его сторонников

записываются столь же осуждаемые личности. Приведем несколько примеров выражений такого рода:

- «Гитлер был католиком. Исповедь заменяет католикам совесть».
- «Называть негра негром – это расизм!».
- «Фашисты любили музыку Вагнера, значит, любить Вагнера – это фашизм».
- «Бесплатного образования и медицины могут требовать только ностальгирующие по коммунизму «совки»!».

- *Ссылки на одобряемых авторов или концепции.*

Здесь можно говорить об авторитетах из другой области или об авторитетах прошлого. Вообще же данный прием «зеркален» по отношению к предыдущему и использует те же самые подтасовки (необоснованное приписывание к «хорошей» концепции или принадлежность к ее неспецифическим, а также негативным элементам. А вот некоторые примеры выражений (ссылки на известные имена), явно нацеленных на информационно-психологические ресурсы общества (формирование «русофобии»)[13]:

- Академик Павлов (1932 г.): «Должен высказать свой печальный взгляд на русского человека – он имеет такую слабую мозговую систему, что не способен воспринимать действительность как таковую. Для него существуют только слова. Его условные рефлексы координированы не с действиями, а со словами». (В соответствии с исследованием, на которое мы сослались, Павлов никогда не говорил и не писал ничего подобного).
- Алексей Толстой: «Московия – русь тайги, монгольская, дикая, звериная». (В соответствии с тем же исследованием трудов Алексея Николаевича Толстого и Алексея Константиновича Толстого, оба писателя никогда ничего подобного не говорили и не писали).
- Иван Аксаков: «Ох как тяжко жить в России, в этом смердючем центре физического и морального разврата, подлости вранья и злодейства». (Тот же исследователь отмечает, что фраза вырвана из контекста и модифицирована. Аксаков сокрушается по поводу неудач России в Крымской войне и винит в этом взяточничество).

Подобного рода примеры можно еще продолжать очень долго.

- *Запугивание последствиями.*

В этом случае сторона, осуществляющая информационную агрессию, обычно даже не пытается отрицать истинности аргументов противника – она лишь упирает на то, что признание этой истинности будет якобы иметь неприемлемо тяжелые последствия. Так, например, смысл некоторых оправданий агрессии США против Ирака в начале текущего века сводится фактически к следующей позиции: «да, мы чудовищно ошиблись, но если это признать, то мы потеряли бы влияние и началась гражданская война». Другой вариант из политической жизни: «свобода слова и творчества – штука хорошая, но, если мы будем ею пользоваться, мусульмане обидятся и устроят нам джихад» или «если мы признаем ошибки нашего лидера, люди отвернутся от нашего учения».

- *Клевета.*

Наверное, термин «клевета» не нуждается в особых пояснениях. Фактически – это распространение заведомо ложной информации. Но представляется, что будет интересно посмотреть на его истоки. Здесь нам может помочь религиозная сфера. Назовем это некоторой духовно-информационной войной. Так вот, в этой войне Люцифер (иначе

[13]Информационная война - небольшое исследование. URL: www.great-country.ru/rubrika_articles/ros/101220-03.html (дата обращения: 10.06.2022).

называемый дьяволом, что в переводе с греческого языка означает «клеветник») распространяет заведомо ложную информацию о Боге и порочит Его перед лицом человека, внушая недоверие к Божьей любви и благодати, милости и истине, достоинству, славе и чести. Если посмотреть на сегодняшний день (2014-2020 гг.), то в этой связи можно привести высказывания таких политических деятелей, как Й. Столтенберг: «Нет никаких сомнений, что в восточной части Украины имеется сильное присутствие России. Там есть российские войска, там есть российское оружие, и Россия продолжает оказывать помощь и тренировать террористов»; Б. Обама: «Российские войска, которые вошли на Украину, – это не гуманитарная или миротворческая миссия. Там находятся российские боевые части с российским оружием и на российских танках. Это факты, которые можно доказать. Они не подлежат сомнению»[14].

- *Оскорбления.*

Оскорбления, в отличие от клеветы, всегда грубы и неприемлемы по форме. Целью оскорблений, как и клеветы, может быть не только создание негативного образа одной из сторон противоборства, но и выведение ее из себя, в надежде, что это еще больше дискредитирует ее образ у наблюдателей. Ярким примером такого приема является высказывание Президента США Дж. Байдена, который в одном из недавних своих выступлений назвал Президента России В. Путина убийцей.

- *Провокации.*

Этот прием связан с двумя предыдущими и направлен на то, чтобы подтолкнуть противодействующую сторону к неким неконструктивным, неодобряемым действиям и тем вызвать отрицательное отношение к ней со стороны наблюдателей. Чаще всего провоцируют на грубость, резкость и т.п. Один из самых простых приемов этого вида – прикинуться дураком (прямое игнорирование аргументов противной стороны и демонстративное непонимание ее тезисов с бесконечными глупыми вопросами). Расчет здесь делается на то, что противная сторона, понимая, что над ней просто издеваются, примет ответные меры, угрожающие ее репутации. Как пример, здесь можно привести не прекращающуюся уже несколько десятилетий полемику об ограничении продвижения НАТО на Восток и сохранении его в границах, по крайней мере, 1997 г.

- *Выдача нейтральных и позитивных качеств за недостатки.*

Этот прием часто сочетается с использованием тенденциозной терминологии: так принципиальность объявляется фанатизмом, смелость – авантюризмом. Характерным примером подобного подхода в международной политике сегодня, например, является вопрос о вступлении в НАТО двух нейтральных стран – Швеции и Финляндии. При этом для оправдания такого решения в ряде западных СМИ независимый статус страны объявляется главной угрозой ее безопасности.

- *Подчеркивание недостатков, не имеющих отношения к теме.*

Логика этого приема может быть выражена, например, такой фразой: «о чем можно говорить с человеком, делающим такие опечатки». Таким образом, противоборствующая сторона, использующая этот прием, может придраться к чему угодно. Основная идея этого метода состоит в том, чтобы найти «нужные» ассоциации и ярлыки, призванные заменить в сознании людей адекватное восприятие противоборствующей стороны. Например, на бывшего президента Украины В. Януковича западные манипуляторы приклеивали ярлык бандита, на В. Путина – ярлык диктатора, на всех русских вообще – ярлык «пьяного быдла».

- *Приписывание скрытых мотивов.*

Когда одна из сторон информационного противоборства не видит возможности придраться ни к каким доводам противника, ни даже к каким-то «отрицательным» его

[14]Интерфакс, Кризис на Украине. URL: http://www.interfax.ru (дата обращения: 10.06.2022).

сторонам, она нередко пытается утверждать (разумеется, голословно), что противник отстаивает свою позицию не ради истины, а якобы из-за неких тайных, корыстных мотивов: «Он не просто так это говорит. Он на зарплате у Моссада». Как пример такого подхода можно рассматривать один из тезисов современного Запада о характере отношений с Россией, который выражается примерно так: «Вся политика России, ее критика современных тенденций развития сплоченного вокруг США глобального цивилизованного общества основана на зависти к успехам объединенного Запада».

6. Пример технологии разработки и реализации конкретной операции информационной войны

Попробуем теперь продемонстрировать некоторый конкретный пример информационно-психологической операции, реально осуществленной в последнее время, и проанализировать ее цели и использовавшиеся приемы для их реализации. Таким, наверное, наиболее ярким примером может явиться инцидент в Солсбери (Великобритания), получивший название «Дело об отравлении Скрипалей». Напомним, что началась эта операция 4 марта 2018 г., когда при невыясненных обстоятельствах были отравлены С. Скрипаль, бывший офицер ГРУ и агент британской разведки МИ-6, и его дочь Ю. Скрипаль, гражданка Российской Федерации.

Как показывает анализ результатов серьезных экспертных исследований, выполненных А.В. Манойло [19], основная цель этой операции – обвинить Россию в разработке и применении (несмотря на целую систему принятых международных актов) химического оружия массового поражения. Как показал автор указанной работы, «Дело Скрипалей» включает два этапа. В основе первого этапа (4 – 22 марта 2018 г.) лежит классическая схема информационного противоборства, так называемая «игра с пошаговым повышением ставок» (рис. 4).

Рис. 4. Развитие событий на этапе «игра с пошаговым повышением ставок»
Fig. 4. The development of events at the stage of «the game with a step-by-step increase in bets»

Анализ представленного развития событий на первом этапе показывает, что, в основном, здесь применяются приемы опровержения аргументации. Наиболее часто мы видим прямые бездоказательные утверждения, ссылки на недостоверные источники и выдачу желаемого за действительное.

Однако развернутый скандал начал постепенно терять интерес у публики. В этой ситуации для продолжения спектакля необходимо было ввести новые повороты и новых действующих лиц. Так появились Петров и Баширов (сотрудники ГРУ) и с 5 сентября 2018 г. начался второй этап, построенный по схеме, также имеющей свое условное название «загонная охота» (рис. 5).

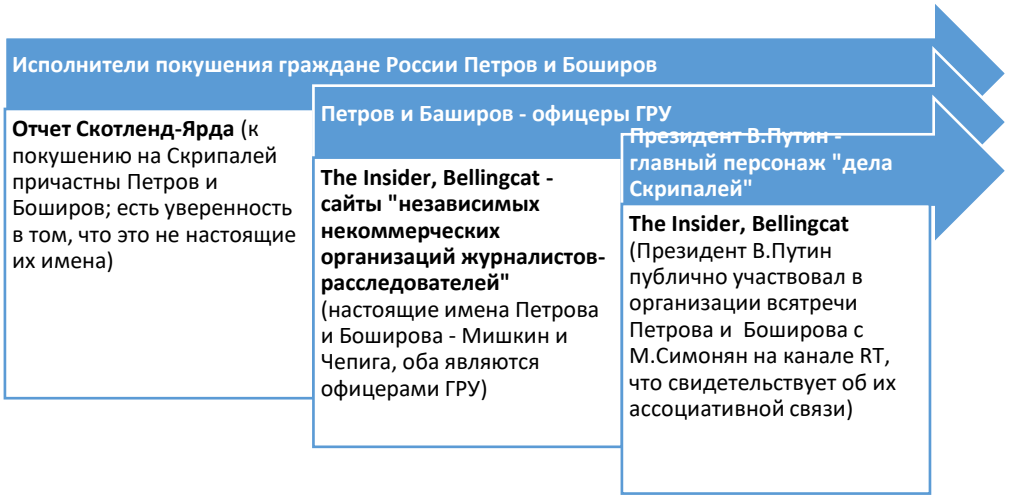

Рис. 5. Развитие событий на этапе «загонная охота»
Fig. 5. The development of events at the stage of «corral hunting»

Целью этого этапа являлось попробовать вывести ответственность за применение химического оружия лично на Президента РФ В.В. Путина, а попутно попробовать скомпрометировать его, используя и другие фейки, в частности о причастности к коррупционным историям, циркулировавшим в то время в западных СМИ («где коррупция, там Путин»).

На этапе «загонная охота» применяются все три рассмотренные нами группы приемов ведения информационной войны. Наиболее часто встречаются такие приемы, как прямые бездоказательные утверждения, некорректное следствие, увод на верхний уровень, инверсия презумпции, клевета.

Заключение

Попробуем сформулировать некоторые выводы из рассмотренного нами материала, определяющие основные задачи сегодняшнего дня в вопросах противодействия развивающейся информационной войне.

1. Ряд стран стремится получить преимущество в создании систем и средств ведения информационной войны, в том числе социально-психологической направленности. Такое развитие событий представляет серьезную угрозу национальной безопасности России.

2. Создание целостного комплекса средств, методов и приемов (в том числе демагогического характера) ведения информационной войны будет осуществляться постепенно, по мере развития в мире базовых информационных технологий и средств информационного противоборства, что позволяет осуществлять мониторинг этого процесса.

3. Тема информационного оружия и информационной войны, в силу своей чрезвычайной важности для безопасности страны, требует комплексной проработки ее военно-стратегических, социально-психологических, правовых, разведывательных и контрразведывательных аспектов, а также координации усилий всех заинтересованных ведомств России.

СПИСОК ЛИТЕРАТУРЫ:

1. Расторгуев С.П. Философия информационной войны. М.: Вузовская книга, МПСИ, 2003. – 301 с. URL: https://klex.ru/pec (дата обращения: 02.06.2022).
2. Ламинина О.Г. Информационные войны: миф или реальность? Гуманитарные ведомости Тульского государственного педагогического университета им. Л.Н. Толстого (сетевое издание). 2018, № 1(25), с. 17–23. URL: https://www.elibrary.ru/item.asp?id=35018244 (дата обращения: 02.06.2022) – EDN UQKSYT.
3. Попова С.В., Федоринов В.Е. Цели и последствия информационной войны. Воздушно-космические силы. Теория и практика. 2018, №6 (6), с. 15–21. URL: https://www.elibrary.ru/item.asp?id=(дата обращения: 02.06.2022) – EDN USAQKU.
4. Левин А.В. Особенности и виды информационных войн. Проблемы Науки. 2017, № 32(114), с. 63–66. URL: https://www.elibrary.ru/item.asp?id=30021833 (дата доступа 02.06.2022) – EDN ZGZDYV.
5. Андрусова Т.Б., Гомонова Ю.Г., Багаева А.П. Информационное оружие и информационные войны. Актуальные проблемы авиации и космонавтики. 2010, № 6, с. 403–404. URL: https://www.elibrary.ru/item.asp?id= (дата обращения: 02.06.2022) – EDN TBIBVT.
6. Добрышин М.М. Особенности применения информационно-технического оружия при ведении современных гибридных войн. I-methods. 2020, т. 12, № 1, с. 1–11. URL: https://www.elibrary.ru/item.asp?id=42636560 (дата обращения: 02.06.2022) – EDN PPGYRU.
7. Мусуралиева М.М. Понятие и сущность информационной войны. Известия вузов (Кыргызстан). 2015, № 1. URL: https://www.elibrary.ru/item.asp?id=23931974 (дата обращения: 02.06.2022) – EDN UDSHHJ.
8. Кихтан В.В., Качмазова З.Н. Информационная война: понятие, содержание и основные формы проявления. Вестник Волжского университета им. В.Н. Татищева. 2018, т. 2, № 2. URL: https://www.elibrary.ru/item.asp?id=35138943 (дата обращения: 02.06.2022) – EDN USGUUQ.
9. Айсаханова Е.С. Информационные войны как результат социального управления и социального взаимодействия в эпоху глобализации. Colloquium-journal. 2019, № 23–3(47). DOI: http://dx.doi.org/10.24411/2520-6990-2019-10774. – EDN YMJZID.
10. Егорова Л.С. Влияние информационных войн на стабильность государства. Коммуникология (электронный журнал). 2018, т. 3, № 2. URL: https://www.elibrary.ru/item.asp?id=35377852 (дата обращения: 02.06.2022) – EDN UVXYSH.
11. Расторгуев С.П. Информационная война. М.: Радио и связь, 1999. – 416 с. URL: https://klex.ru/g5 (дата обращения: 02.06.2022).
12. Манойло А.В. Информационные войны и психологические операции. Руководство к действию. М.: Горячая линия – Телеком. 2022. – 496 с. URL: https://www.techbook.ru/book.php?id_book=1036 (дата обращения: 02.06.2022).
13. Бураева Л.А. Информационное противостояние как способ ведения информационных войн. Пробелы в российском законодательстве. 2018, № 3, с. 59–60. URL: https://www.elibrary.ru/item.asp?id=35102567 (дата обращения: 02.06.2022) – EDN XQNMZV.
14. Особенности ведения современных информационных войн в СМИ и сети Интернет. Мировая политика. 2017, № 4, с. 64–74. URL: https://www.elibrary.ru/item.asp?id=32490653 (дата обращения: 02.06.2022) – EDN YPXFWM.
15. Фролов Н.В. Социальные сети как инструмент ведения информационных войн. Социодинамика. 2018, № 8, с. 1–6. URL: https://www.elibrary.ru/item.asp?id=35427109 (дата обращения: 02.06.2022) – EDN XWFFSX.
16. Ремарчук В.Н., Бочарников И.В., Гушер А.И., Микрюков В.Ю., Зиновьева О.М., Солодухин Ю.Н., Белозеров В.К., Харичкин И.К., Манойло А.В., Овсянникова О.А., Герейханов Г.П., Винокуров В.И., Ружейников В.В., Люткене Г.В., Викулов С.Ф., Зеленков М.Ю. Эволюция форм, методов и инструментов противоборства в современных конфликтах. М.: Экон-Информ, 2015. – 218 с. URL: https://www.elibrary.ru/item.asp?id=25827347 (дата обращения: 02.06.2022) – EDN VTERIZ.
17. Орешко М.Н. Феномен «фейк» новостей в современной информационной войне. Инновационная наука. 2019, № 1, с. 140–142. URL: https://www.elibrary.ru/item.asp?id=36868166 (дата обращения: 02.06.2022) – EDN YVLDRB.
18. Белоножкин В.И., Остапенко Г.А. Информационные аспекты противодействия терроризму. М.: Горячая линия – Телеком, 2009. – 112 с. URL: https://www.elibrary.ru/item.asp?id=20577792 (дата обращения: 02.06.2022) – EDN RIHXFJ.
19. Манойло А.В. «Дело Скрипалей» как операция информационной войны. Вестник Московского государственного областного университета (электронный журнал). 2019, № 1, с. 72–97. DOI: http://dx.doi.org/10.18384/2224-0209-2019-1-939 (дата обращения: 02.06.2022) – EDN ZDHVKP.

REFERENCES:
[1] Rastorguev S.P. The philosophy of information warfare. M.: University book, MPSI, 2003. – 301 p. URL: https://klex.ru/pec (accessed: 02.06.2022) (in Russian).
[2] Laminina O.G. Information wars: myth or reality? Humanities Bulletin of Tula State Pedagogical University named after L.N. Tolstoy (online edition). 2018, no. 1(25), p. 17–23. URL: https://www.elibrary.ru/item.asp?id=35018244 (accessed: 02.06.2022) – EDN: UQKSYT (in Russian).
[3] Popova S.V., Fedorinov V.E. Goals and consequences of the information war. Aerospace forces. Theory and practice, 2018, no. 6(6), p. 15–21. URL: https://www.elibrary.ru/item.asp?id=35123455 (accessed: 02.06.2022) – EDN USAQKU (in Russian).
[4] Levin A.V. Features and types of information wars. Problems of Science. 2017, no. 32(114). URL: https://www.elibrary.ru/item.asp?id=30021833 (accessed: 02.06.2022) – EDN ZGZDYV (in Russian).
[5] Andrusova T.B., Gomonova Yu.G., Bagaeva A.P. Information weapons and information wars. Actual problems of aviation and cosmonautics. 2010, no. 6, p. 403–406. URL: https://www.elibrary.ru/item.asp?id=22634497 (accessed: 02.06.2022) – EDN TBIBVT (in Russian).
[6] Dobryshin M.M. Features of the use of information technology weapons in the conduct of modern hybrid wars. I-methods, 2020, vol. 12, no. 1, p. 1–11. URL: https://www.elibrary.ru/item.asp?id=42636560 (accessed: 02.06.2022) – EDN PPGYRU (in Russian).
[7] Musuralieva M.M. The concept and essence of information warfare. Izvestiya vuzov (Kyrgyzstan). 2015, no. 1. URL: https://www.elibrary.ru/item.asp?id=23931974 (accessed: 02.06.2022) – EDN UDSHHJ (in Russian).
[8] Kihtan V.V., Kachmazova Z.N. Information warfare: concept, content and main forms of manifestation. Bulletin of the V.N. Tatishchev Volga State University. 2018, vol. 2, no. 2. URL: https://www.elibrary.ru/item.asp?id=35138943 (accessed: 02.06.2022) – EDN USGUUQ (in Russian).
[9] Aisakhanova E.S. Information wars as a result of social management and social interaction in the era of globalization. Colloquium-journal. 2019, no. 23–3(47). DOI: http://dx.doi.org/10.24411/2520-6990-2019-10774. – EDN YMJZID (in Russian).
[10] Egorova L.S. The influence of information wars on the stability of the state. Communicologiya (Electronic journal). 2018, vol. 3, no. 2. URL: https://www.elibrary.ru/item.asp?id=35377852 (accessed: 02.06.2022) – EDN UVXYSH (in Russian).
[11] Rastorguev S.P. Information Warfare. M.: Radio and Communications, 1999. – 416 p. URL: https://klex.ru/g5 (accessed: 02.06.2022) (in Russian).
[12] Manoilo A.V. Information warfare and psychological operations. Guide to action. M.: Hotline – Telecom. 2022. – 496 p. URL: https://www.techbook.ru/book.php?id_book=1036 (accessed: 02.06.2022) (in Russian).
[13] Buraeva L.A. Information confrontation as a way of conducting information wars. Gaps in Russian Legislation. 2018, no. 3, p. 59–60. URL: https://www.elibrary.ru/item.asp?id=35102567 (accessed: 02.06.2022) – EDN XQNMZV (in Russian).
[14] Features of conducting modern information wars in the media and the Internet. World Politics. 2017, p. 64–74. no. 4. URL: https://www.elibrary.ru/item.asp?id=32490653 (accessed: 02.06.2022) – EDN YPXFWM (in Russian).
[15] Frolov N.V. Social networks as a tool for conducting information wars. Sociodynamics. 2018, no. 8, p. 1–6. URL: https://www.elibrary.ru/item.asp?id=35427109 (accessed: 02.06.2022) – EDN XWFFSX (in Russian).
[16] Remarchuk V.N., Bocharnikov I.V., Gusher A.I., Zinoveva O.M., Belozerov V.K., Kharichkin I.K., Manoilo A.V., Ovsyannikova O.A., Gereikhanov G.P., Vinokurov V.I., Vikulov S.F., Zelenkov M.YU. Evolution of forms, methods and tools of confrontation in modern conflicts, 2015. – 218 p. URL: https://www.elibrary.ru/item.asp?id=25827347 (accessed: 02.06.2022) (in Russian).
[17] Oreshko M.N. The phenomenon of "fake" news in the modern information war. Innovative Science. 2019, no. 1, p. 140–142. URL: https://www.elibrary.ru/item.asp?id=36868166 (accessed: 02.06.2022) – EDN YVLDRB (in Russian).
[18] Belonozhkin V.I., Ostapenko G.A. Information aspects of countering terrorism. M.: Hotline – Telecom, 2009. – 112 p. URL: https://www.elibrary.ru/item.asp?id=20577792 (accessed: 02.06.2022) – EDN RIHXFJ (in Russian).
[19] Manoilo A.V. "The Skripal case" as an information war operation. Bulletin of the Moscow State Regional University (electronic journal). 2019, no. 1, p. 72–97. DOI: http://dx.doi.org/10.18384/2224-0209-2019-1-939 (accessed: 02.06.2022) – EDN ZDHVKP (in Russian).

Поступила в редакцию – 02 июня 2022 г. Окончательный вариант – 27 августа 2022 г.
Received – June 02, 2022. The final version – August 27, 2022.

Александр С. Мосолов[1], Андрей Е. Краснов[2], Николай А. Урбан[3]
[1]Российский химико-технологический университет им. Д.И. Менделеева, Миусская пл., 9, Москва, 125047, Россия
[2,3]Российский государственный социальный университет, ул. Вильгельма Пика, 4, стр. 1, Москва,129226, Россия
[1]e-mail: asmosolov@yandex.ru, https://orcid.org/0000-0002-3266-9505
[2]e-mail: krasnovmgutu@yandex.ru, https://orcid.org/0000-0002-4075-4427
[3]e-mail: urbannikolai@mail.ru, https://orcid.org/0000-0002-8047-1499

О ПРИМЕНЕНИИ МЕТОДА АНАЛИЗА УЯЗВИМОСТЕЙ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА ПРОИЗВОДСТВЕННОГО ОБЪЕКТА ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АСУ ТП С УЧЁТОМ ВЗАИМОСВЯЗИ КОМПОНЕНТОВ

DOI: http://dx.doi.org/10.26583/bit.2022.3.03

Аннотация. Цель статьи – анализ уязвимости систем, обеспечивающих процессы жизнедеятельности объекта топливно-энергетического комплекса. Применение метода смещённого идеала, а также метода сокращённого анализа иерархий позволило найти наиболее уязвимые элементы технологических систем и выявить зависимость работоспособности этих элементов от защищённости информационных потоков в автоматизированных системах управления технологическими процессами. Показана необходимость формирования обоснованных требований к политике информационной безопасности предприятия и акцентирования внимания на обеспечение достаточного уровня защиты от угроз элементам информационной системы предприятия. Исполнение таких угроз может привести к последствиям, наносящих наибольший ущерб по критериям: зона чрезвычайной ситуации, экономический ущерб, количество пострадавших, вероятность отказа системы. Проведён анализ значимости угроз для информационных систем, и анализ устойчивости, как отдельных компонентов, так и их агрегатов. Показан характер взаимосвязанности (отношений) компонентов информационных систем предприятия. В рамках рассмотрения угроз для компонентов информационных систем выявлена иерархическая зависимость защищённости сложных активов информационной системы от защищённости базовых компонентов низшего уровня. Разработана модель угроз на основании утверждённого Федеральной службой по техническому и экспортному контролю перечня угроз в базе данных угроз информационной безопасности для информационных систем. Применение данного подхода позволяет сформировать положения для политики информационной безопасности предприятия и предложить специалистам по обеспечению информационной безопасности разработать меры программно-аппаратной защиты для информационной системы предприятия.

Ключевые слова: угроза, риск, устойчивость, политика информационной безопасности, технологические системы, критическая информационная инфраструктура, топливно-энергетический комплекс.
Для цитирования: МОСОЛОВ, Александр С.; КРАСНОВ, Андрей Е.; УРБАН, Николай А. О ПРИМЕНЕНИИ МЕТОДА АНАЛИЗА УЯЗВИМОСТЕЙ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА ПРОИЗВОДСТВЕННОГО ОБЪЕКТА ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АСУ ТП С УЧЁТОМ ВЗАИМОСВЯЗИ КОМПОНЕНТОВ. Безопасность информационных технологий, [S.l.], т. 29, № 3, с. 38–52, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1434. DOI: http://dx.doi.org/10.26583/bit.2022.3.03.

Alexander S. Mosolov[1], Andrey E. Krasnov[2], Nikolay A. Urban[3]
[1]D.I. Mendeleev University of Chemical Technology of Russia, Miusskaya square, 9, Moscow, 125047, Russia
[2,3]Russian State Social University, Wilhelm Pik str., 4, p. 1, Moscow,129226, Russia
[1]e-mail: asmosolov@yandex.ru, https://orcid.org/0000-0002-3266-9505

[2]*e-mail: krasnovmgutu@yandex.ru, https://orcid.org/0000-0002-4075-4427*
[3]*e-mail: urbannikolai@mail.ru, https://orcid.org/0000-0002-8047-1499*

On the application of the vulnerability analysis method of the technological process of the production facility to ensure the information security of the automated process control system, taking into account the interrelation of components

DOI: http://dx.doi.org/10.26583/bit.2022.3.03

Abstract. The purpose of the paper is to analyze the vulnerability of systems that ensure the processes of vital activity of an object of the fuel and energy complex. The application of the shifted ideal method, as well as the method of reduced hierarchy analysis, made it possible to find the most vulnerable elements of technological systems and to identify the dependence of the operability of these elements on the security of information flows in automated process control systems. The need in forming reasonable requirements for the information security policy of the enterprise and focusing on ensuring a sufficient level of protection against threats to the elements of the enterprise information system is demonstrated. The execution of such threats can lead to consequences that cause a huge damage according to the following criteria: the emergency zone, economic damage, the number of victims, the probability of system failure. The analysis of the significance of threats to information systems as well as the analysis of the stability of both individual components and their aggregates are carried out. The nature of the interconnectedness (relationships) of the components of information systems of the enterprise is shown. As part of the consideration of threats to the components of information systems, the hierarchical dependence of the security of complex assets of the information system on the security of the basic components of the lowest level is revealed. A threat model has been developed based on the list of threats approved by the Federal Service for Technical and Export Control in the database of information security threats for information systems. The application of this approach makes it possible to form provisions for the information security policy of the enterprise and to invite information security specialists to develop the software and hardware protection for the enterprise information system.

Keywords: threat, risk, stability, information security policy, technological systems, critical information infrastructure, fuel and energy complex.
For citation: MOSOLOV, Alexander S.; KRASNOV, Andrey E.; URBAN, Nikolay A. On the application of the vulnerability analysis method of the technological process of the production facility to ensure the information security of the automated process control system, taking into account the interrelation of components. IT Security (Russia), [S.l.], v. 29, no. 3, p. 38–52, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1434. DOI: http://dx.doi.org/10.26583/bit.2022.3.03.

Введение

Одной из важных составляющих безопасности объектов топливно-энергетического комплекса (ТЭК) является обеспечение его технологической безопасности. В соответствии с Федеральным законом № 256-ФЗ[1] защитные меры формируются на основании присвоенной объекту категории потенциальной опасности от акта незаконного вмешательства (АНВ) и установленных уровней защищенности его критическим элементам. В 75% из общего количества выполненных проектов по категорированию в качестве АНВ рассматривают угрозу «технического воздействия», включая информационное воздействие на информационную систему предприятия (АСУ ТП) [1], направленное на дестабилизацию функционирования объекта и нарушение технологических процессов [2].

Целью совершения АНВ является причинение ущерба населению, окружающей среде, объекту и, в целом, для государства. При этом категория определяется по

[1]Федеральный закон № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» от 21.07.2011 г.

наибольшему значению показателя одного из критериев категорирования: зона чрезвычайной ситуации, социальный и материальный (экономический) ущерб[1].

Новизна предлагаемого в настоящей статье подхода в том, что предлагается оценивать уязвимость производственно-технологического процесса по совокупности значений показателей множества критериев (включая, но не ограничиваясь критериями категорирования) для определения наиболее привлекательной комбинации отказов [3], к которой будет стремиться привести аварийную ситуацию потенциальный нарушитель. При этом возможно обнаружение уязвимых элементов как, собственно, в технологическом процессе, так и прогнозирование привлекательности наиболее уязвимых технологических блоков в инфраструктуре производственного цикла объекта [4].

Для борьбы с угрозами информационной безопасности применяют различные методики [5–6], самостоятельные программные решения и отдельные комплексы для контроля за параметрами информационной инфраструктуры предприятия [7–8], алгоритмы целевого анализа уязвимости производственно-технологических процессов опасных производственных и критически важных объектов [3].

В [9] рассмотрена система прогнозирования и оценки безопасности опасного производственного объекта с использованием комплексной модели обеспечения безопасности.

В [10] авторы рекомендуют при построении системы защиты от разрушительных программных воздействий (РПВ) использовать декомпозицию задачи выбора рационального варианта системы защиты, что связано с большим количеством ограничений и частных показателей, требующих учёта при проектировании, что, в свою очередь, ссылается на три функциональные категории системы защиты от РПВ – подсистему обнаружения РПВ, подсистему противодействия РПВ и подсистему устранения последствий РПВ.

В [11] отмечены достоинства применения методик и моделей по проектированию систем информационного обеспечения для решения задач технической защиты информации, рассмотрены методы поддержки выбора с расчетом эффективности проектируемой модели посредством факторного анализа. Данный анализ достигается с помощью подхода по применению правила Фишберна, подхода по анализу иерархий Т. Саати, подхода по применению мультипликативной функции Кобба-Дугласа.

В [12] рассмотрены практики по реализации политики безопасности на базе модели угроз информационной безопасности, выстраиваемой по определённой последовательности шагов, как следует из примера использования такой практики на примере предприятий.

1. Определение уязвимости производственно-технологического процесса

Вопросы обеспечения информационной безопасности в АСУ ТП не могут рассматриваться без учета самой природы химических и нефтехимических процессов на опасных производственных объектах (ОПО). Принцип равновероятностной защиты информационного периметра не применим, если существует вероятность потенциальной угрозы АНВ в отношении уязвимых элементов технологической схемы ОПО, для их определения которых применяют метод анализа и оценки риска последствий возможных комбинаций «отказов» по совокупности значений показателей существенно значимых критериев.

Число комбинаций определяется с помощью формулы числа сочетаний из n элементного множества наборами по k элементов:

$$C_n^k = \frac{n!}{(n-k)!*k!}. \quad (1)$$

«Вес» привлекательности комбинации «отказов» в [13] рассчитывают на базе принятых в [1] критериев с использованием методов экспертных оценок: методов полного и сокращенного анализа иерархий, метода многокритериальной комбинации («метода смещённого идеала»).

Для анализа рисков на опасных производственных объектах, к которым относят объекты топливно-энергетического комплекса, применяют модели и алгоритмы прогнозирования эффективности управлением промышленной безопасности и антитеррористической защищенностью таких объектов [14, 15].

Описанный в [13] метод направлен на повышение эффективности процесса категорирования объектов КИИ[2,3]; следует учитывать отсутствие в Указе Президента № 31с[4] таких необходимых операций, как определение критических сегментов в объекте критической информационной инфраструктуры, оценка риска отключения критического элемента, оценка эффективности АСУ ТП предприятия при реагировании на компьютерные атаки.

Разработанную в [13] модель можно использовать для определения критических сегментов в объекте КИИ; уязвимым элементам технологической схемы соответствуют активы и ресурсы объекта АСУ ТП, объединенные в критические сегменты. При этом сегментам или элементам критических информационных инфраструктур присваивают «категории значимости» объектов, а базы критериев значимости КИИ определены в Постановлении Правительства РФ № 127[5].

Степень защиты элемента технологической схемы должна быть не ниже установленных нормативов по обеспечению технологической безопасности[6], аналогичные положения применимы и к АСУ ТП.

Влияние информационных угроз на устойчивость объектов определяется методологией комплексного оценивания уязвимости КИИ и её критических элементов[7].

Информационные потоки данных наиболее уязвимы, и необходимо расширять спектр защитных механизмов, чтобы не допустить, в т.ч. утечки персональных данных[8].

Отнесение элементов объекта КИИ к критичным или некритичным возможно определить в результате анализа фрагмента информационной системы, используя значения показателя вероятности отказа элемента технологического процесса и вероятности его безотказной работы.

Одним из вариантов модели подобного подхода может быть формула (2) из [13]:

$$P = (p_{iотк} * p_{(i+n)отк} * \dots) * (p_{(i+n+k)б/отк} * \dots). \quad (2)$$

[2]Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017.

[3]Постановлением Правительства РФ от 24 декабря 2021 г. N 2431«О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. N 127».

[4]Указ Президента Российской Федерации от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». – 3 с.

[5]Постановление Правительства РФ № 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» от 8 февраля 2018 г.

[6]Федеральный закон № 116-ФЗ «О промышленной безопасности опасных производственных объектов» от 21.07.1997.

[7]Методика оценки угроз безопасности информации. ФСТЭК России 5 февраля 2021 года. URL: https://docs.cntd.ru/document/607699443 (дата обращения: 22.04.2022).

[8]Федеральный закон "О персональных данных" от 27.07.2006 № 152-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 22.04.2022).

Итоговое значение P будет являться показателем критичности фрагмента системы. Последовательная проверка фрагментов системы позволит определить наиболее уязвимый и привлекательный к АНВ актив системы.

С помощью данного метода может быть решена проблема анализа и оценки бесперебойной работы технического узла.

2. Анализ влияния рисков информационной безопасности на составляющие информационной системы субъекта КИИ

2.1 Уязвимости базовых элементов информационной системы

Для проведения анализа влияния рисков ИБ был применён подход, рассматривающий трёхуровневую иерархическую структуру отношений базовых составляющих информационной системы (ИС) [1].

Иерархическая структура отношений базовых активов ИС представлена иерархическим графом на рис. 1, где агрегат активов представлен в виде A_{12345} и включает взаимодействия между элементами A_1, A_2, A_3 (программное обеспечение BIOS A_1, загрузчики BIOS A_2, главные атрибуты (ключи) загрузчиков A_3), и элементами A_4, A_5 (загрузочные записи операционной системы A_4, системные и пользовательские данные A_5), связанными через их агрегаты – NVRAM-микросхему A_{123} и жёсткий диск A_{45}.

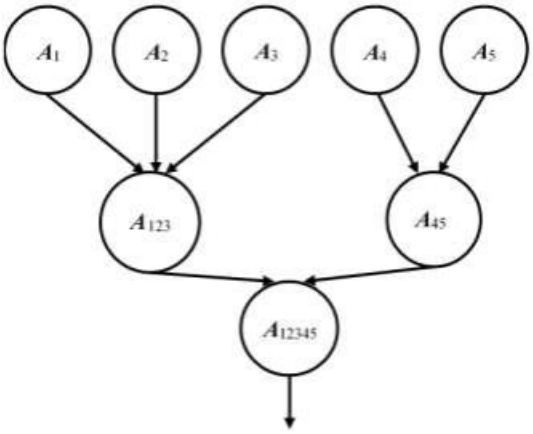

Рис. 1. Граф иерархических уровней связей составляющих ИС
Fig.1. Graph of hierarchical levels of connections of the components of the IC

2.1.1 Угрозы составляющим ИС. Возможность выбора угрозы методом экспертных оценок

Ниже приведены защитные меры от основных угроз (табл.1) согласно базе данных ФСТЭК России[9]:

Kaspersky Industrial CyberSecurity (KICS),

KICS for Nodes, KICS for Networks, Kaspersky Security Center.

KICS for Nodes.

KICS for Networks.

Kaspersky Security Center.

Для определения наиболее вероятных угроз в отношении элементов АСУ ТП среди сотрудников IT-отдела целесообразно провести экспертный опрос на предмет выявления наиболее уязвимого элемента, приоритетного для АНВ.

[9]Банк данных угроз безопасности информации [Информационный ресурс ФСТЭК].URL: https://bdu.fstec.ru/ (дата обращения: 22.04.2022).

Таблица 1. Основные угрозы составляющим ИС

Наименование угрозы
УБИ.004: Угроза аппаратного сброса пароля BIOS (Модификация авторизационной информации).
УБИ.005: Угроза внедрения вредоносного кода в BIOS.
УБИ.009: Угроза восстановления предыдущей уязвимой версии BIOS
УБИ.018: Угроза загрузки нештатной операционной системы
УБИ.032: Угроза использования поддельных цифровых подписей BIOS.
УБИ.057: Угроза неконтролируемого копирования данных внутри хранилища больших данных.
УБИ.060: Угроза неконтролируемого уничтожения информации хранилищем больших данных.
УБИ.067: Угроза неправомерного ознакомления с защищаемой информацией.
УБИ.088: Угроза несанкционированного копирования защищаемой информации.
УБИ.091: Угроза несанкционированного удаления защищаемой информации.
УБИ.144: Угроза программного сброса пароля BIOS
УБИ.154: Угроза установки уязвимых версий обновления программного обеспечения BIOS.

В качестве примера приведена табл. 2 с результатами опроса семи специалистов/экспертов, которые в качестве наиболее вероятной стратегии воздействия на АСУ ТП, с целью дестабилизации производственного процесса, выделили угрозы, которые окажут воздействие на базу данных параметров потока энергоносителя.

Таблица 2. Результаты экспертного опроса по выделению угрозы в отношении АСУ ТП

эксперт / угроза	1	2	3	4	5	6	7	Совокупная оценка
УБИ.004	5	1	3	6	4	10	2	4,43
УБИ.005	4	9	5	6	7	8	7	6,57
УБИ.009	4	5	6	7	16	8	7	7,57
УБИ.018	3	10	7	3	5	4	6	5,43
УБИ.032	1	9	8	7	6	10	5	6,57
УБИ.057	18	16	11	10	15	13	14	13,86
УБИ.060	12	9	11	9	4	7	9	8,71
УБИ.067	15	9	12	15	10	10	17	12,57
УБИ.088	14	10	10	11	20	13	15	13,29
УБИ.091	12	8	11	11	3	9	1	7,86
УБИ.144	6	6	10	8	4	7	10	7,29
УБИ.154	6	8	6	7	6	11	7	7,29

Данный выбор был обусловлен предоставленной информацией о наличии уязвимого элемента в производственном процессе, а именно, клапаном на подводящем трубопроводе.

По результатам опроса, в данном конкретном случае, эксперты выделили угрозы УБИ.057, УБИ.067, УБИ.088, поскольку соответствующие средние значения экспертных оценок существенно выше остальных.

На следующем этапе целесообразно для каждой угрозы определить приоритетное значение. Для этой цели рассматриваются возможные критерии, по которым определяются последствия для ИС и в целом объекта в случае реализации той или иной угрозы: УБИ.057, УБИ.067, УБИ.088. Выбор критериев обуславливается размером потенциальных рисков, анализ и оценка которых осуществляется специалистами, эксплуатирующими непосредственно АСУ ТП, производственно-технологические процессы и установки, представителями «Ростехнадзора» и МЧС. Основную угрозу определяем методами «Сокращенного анализа иерархий», «Полного анализа иерархий», «Смещенного идеала» с помощью программного комплекса [16]. Значения показателей критериев имеют разные единицы измерений, поэтому в каждом методе применяют формулы нормирования:

для метода «Полного анализа иерархий» –

$$S_i = \sum_i^j (B_{Sj} \cdot K_{ij}) \tag{3}$$

для метода «Сокращенного анализа иерархий» –

$$K_{ij} = \frac{K_{исх.ij}}{K_{сум.j}} \tag{4}$$

для метода «Смещенного идеала» –

$$d_j^i = \frac{k_j^i - k_j^-}{k_j^+ - k_j^-} \qquad L_i^p = \left[\sum_{j=1}^{m} (V_j d_j^i)^p\right]^{1/p}, \tag{5}$$

где $K_{исх,ij}$ – текущее нормированное значение показателя j-го критерия для i-ой угрозы,

$K_{сум,j}$ – сумма нормированных значений показателей i,

B_{sj} – показатель «важности» i-ой угрозы по отношению к j-му критерию,

S_i – сумма нормированных значений показателей j- того критерия по i-ой угрозе с учетом важности угрозы по отношению к критерию,

k^+ – максимальное нормированное значение по j-му критерию,

k^- – минимальное нормированное значение по j-му критерию.

Экспертные оценки формируются экспертами с учетом структуры АСУ ТП (рис. 2), поскольку уязвимость ресурсов и активов зависит от нижнего, среднего или верхнего уровня АСУ ТП.

Исследуя возможности воздействии на АСУ ТП объекта, в качестве потенциального нарушителя рассматривают начальника установки, который действует совместно с представителем соответствующей службы.

Динамика активности угроз зависит от субъекта, участвующего в технологическом информационном процессе, а время начала реализации угрозы ($t0$) может быть спрогнозировано.

Варианты атак на информационную систему предприятия, угрозы и защита от них представлены в табл. 3.

Рис. 2. Уровни АСУ ТП
Fig. 2. Automated control system levels

Таблица 3. Варианты атак, угроз и защитных мероприятий в АСУ ТП

Атаки	Угрозы	Защита
Внедрение вредоносного программного обеспечения	Получение доступа к системе АСУ ТП третьими лицами Нарушение в работе АСУ ТП	Антивирусная защита Управление доступом Идентификация и аутентификация
Компьютерная атака типа «отказ в обслуживании» (DoS, DDoS)	Полный отказ в обслуживании системы	Предотвращение вторжений Управление обновлениями программного обеспечения
Непреднамеренное отключение системы (без злого умысла)	Порча оборудования, удаление, искажение файлов с важной информацией или программ	Информирование и обучение персонала Обеспечение действий в нештатных ситуациях

Схема реагирования на события информационной безопасности представлена на рис. 3.

2.1.2 Построение модели значимости угроз

Меры реализации и меры уязвимости ***конфиденциальности***, ***целостности*** и ***доступности*** составляющих [17] (или активов A) ИС выстраиваются согласно представленной выше моделей оценки весов угроз (формулы 2–5) и схеме реагирования на события ИБ (рис. 3):

– $\mu_c(T|A_n)$ и $\mu_c(V|A_n)$ – мера (степень) реализации угрозы безопасности (security threat) и мера (степень) уязвимости (vulnerability) ***конфиденциальности*** актива A_n соответственно;

– $\mu_i(T|A_n)$ и $\mu_i(V|A_n)$ – мера (степень) реализации угрозы безопасности и мера (степень) уязвимости ***целостности*** актива A_n соответственно;

– $\mu_a(T|A_n)$ и $\mu_a(V|A_n)$ – мера (степень) реализации угрозы безопасности и мера (степень) уязвимости ***доступности*** актива A_n соответственно.

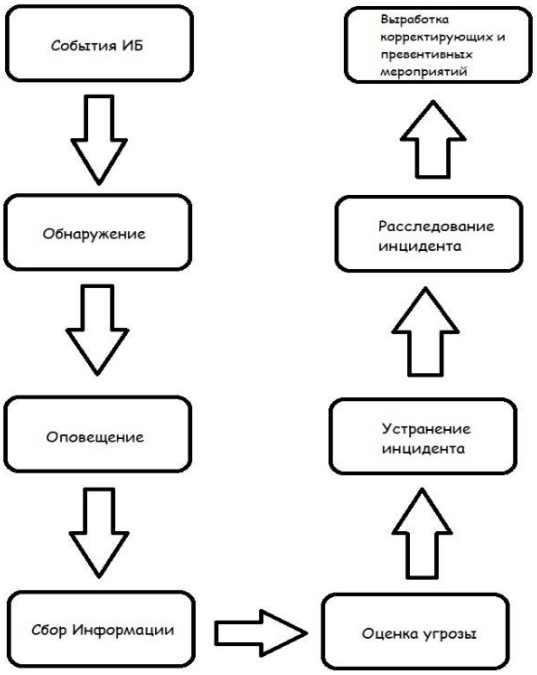

Рис. 3. Схема реагирования на события ИБ
Fig. 3. Response to information security events scheme

Значения всех мер μ задаются в интервале (0÷1). Зададим меры рисков (risk) конфиденциальности, целостности и доступности актива A_n (n = 1, 2, …, N) в виде нечеткого «И»:

$$\mu_c(R|A_n) = k_c(A_n)\ \mu_c(T|A_n)\ \mu_c(V|A_n);$$

$$\mu_i(R|A_n) = k_i(A_n)\ \mu i(T|A_n)\ \mu i(V|A_n);$$

$$\mu_a(R|A_n) = k_a(A_n)\ \mu_a(T|A_n)\ \mu_a(V|A_n); \quad (6)$$

$$k_c(A_n) = K_c(A_n)/[K_c(A_n) + K_i(A_n) + K_a(A_n)];$$

$$k_i(A_n) = K_i(A_n)\ /[K_c(A_n) + K_i(A_n) + K_a(A_n)];$$

$$k_a(A_n) = K_a(A_n)/[K_c(A_n) + K_i(A_n) + K_a(A_n)],$$

где $K_c(A_n)$, $K_i(A_n)$ и $K_a(A_n)$ – ненормированные степени значимости угроз конфиденциальности, целостности и доступности, а угрозы безопасности и уязвимости являются независимыми [1].

Вместо усредненного значения риска Rср(An) для каждого актива An (n = 1, 2, …, N) было рассчитано значение технического риска по выражению

$$Rcia(An) = Rc(An) + Ri(An) + Ra(An) - Rc(An) * Ri(An) - Rc(An) * Ra(An) - Ri(An) * Ra(An) + Rc(An) * Ri(An) * Ra(An). \quad (7)$$

Проведены расчёты по представленным формулам при ненормированных степенях значимости, представленных в 5-балльной системе (табл. 4).

Таблица 4. Значения мер для активов ИС

Номер актива	Актив 1	Актив 2	Актив 3	Актив 4	Актив 5
$K_c(A_n)$	1	3	3	4	5
$K_i(A_n)$	3	3	1	3	4
$K_a(A_n)$	4	2	4	2	1
$\mu_c(T/A_n)$	0,20	0,60	0,60	0,80	1
$\mu_i(T/A_n)$	0,60	0,60	0,20	0,60	0,80
$\mu_a(T/A_n)$	0,80	0,40	0,80	0,40	0,20
$\mu_c(V/A_n)$	0,80	0,40	0,40	0,20	1
$\mu_i(V/A_n)$	0,40	0,40	0,80	0,40	0,20
$\mu_a(V/A_n)$	0,20	0,60	0,20	0,60	0,80
$k_c(A_n)$	0,13	0,38	0,38	0,44	0,50
$k_i(A_n)$	0,38	0,38	0,13	0,33	0,40
$k_a(A_n)$	0,50	0,25	0,5	0,22	0,10
$\mu_c(R/A_n)$	0,02	0,09	0,09	0,07	0,50
$\mu_i(R/A_n)$	0,09	0,09	0,02	0,08	0,06
$\mu_a(R/A_n)$	0,08	0,06	0,08	0,05	0,02

2.2 Устойчивость компонентов информационной системы

2.2.1 Устойчивости элементарных компонентов информационной системы

Устойчивость/надежность элементарных компонентов или активов ИС к потере их конфиденциальности (c), целостности (i) и доступности (a) рассчитывалась при условии зависимости рисков друг от друга [1], причём расчёт значения риска для каждого актива применялся с использованием рекурсии:

$$\mu_{ci}(R|A_n) = \mu_c(R|A_n) + \mu_i(R|A_n) - \mu_c(R|A_n)\,\mu_i(R|A_n); \quad (8)$$
$$\mu_{cia}(R|A_n) = \mu_{ci}(R|A_n) + \mu_a(R|A_n) - \mu_{ci}(R|A_n)\,\mu_a(R|A_n).$$

Тогда из (5) получим выражение для расчета совокупной меры риска для каждого актива A_n:

$$\mu_{cia}(R|A_n) = \mu_c(A_n) + \mu_i(A_n) + \mu_a(A_n) - \mu_c(A_n)\,\mu_i(A_n) - \mu_c(A_n)\,\mu_a(A_n) - \mu_i(A_n)\,\mu_a(A_n) + \mu_c(A_n)\,\mu_i(A_n)\,\mu_a(A_n). \quad (9)$$

Устойчивости отдельных активов рассчитывались, как в [13]:

$$s_{cia}(A_n) = 1 - \mu_{cia}(R|A_n). \quad (10)$$

Согласно (10), получается набор совокупных мер риска активов приведенный в табл. 5.

Таблица 5. Устойчивость компонентов ИС к угрозам ИБ

№A	A_1	A_2	A_3	A_4	A_5
μ_{cia} (An)	0,18	0,22	0,18	0,19	0,54
$s_{cia}(A_n)$	0,82	0,78	0,82	0,81	0,46

2.2.2 Устойчивости агрегатов активов

Рассмотрим степени s устойчивости агрегатов ИС к угрозам на основе иерархических уровней их взаимодействия с помощью графа, представленного на рис. 4.

В работе [1] приведены различные методы оценки степеней устойчивости к угрозам агрегатов, которые применимы ко всем иерархическим уровням графа ИС.

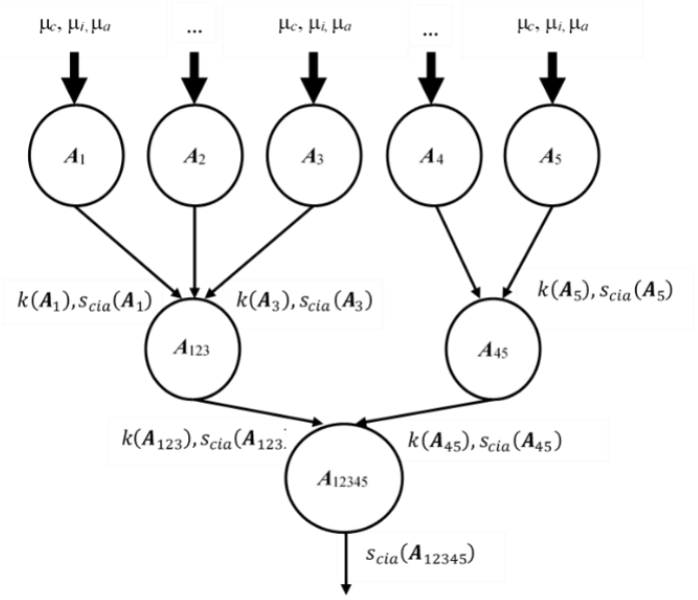

Рис. 4. Граф расчёта устойчивости агрегатов ИС
Fig. 4. Graph for calculating the stability of IC aggregates

Для расчёта по аналогии с (6) будем использовать нормированные коэффициенты $k(A_n) = K(A_n)/ \sum K(A_n)$ значимостей активов, где $K(A_n)$ – ненормированные коэффициенты их значимостей, а $n = 1, 2, \ldots, N$.

Рассмотрим устойчивость агрегатов при сильной зависимости компонентов. В связи с тем, что подсистема загрузки персонального компьютера является последовательной, успешность загрузки операционной системы в значительной мере зависит от состояния защищённости и функционирования BIOS материнской платы компьютера, а также состояния защищённости и функционирования жёсткого диска. Тем самым зависимость между данными компонентами будет сильной.

На формальном уровне сильное взаимодействие активов обусловлено их полной взаимозависимостью [1]. Определим степень устойчивости агрегатов при сильном взаимодействии их парных элементов, как:

$$s_{cia}(A_{12}) = \frac{k(A_1)k(A_2)s_{cia}(A_1)s_{cia}(A_2)}{k(A_1)+ k(A_2) - k(A_1)(A_2)}. \quad (11)$$

Тогда для агрегата A_{123} получим:

$$scia(A_{123}) = \frac{k(A_1)k(A_2)s_{cia}(A_1)s_{cia}(A_2)+ k(A_1)k(A_3)s_{cia}(A_1)s_{cia}(A_3)+ k(A_2)k(A_3)s_{cia}(A_2)s_{cia}(A_3)}{1- k(A_1)k(A_2)- k(A_1)k(A_3)-k(A_2)k(A_3)+ 2\,k(A_1)k(A_2)k(A_3)} - \frac{2\,k(A_1)k(A_2)k(A_3)s_{cia}(A_1)s_{cia}(A_2)s_{cia}(A_3)}{1- k(A_1)k(A_2)- k(A_1)k(A_3)-k(A_2)k(A_3)+ 2\,k(A_1)k(A_2)k(A_3)}. \quad (12)$$

Так, при $k(A_1) = k(A_2) = k(A_3)$ и $s_{cia}(A_1) = s_{cia}(A_2) = s_{cia}(A_3) = 1$, получим $s_{cia}(A_{123}) \cong 1$. При $s_{cia}\,(A_1) = 0$, $s_{cia}(A_2) = s_{cia}(A_3) = 1$ получим $s_{cia}\,(A_{123}) \cong 0.02$. Тем самым, выход из строя одного актива приводит к потере устойчивости агрегата.

Похожим образом обстоит ситуация и с агрегатом A_{45}. Степень его устойчивости определяется аналогично (8):

$$s_{cia}(A_{45}) = \frac{k(A_4)k(A_5)s_{cia}(A_4)s_{cia}(A_5)}{k(A_4)+ k(A_5)- k(A_4)k(A_5)}. \quad (13)$$

Так, при $k(A_4) = k(A_5)$ и $s_{cia}(A_4) = s_{cia}(A_5) = 1$, получим $s_{cia}(A_{45}) = 1$. При $s_{cia}(A_4) = 0$, $s_{cia}(A_5) = 1$, получим $s_{cia}(A_{45}) = 0$.

В связи с этим, можно утверждать, что выход из строя одного актива приводит к потере устойчивости агрегата, а выход из строя одного из агрегатов также приведёт к потере устойчивости всей системы в целом.

Так, действительно, при нарушении процедуры запуска операционной системы, по различным причинам, конечное состояние информационной системы будет зависеть от успешности разрешения возникших проблем от реализации угроз, направленных на нарушение работоспособности элемента информационной системы. Например, нарушение работоспособности терминала оператора, закреплённого за определённым элементом производственного процесса предприятия, или же сервера производственной сети, могут привести к различным результатам в зависимости от степени тяжести последствий атаки на конкретный элемент.

3. Обсуждение результатов

Из приведенного исследования следует, что наиболее подвержены риску взаимозависимые активы ИС, у которых потеря устойчивости одного из них приводит к потере устойчивости всех подсистем или агрегатов, состоящих их этих активов. Поэтому необходимо дублирование таких подсистем. В действительности, существующие меры по резервному копированию данных, в том числе, создание RAID-массивов, является прямым следствием применения таких мер. В последнее время и потребительские платформы стали оснащать дублируемыми микросхемами BIOS, с помощью которых можно восстановить исходный образ и настройки BIOS.

Персональный компьютер является довольно уязвимым элементом информационной среды, особенно, если у нарушителя есть непосредственный доступ к нему. Самые простые пути воздействия на ИС, при которых будет утрачена работоспособность ИС, включают воздействие на жёсткий диск, но защита программного обеспечения BIOS материнской платы позволяет ограничить доступ к жёсткому диску и его составляющим компонентам, а при отсутствии защиты энергонезависимого сегмента памяти и его главных функционирующих компонентов у злоумышленника будут открыты наиболее простые пути исполнения угроз по направлению к информационной системе в целом.

Поэтому важно всестороннее обеспечение защиты в соответствии со следующими рекомендациями, которые могут стать соответствующими положениями в политике информационной безопасности [18]:

– при работе с конфиденциальными данными шифровать жёсткие диски; это позволяет ограничить конечное время совершения атаки на ИС при допустимом времени реагирования на инциденты;

– для защиты содержимого жёстких дисков отключать дополнительные возможности по загрузке нештатных операционных систем и создать пароль BIOS для предотвращения изменения параметров состояния ПО микросхемы;

– при наличии возможности использовать собственноручно написанные сертификаты безопасности, встраиваемыми в энергонезависимую память BIOS, что

позволяет загружать только разрешённые системы и загрузчики, что позволит, в конечном счёте, оградиться от реализации угроз, направленных на ИС;

– проводить резервное копирование важных данных, а также дублировать элементы информационной системы с наиболее интенсивными потоками обмена информацией с другими элементами, от работоспособности которых зависит работа всей системы в целом.

Заключение

В настоящей статье предлагается оценивать уязвимость производственно-технологического процесса и обнаруживать уязвимые элементы обслуживаемых данные процессы информационных систем посредством анализа совокупности значений показателей критериев в границах требований Законодательства126.

Впервые для определения критических сегментов в объекте КИИ, в т.ч. для определения уязвимости базовых элементов АСУ ТП для обеспечения устойчивости объектов КИИ, в качестве критериев предлагается рассматривать меры уязвимости агрегатов, конфиденциальность, доступность, целостность.

Предложенная система оценки безопасности на опасных производственных объектах, при интеграции усилий специалистов-технологов и IT-специалистов по ее совершенствованию, позволит расширить возможности программного обеспечения, обеспечить устойчивость отдельных элементов АСУ ТП и усилить меры по обеспечению комплексной безопасности ОПО в целом.

СПИСОК ЛИТЕРАТУРЫ:

1. Краснов Андрей Е., Мосолов Александр С., Феоктистова Наталия А. Оценивание устойчивости критических информационных инфраструктур к угрозам информационной безопасности. Безопасность информационных технологий, [S.l.], т. 28, № 1, с. 106–120, 2021. ISSN 2074-7136. DOI: https://doi.org/10.26583/bit.2021.1.09. – EDN JMVYBG.
2. Глава 3. Информационно-экономическая безопасность как специфический элемент системы безопасности постиндустриального общества. 2016, с. 96–170. URL: https://www.elibrary.ru/item.asp?id=28962874 (дата обращения: 22.04.2022 г.) – EDN YJUQWX.
3. Губина Т.А., Мосолов А.С., Акинин Н.И. Алгоритм метода определения приоритетного сценария развития аварийной ситуации на объекте защиты. М.: Кокс и химия, 2019, № 6, с. 41–49. URL: https://www.elibrary.ru/item.asp?id=38220548 (дата обращения: 22.04.2022) – EDN EEOQRG.
4. Ковальский Ф.С., Мосолов А.С., Акинин Н.И. Анализ применения методов смещенного идеала и анализа иерархий при категорировании объекта топливно-энергетического комплекса. РХТУ им. Д.И. Менделеева. 2021, № 3, с. 15–20. URL: https://elibrary.ru/item.asp?id=45165274 (дата обращения: 22.04.2022). DOI: http://dx.doi.org/10.24000/0409-2961-2021-3-15-20 – EDN UFCAWP.
5. Захаров А.А., Римша А.С., Харченко А.М., Зулькарнеев И.Р. Анализ информационной безопасности автоматизированных систем управления техническими процессами газодобывающего предприятия. 2017, № 3(25), с. 24–33. URL: https://www.elibrary.ru/item.asp?id=30770417 (дата обращения: 22.04.2022) – EDN ZXJBRT.
6. Трещев И.А., Вильдяйкин Г.Ф., Ядыменко К.А. О подходе к анализу защищенности корпоративных информационных систем. ФГБОУ ВПО «Комсомольский-на-Амуре государственный технический университет». 2014, № 3, с. 41. URL: https://www.elibrary.ru/item.asp?id=23580615 (дата обращения: 22.04.2022) – EDN TWAJRH.
7. Чиликиди А.Г. «АСА ИБ». Свидетельство о государственной регистрации программы для ЭВМ RU 2020619745. Дата публикации 24.08.2020, бюл. № 9. URL: https://www1.fips.ru/ofpstorage/Doc/PrEVM/RUNWPR/000/002/020/619/745/2020619745-00001/document.pdf (дата обращения: 22.04.2022).
8. Чиликиди А.Г. «ГРИФОН». Свидетельство о государственной регистрации программы для ЭВМ RU 2021614176. Дата публикации 19.03.2021, бюл. № 3. URL: https://www1.fips.ru/ofpstorage/Doc/PrEVM/RUNWPR/000/002/021/614/176/2021614176-00001/document.pdf (дата обращения: 22.04.2022).

9. Ганченко П.В., Ибадулаев Д.В., Космичев В.П., Лузанов В.Ф., Обломский С.Б., Степанов И.В. Система прогнозирования и оценки безопасности опасного производственного объекта с использованием комплексной модели обеспечения безопасности. URL: https://elibrary.ru/item.asp?id=37814786 (дата обращения: 22.04.2022) – EDN IIPOID.
10. Дроботун Е.Б. Синтез систем защиты автоматизированных систем управления от разрушающих программных воздействий. Военная академия воздушно-космической обороны им. Маршала Советского Союза Г.К. Жукова. 2016, № 3, с. 51–59. URL: https://elibrary.ru/item.asp?id=27537411 (дата обращения: 22.04.2022) – EDN XEPQDX.
11. Соловьев С.В., Язов Ю.К. Информационное обеспечение деятельности по технической защите информации. Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю России, г. Воронеж, Россия. 2021, № 1 (41), с. 69–79. DOI: http://dx.doi.org/10.21681/2311-3456-2021-1-69-79.
12. Региональная информатика и информационная безопасность. Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления. Том. Выпуск 2. 2016. – 491 с. URL: https://elibrary.ru/item.asp?id=27552889 (дата обращения: 22.04.2022) – EDN XEYLCZ.
13. Губина Т.А., Мосолов А.С., Мосолов А.А. Система оценки безопасности опасного производственного объекта. RU №2709155 C1 от 02.04.2019. Опубликован 16.12.2019. Бюл. №35. МПК G06Q 10/06.
14. Тютин А.В. Организационно-методический аспект совершенствования подсистемы информационной безопасности объектов промышленного комплекса региона: автореф. дис. ... канд. экон. наук: 08.00.05. Иван. гос. ун-т. – Иваново, 2004. – 23 с. URL: https://viewer.rsl.ru/ru/rsl01002665244?page=16&rotate=0&theme=white (дата обращения: 22.04.2022).
15. Метод обработки экспертных оценок для оценки уязвимости производственно-технологического процесса, определяем основную угрозу. Свидетельство о государственной регистрации программы для ЭВМ RU 2021663111. Дата публикации 11.08.2021, бюл. № 9.
16. Кирсанов С.В. Метод оценки угроз информационной безопасности АСУ ТП газовой отрасли. Доклады ТУСУР. 2013, № 2 (28), с. 112–115. URL: https://cyberleninka.ru/article/n/metod-otsenki-ugroz-informatsionnoy-bezopasnosti-asu-tp-gazovoy-otrasli (дата обращения: 22.04.2022).
17. Дорофеев А.В., Марков А.С. Менеджмент информационной безопасности: основные концепции. Вопросы кибербезопасности. 2014, № 1(2). URL: https://cyberleninka.ru/article/n/menedzhment-informatsionnoy-bezopasnosti-osnovnye-kontseptsii (дата обращения: 22.04.2022).

REFERENCES:

[1] Krasnov Andrey E., Mosolov Alexander S., Feoktistova Nataliya A. Assessing the resilience of critical information infrastructures to information security threats. IT Security (Russia), [S.l.], vol. 28, no. 1, p. 106–120, 2021. ISSN 2074-7136. DOI: https://doi.org/10.26583/bit.2021.1.09. – EDN JMVYBG (in Russian).
[2] Chapter 3. Information and economic security as a specific element of the security system of post-industrial society. 2016, p. 96–170. URL: https://www.elibrary.ru/item.asp?id=28962874 (accessed: 22.04.2022) – EDN YJUQWX (in Russian).
[3] Gubina T.A., Mosolov A.S., Akinin N.I. Algorithm of the method for determining the priority scenario of the development of an emergency situation at the protection facility. 2019, no. 6, p. 41–49. URL: https://www.elibrary.ru/item.asp?id=38220548 (accessed: 22.04.2022) – EDN EEOQRG (in Russian).
[4] Kovalsky F.S., Mosolov A.S., Akinin N.I. Analysis of the application of methods of displaced ideal and hierarchy analysis in the categorization of the fuel and energy complex object. D.I. Mendeleev Russian Technical University. 2021, no. 3, p. 15–20. URL: https://elibrary.ru/item.asp?id=45165274 (accessed: 22.04.2022). DOI: http://dx.doi.org/10.24000/0409-2961-2021-3-15-20. – EDN UFCAWP (in Russian).
[5] Zakharov A.A., Rimsha A.S., Kharchenko A.M., Zulkarneev I.R. Analysis of information security of automated control systems for technical processes of a gas producing enterprise. 2017, no. 3(25), p. 24–33. URL: https://www.elibrary.ru/item.asp?id=30770417 (accessed: 22.04.2022) – EDN ZXJBRT (in Russian).
[6] Трещев И.А., Вильдяйкин Г.Ф., Ядыменко К.А. О подходе к анализу защищенности корпоративных информационных систем. ФГБОУ ВПО «Комсомольский-на-Амуре государственный технический университет». 2014, № 3, с. 41. URL: https://www.elibrary.ru/item.asp?id=23580615 (дата обращения: 22.04.2022) – EDN TWAJRH (in Russian).
[7] Chilikidi A.G. ASA IB. Certificate of state registration of a computer program. RU 2020619745. URL: https://www.elibrary.ru/item.asp?id=43965451 (accessed: 22.04.2022) (in Russian).
[8] Chilikidi A.G. GRIFON. Certificate of state registration of a computer program. RU 2021614176. URL: https://www.elibrary.ru/item.asp?id=45820045 (accessed: 22.04.2022) (in Russian).

[9] Ganchenko P.V., Ibadulaev D.V., Kosmichev V.P., Luzanov V.F., Oblomsky S.B., Stepanov I.V. The system of forecasting and assessing the safety of a hazardous production facility using an integrated safety model. URL: https://elibrary.ru/item.asp?id=37814786 (accessed: 22.04.2022) – EDN IIPOID (in Russian).

[10] Drobotun E.B. Synthesis of protection systems for automated control systems from destructive software influences. Military Academy of Aerospace Defense named after Marshal of the Soviet Union G.K. Zhukov. 2016, no. 3, p. 51–59. URL: https://elibrary.ru/item.asp?id=27537411 (accessed: 22.04.2022) – EDN XEPQDX (in Russian).

[11] Solovyov S.V., Yazov Y. K. Information support of activities on technical protection of information. State Research Testing Institute of Problems of Technical Protection of Information of the Federal Service for Technical and Export Control of Russia, Voronezh, Russia. 2021, no. 1 (41), p. 69–79. DOI: http://dx.doi.org/10.21681/2311-3456-2021-1-69-79 (in Russian).

[12] Regional informatics and information security. St. Petersburg Society of Informatics, Computer Technology, communication and Control Systems. Tom. Issue 2. 2016. – 491 p. URL: https://elibrary.ru/item.asp?id=27552889 (accessed: 22.04.2022) – EDN XEYLCZ (in Russian).

[13] Gubina T.A., Mosolov A.S., Mosolov A.A. Sistema otsenki besopastnosti opasnogo proisvodstvennogo ob''ekta [Safety assessment system for a hazardous production facility]. Patent RU 2709155 C1, 02.04.2019 (in Russian).

[14] Tyutin A.V. Organizational and methodological aspect of improving the subsystem of information security of objects of the industrial complex of the region: abstract. dis. ... Candidate of Economic Sciences: 08.00.05. Ivan. state. un-t. – Ivanovo, 2004. – 23 p. URL: https://viewer.rsl.ru/ru/rsl01002665244?page=16&rotate=0&theme=white (accessed: 22.04.2022) (in Russian).

[15] Method for processing expert assessments for assessing the vulnerability of the production and technological process, vulnerability assessment. Certificate of state registration of the computer program RU 2021663111, dated August 11, 2021 (in Russian).

[16] Kirsanov S.V. Method of assessing threats to information security of automated control systems of the gas industry. TUSUR reports. 2013, no. 2 (28), p. 112–115. URL: https://cyberleninka.ru/article/n/metod-otsenki-ugroz-informatsionnoy-bezopasnosti-asu-tp-gazovoy-otrasli (accessed: 22.04.2022) (in Russian).

[17] Dorofeev A.V., Markov A.S. Information security management: basic concepts. Issues of cybersecurity. 2014, no. 1(2). URL: https://cyberleninka.ru/article/n/menedzhment-informatsionnoy-bezopasnosti-osnovnye-kontseptsii (accessed: 22.04.2022) (in Russian).

Поступила в редакцию – 26 апреля 2022 г. Окончательный вариант – 28 августа 2022 г.
Received – April 26, 2022. The final version – August 28, 2022.

Никита И. Белов
Национальный исследовательский университет ИТМО,
Кронверкский пр., 49, Санкт-Петербург, 197101
e-mail: nikit.belov@gmail.com, https://orcid.org/0000-0003-0644-1547

МЕТОДЫ ЦЕЛОСТНОГО ПРЕОБРАЗОВАНИЯ ИЗОБРАЖЕНИЙ ПРИ АУТЕНТИФИКАЦИИ ЧЕЛОВЕКА ПО ТЕРМОГРАММЕ ЛИЦА

DOI: http://dx.doi.org/10.26583/bit.2022.3.04

Аннотация. **Цель работы.** Данное исследование проведено для изучения применимости методов целостного преобразования изображений к задаче аутентификации личности человека по термографическому изображению его лица. **Предмет исследования**. Данная работа включает исследование методов целостного преобразования изображений применительно к задаче аутентификации человека по термографическому снимку его лица. Собраны наборы данных изображений лиц в дальнем инфракрасном диапазоне (LWIR). Новизна исследования состоит в особенностях набора данных изображений, собранных в реальных условиях, оказывающих влияние на качество аутентификации, таких как мимика, ношение очков или медицинской маски, нанесение грима/косметики, различная освещенность и температурные условия окружающей среды, повороты головы. **Методы**. Исследуемые методы основаны на построении и выделении признаков изображения при сокращении размерности и преобразовании изображения в другую форму представления. Методы применяются при решении задачи выделения признаков на изображениях, при аутентификации по 2D-изображению лица и при решении других задач компьютерного зрения. В данной статье рассматриваются классические методы целостного преобразования изображений: анализ главных компонент, анализ главных компонент с применением ядра, анализ линейного дескриптора, анализ независимых компонент, усеченное сингулярное разложение, дискретное косинусное преобразование. В качестве меры близости изображений используется евклидово расстояние между векторами признаков изображения. **Основные результаты**. Тестирование методов было выполнено на наборе термограмм, состоящем из 632 тысяч изображений лиц 158 человек. В качестве метрики для оценки качества сопоставления выбранных методов использована F-мера. В результате проведенного эксперимента, метод анализа независимых компонент показал наиболее высокие значения метрики F-меры – 0,72. **Практическая значимость**. Результаты работы могут найти применения в системах управления и контроля доступом для повышения отказоустойчивости аутентификации лиц. Использование рассмотренных методов эффективно в задачах обработки термографических снимков для аутентификации человека по вторичным признакам, в частности по рисунку его вен и сосудов на лице, в случаях изменения мимики и внешности по средству нанесения грима и носимых аксессуаров.

Ключевые слова: компьютерное зрение, алгоритм аутентификации, термограмма лица, методы целостного преобразования, анализ главных компонент, анализ линейного дескриптора, анализ независимых компонент, усеченное сингулярное разложение, дискретное косинусное преобразование.

Для цитирования: БЕЛОВ, Никита И. МЕТОДЫ ЦЕЛОСТНОГО ПРЕОБРАЗОВАНИЯ ИЗОБРАЖЕНИЙ ПРИ АУТЕНТИФИКАЦИИ ЧЕЛОВЕКА ПО ТЕРМОГРАММЕ ЛИЦА. Безопасность информационных технологий, [S.l.], т. 29, № 3, с. 53–61, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1432. DOI: http://dx.doi.org/10.26583/bit.2022.3.04.

Nikita I. Belov
National Research University ITMO,
Kronverksky Ave., 49, Saint Petersburg, 197101
e-mail: nikit.belov@gmail.com, https://orcid.org/0000-0003-0644-1547

Methods of image transformation for person authentication using face thermographic image

DOI: http://dx.doi.org/10.26583/bit.2022.3.04

Abstract. The purpose of the paper is to study the holistic image transformation methods for person's identity authentication from a thermographic image of faces. Within this study the datasets of images of faces in the far infrared range (LWIR) have been collected. The novelty of the study consists in the features of the dataset of images which collected in real conditions that affect the quality of authentication, such as facial expressions, wearing glasses or a medical mask, applying makeup / cosmetics, different illumination and temperature conditions of the environment, head turns. The methods under the study are based on the construction and selection of image features while reducing the dimension and converting the image into another form of representation. These methods are used to solve the problem of distinguishing features in images, in authentication person identity by 2D image of his face and allows solving other computer vision problems. This paper discusses classical methods of integral image transformation: principal component analysis, principal component analysis using a kernel, linear descriptor analysis, independent component analysis, truncated singular value decomposition, discrete cosine transformation. As a measure of the proximity of images, the Euclidean distance between the vectors of image features is used. Testing of the methods was performed on a set of thermograms consisting of 632 thousand images of the faces of 158 people. The F-measure was used as a metric to assess the quality of comparison of the selected methods. As a result of the experiment, the independent component analysis method showed the highest values of the F-measure metric – 0.72. The results of the study can find applications in access control and control systems to increase the fault tolerance of authentication of persons. The use of the considered methods is effective in the tasks of processing thermographic images for authenticating a person by secondary signs, by the pattern of his veins and vessels on the face, in cases of changes in facial expressions and appearance by means of applying makeup and wearable accessories.

Keywords: computer vision, authentication algorithm, face thermogram, holistic transformation methods, principal component analysis, linear descriptor analysis, independent component analysis, truncated singular value decomposition, discrete cosine transformation.

For citation: BELOV, Nikita I. Methods of image transformation for person authentication using face thermographic image. IT Security (Russia), [S.l.], v. 29, no. 3, p. 53–61, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1432. DOI: http://dx.doi.org/10.26583/bit.2022.3.04.

Введение

В настоящее время алгоритмы распознавания лиц [1] широко используются в различных системах: как в мобильных устройствах, так и в системах принятия платежей. Существует большое количество методов (методы на основе нейросетевых архитектур, методы целостного преобразования изображения, статистические методы, методы выделения локальных признаков на изображении), применяющихся для задачи аутентификации личности человека, демонстрирующие высокое качество распознавания и аутентификации на основе 2D изображений лиц [2]. Также растет и количество способов обхода таких алгоритмов, в частности, данные методы уязвимы перед изменениями условий снятия снимка лица человека, такими как освещение, изменение мимики, внешности, ракурса съемки. В связи с этим необходимо рассмотреть иные способы установления личности человека, устойчивые к подобным воздействиям. Методами, замещающих или дополняющих данные алгоритмы, могут стать методы на основе аутентификации человека по изображению его лица на изображении в дальнем инфракрасном диапазоне (Long-Wavelength Infrared Specter, LWIR).

Снимки в LWIR диапазоне являются уникальными для каждого отдельного человека. Используя аппаратуру с высоким разрешением в целях получения термограмм, возможно увидеть сети сосудов и вен на лице человека [3].

Цель данной работы – исследование классических методов целостного преобразования изображений в задаче аутентификации человека применительно к снимкам лица в LWIR диапазоне (8–14 мкм) с учетом изменчивости условий снятия снимка и внешности персон.

1. Сбор выборки для проведения эксперимента

Сбор данных для формирования выборки производился с помощью тепловизора Seek Thermal Compact Pro. Характеристики устройства указаны в табл. 1.

Таблица 1. Характеристики тепловизора для сбора и анализа данных

Характеристика	Показатель
Температурный диапазон	от –40°C до +330 °C
Угол обзора	32°
Разрешение	320 x 240 px
Дальность видимости	до 550 м
Фокус	регулируемый
Частота обновления кадров	9 Гц

При подготовке были собраны короткие видеофрагменты по 20–40 с изображений лиц 158 человек выполняющих вращательные движения головой, к ним были добавлены видеоролики, где те же люди изображены после нанесения средств маскировки лица (грим, косметика), видеофрагменты с использованием носимых аксессуаров (очки, медицинские маски), видеофрагменты с охлаждением внешних тканей лица и их нагревом, видеофрагменты с изменением мимики, а также видеофрагменты с нанесением накладных усов, бороды.

В табл. 2 приведено сравнение наборов данных термографических снимков из открытых источников и собранных в данном исследовании. Недостатком известных исследований является сложность их практического применения в реальных условиях, так как внешность людей изменчива, как и условия окружающей среды (смена времен года, смена времени суток и др.). Также в исследованиях использовалось малое количество персон в выборке, что понижает вариативность уникальных признаков и искусственно повышает качество работы алгоритмов аутентификации. В настоящей работе, собранная выборка состоит из двух типов изображений: снимков лиц людей и термограмм в LWIR-диапазоне.

На следующем шаге видеофрагменты были нарезаны на кадры и проведена предварительная обработка (нормализация изображений) данных для дальнейшей передачи данных по одному из алгоритмов целостного преобразования изображения. Пример изображений из собранных данных представлен на рис. 1.

Таблица 2. Сравнительная характеристика наборов данных из открытых источников и собранного набора данных

Условия	Набор данных				
	Equinox database [4, 5]	RGB-DT face dataset [6]	NIST database [7]	University of Notre Dame [8]	Собранные данные
Количество изображений	14 560	45 900	25 000	2 293	632 000
Количество человек в наборе данных	91	51	91	82	158
Тип изображений	LWIR	LWIR	Фото и LWIR	LWIR	Фото и LWIR
Движение головы	+	+	–	–	+
Выражение лица (улыбка, грусть, спокойствие)	+	+	+	+	+
Изменение освещения	+	–	–	–	+
Изменение внешности (очки)	+	+	+	+	+
Изменение внешности (грим/косметика)	–	–	–	–	+
Изменение внешности (усы/борода)	–	–	–	–	+
Изменение внешности (ношение медицинской маски)	–	–	–	–	+
Изменение температуры окружающей среды	–	–	–	–	+

Рис. 1. Пример изображений из собранной выборки
Fig. 1. Thermal image example from the data set

2. Методы целостного преобразования изображения

В статье рассматриваются методы целостного преобразования изображения, которые широко применяются в задачах аутентификации человека в задаче аутентификации по 2D изображению лица человека. Данные методы базируются в первую очередь на идее аппроксимации данных и нахождения их проекции в пространстве. В частности, ряд ниже приведенных методов используется для выделения признаков изображения и сокращения их размерности, для дальнейшего сопоставления полученных векторов признаков изображения применяется меры расстояний или классификационные алгоритмы.

По данной тематике существует ряд работ зарубежных исследователей, где представлена оценка методов целостного преобразования изображений для термографических снимков: анализ главных компонент (Principal Component Analysis, PCA), анализ главных компонент с применением ядра (Kernel Principal Component Analysis, Kernel PCA), анализ линейного дескриптора (Linear Descript Analysis, LDA), анализ независимых компонент (Independend Component Analysis, ICA), усеченное сингулярное разложение (Truncated Singular Value Decomposition, T-SVD) и дискретное косинусное преобразование (Discrete Cosine Transform, DCT) [9]. Приведенные оценки не подходят для применения к выборкам обучения и тестирования моделей по количеству термограмм и по качественным характеристикам.

Алгоритм анализа главных компонент с применением ядра или Kernel PCA, является расширением базового метода PCA. Один из главных недостатков оригинального алгоритма в том, что он использует линейное разложение и испытывает трудности при преобразовании изображений, имеющих сложные нелинейные структуры [10]. Принцип его работы, это повышение размерности исходного изображения, для выделения в пространстве более высоких размерностей векторов, описывающих исходное изображение более полно.

Метод анализа линейного дескриптора LDA, также очень похож на метод анализа главных компонент PCA. Его основная идея схожа, требуется преобразовать изображение в одномерный вектор и уменьшить размерность исходного пространства. Кроме того, в данном методе учитывается класс, к которому принадлежит пиксель (2 класса: лицо или не лицо) [11].

Анализ независимых компонент ICA – метод, основанный на гипотезе о том, что объекты в рассматриваемом пространстве статистически независимы друг от друга. Данный метод позволяет выявить скрытые признаки на изображении путем понижения размерности [12].

Метод дискретного косинусного преобразования (DCT) является аналогом дискретного преобразования Фурье, преобразуя входное изображение из пространственной в частотную область [13].

Метод усеченного сингулярного разложения (T-SVD) имеет одно очень весомое преимущество перед рассмотренными ранее методами [14]. В отличие от них данный алгоритм не используется нормализацию изображения и хорошо работает с разряженными матрицами, не преобразуя их дополнительно.

3. Эксперимент

Алгоритмы, используемые в данной работе, успешно применяются в задачах аутентификации человека по 2D изображению [2]. Был проведен эксперимент по изучению возможности аутентификации людей по изображению их лица в LWIR

диапазоне применяя рассматриваемые методы. Блок схема проведения эксперимента представлена на рис. 2.

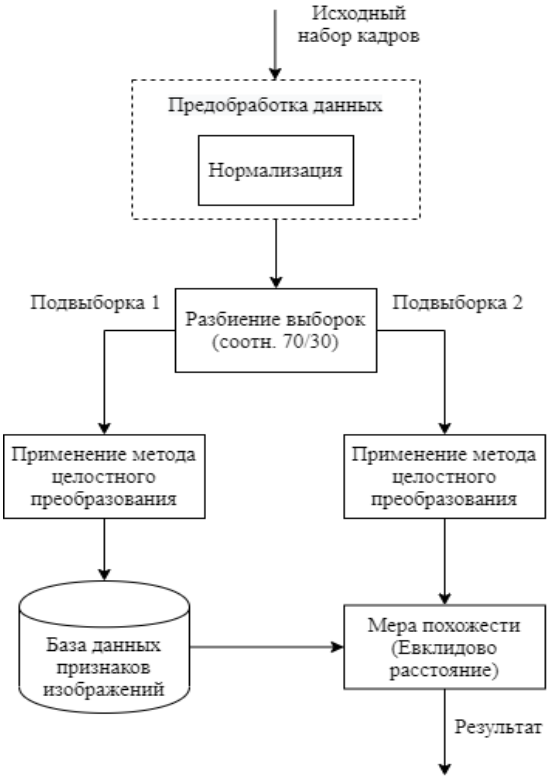

Рис. 2. Блок-схема проведения эксперимента
Fig. 2. Block diagram of the experiment

Первостепенно исходные данные предварительно обрабатывались методом минмакс нормализации (X_{norm})

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}},$$

где X – тензор изображения, X_{min} – минимальное значения пикселя на изображении, X_{max} – максимальное значения пикселя на изображении.

Далее, данные были разделены на 2 подвыборки: первая используется для создания базы данных векторов признаков изображений для каждого человека, вторая для проверки качества работы алгоритма. Таким образом после получения значений векторов, соответствующих каждому человеку из подвыборки 1, данные заносились в базу данных для дальнейшего сопоставления.

На последнем этапе проводится операция сопоставления векторов полученных в ходе использования методов целостного преобразования изображения над изображениями в подвыборке 2 и изображений векторов признаков изображений хранящихся в базе данных, с помощью меры расстояния, в данном случае Евклидова расстояния (d)

$$d(x,y) = \sqrt{\sum_{k=1}^{n} (x_k - y_k)^2},$$

где x и y – координаты вектора в пространстве.

После выполнения всех этапов преобразования термограмм в векторное представление, по средству использования методов целостного преобразования, по результатам сопоставления меры похожести опытным путем было выбрано пороговое значение равное 0.4. Результаты работы алгоритмов приведены в табл. 3 и были рассчитаны по метрике точности F-мера (F_β)

$$F_\beta = (1 + \beta^2)\ \frac{\text{precision} \cdot \text{recall}}{(\beta^2 \cdot \text{precision}) + \text{recall}},$$

где β – вес точности метрики (принимает значение в диапазоне $0 < \beta < \infty$), в нашем случае $\beta = 1$. Так как, при $\beta = 1$ значение метрики является сбалансированным между полнотой (recall) и точностью (precision).

Для расчета метрики точности F-мера первоначально на основе матрицы ошибок рассчитывается полнота (recall) и точность (precision)

$$\text{recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}, \quad \text{precision} = \frac{\text{TP}}{\text{TP} + \text{FP}},$$

где TP – истинно положительные срабатывания системы, TN – истинно отрицательные срабатывания системы, FN – ложно отрицательные срабатывания системы, FP – ложно положительные срабатывания системы.

Таблица 3. Результаты работы алгоритмов распознавания

Метод преобразования изображения	Значение метрики F-мера
PCA	0.34
Kernel PCA	0.45
LDA	0.48
ICA	0.72
T-SVD	0.56
DCT	0.56

Классический алгоритм PCA, LDA и Kernel PCA обладают худшими показателями F-меры среди рассмотренных, значение F-меры не превышает 0,5. Методы DCT и T-SVD с задачей выделения признаков лица справились на одном уровне и имеют одинаковое значение точности 0,56. Отметим, что в ходе проведения эксперимента, метод ICA показал лучшие результаты относительно остальных методов для термограмм лица человека при сопоставлении векторов признаков, значение F-меры для данного метода составляет 0.72. Данный метод, также демонстрирует лучшие показатели точности по сравнению с методами выделения локальных признаков с изображения [15].

Заключение

В данной работе были исследованы шесть алгоритмов целостного преобразования изображений применительно к задаче аутентификации человека по термографическому снимку лица. Для проведения эксперимента был собран набор данных, состоящий из 632 000 изображений лиц 158 человек, максимально приближенный к реальным условиям эксплуатации подобных систем.

Полученные результаты в ходе эксперимента показали, что в задаче аутентификации по термограмме лица человека метод анализа независимых компонент ICA показал наилучший результат – значение метрики F-мера=0.72.

Также на основе полученных результатов, необходимо отметить, что оригинальные методы целостного преобразования изображений, в целом, не лучшим образом справляются с задачей, однако различные вариации и расширения классических методов, могут существенно повысить значения метрики точности и улучшить процесс аутентификации по термограмме лица человека.

В дальнейших работах планируется рассмотреть марковские модели распознавания лиц и методы на основе нейросетевых архитектур и сравнить их с методами целостного преобразования изображения и методами выделения локальных признаков.

СПИСОК ЛИТЕРАТУРЫ:

1. Zhao W., Chellappa R., Phillips P.J. and Rosenfeld A. Face recognition: A literature survey. ACM Comput. Surv. 2003, vol. 35, issue 4, p. 399–458. DOI: https://doi.org/10.1145/954339.954342.
2. Кузнецов Д.А., Дамм В.А., Кузнецов А.В., Трегубов Р.Б. Сравнительный анализ популярных методов распознавания лиц на изображениях. Научный результат. Информационные технологии. 2019, № 4, с. 3–9. URL: https://cyberleninka.ru/article/n/sravnitelnyy-analiz-populyarnyh-metodov-raspoznavaniya-lits-na-izobrazheniyah (дата обращения: 25.07.2022).
3. Jain A.K., Ross A. and Prabhakar S. An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology. 2004, vol. 14, no. 1, p. 4–20. DOI: https://doi.org/10.1109/TCSVT.2003.818349.
4. Bendada A. and Akhloufi M.A. Multispectral Face Recognition in Texture Space. Canadian Conference on Computer and Robot Vision. 2010, p. 101–106. DOI: https://doi.org/10.1109/CRV.2010.20.
5. Méndez, H., Martín, C.S., Kittler, J., Plasencia, Y., García-Reyes, E. (2009). Face Recognition with LWIR Imagery Using Local Binary Patterns. In: Tistarelli, M., Nixon, M.S. (eds) Advances in Biometrics. ICB 2009. Lecture Notes in Computer Science, vol 5558. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-642-01793-3_34.
6. Nikisins O., Nasrollahi K., Greitans M. and Moeslund T.B. RGB-D-T Based Face Recognition. 22nd International Conference on Pattern Recognition. 2014, p. 1716–1721. DOI: https://doi.org/10.1109/ICPR.2014.302.
7. Bebis George et al. Face recognition by fusing thermal infrared and visible imagery. Image and Vision Computing 24.7 (2006): p. 727–742. DOI: https://doi.org/10.1016/j.imavis.2006.01.017.
8. Palm R.B. Prediction as a candidate for learning deep hierarchical models of data. 2012. URL: http://www2.imm.dtu.dk/pubdb/views/publication_details.php?id=6284 (дата обращения: 06.08.2022)
9. Kaur R. and Himanshi E. Face recognition using Principal Component Analysis. IEEE International Advance Computing Conference (IACC). 2015, p. 585–589. DOI: https://doi.org/10.1109/IADCC.2015.7154774.
10. Huang G.H., Shao H.H. Kernel Principal Component Analysis and Application in Face Recognition. Computer Engineering, Shanghai, 2004. URL: https://www.semanticscholar.org/paper/Kernel-Principal-Component-Analysis-and-Application-Hui-he/61221c884c40f2176c61f5b303222bd0a65b425b (дата обращения: 06.08.2022).
11. Xiaogang wang and Xiaoou Tang: Random Sampling for Subspace Face Recognition. International Journal of Computer Vision 70, p. 91–104, 2006. URL: https://mmlab.ie.cuhk.edu.hk/pdf/wangTijcv06.pdf (дата обращения: 10.08.2022).
12. Turk M.A. and Pentland A.P. Face recognition using eigenfaces Proceedings. IEEE Computer Society Conference on Computer Vision and Pattern Recognition. 1991, p. 586–591. DOI: https://doi.org/10.1109/CVPR.1991.139758.
13. Loeffler C., Ligtenberg A. and Moschytz G.S. Practical fast 1-D DCT algorithms with 11 multiplications. International Conference on Acoustics, Speech, and Signal Processing. 1989, vol. 2, p. 988–991. DOI: https://doi.org/10.1109/ICASSP.1989.266596.
14. Ahmed N., Natarajan T. and Rao K.R. Discrete Cosine Transform. IEEE Transactions on Computers. 1974, vol. C-23, no. 1, p. 90-93. DOI: https://doi.org/10.1109/T-C.1974.223784.
15. Белов Н.И., Ермак М.А., Дубинич Е.А., Кузнецов А.Ю. Методы выделения локальных признаков лица на изображении при аутентификации человека по термограмме. Научно-технический вестник информационных технологий, механики и оптики. 2022, т. 22, № 2(138), с. 279–286. DOI: https://doi.org/10.17586/2226-1494-2022-22-2-279-286. – EDN JFLCZJ.

REFERENCES:

[1] Zhao W., Chellappa R., Phillips P.J. and Rosenfeld A. Face recognition: A literature survey. ACM Comput. Surv. 2003, vol. 35, issue 4, p. 399–458. DOI: https://doi.org/10.1145/954339.954342.

[2] Kuznetsov D.A., Damm V.A., Kuznetsov A.V., Tregubov R.B. Popular methods of face images recognition comparative analysis of. Nauchniy resultat. Informacionnie technologii. 2019. № 4, p. 3–9. URL: https://cyberleninka.ru/article/n/sravnitelnyy-analiz-populyarnyh-metodov-raspoznavaniya-lits-na-izobrazheniyah (accessed: 25.07.2022) (in Russian).

[3] Jain A.K., Ross A. and Prabhakar S. An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology. 2004, vol. 14, no. 1, p. 4–20. DOI: https://doi.org/10.1109/TCSVT.2003.818349.

[4] Bendada A. and Akhloufi M.A. Multispectral Face Recognition in Texture Space. Canadian Conference on Computer and Robot Vision. 2010, p. 101–106. DOI: https://doi.org/10.1109/CRV.2010.20.

[5] Méndez, H., Martín, C.S., Kittler, J., Plasencia, Y., García-Reyes, E. (2009). Face Recognition with LWIR Imagery Using Local Binary Patterns. In: Tistarelli, M., Nixon, M.S. (eds) Advances in Biometrics. ICB 2009. Lecture Notes in Computer Science, vol 5558. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-642-01793-3_34.

[6] Nikisins O., Nasrollahi K., Greitans M. and Moeslund T.B. RGB-D-T Based Face Recognition. 22nd International Conference on Pattern Recognition. 2014, p. 1716–1721. DOI: https://doi.org/10.1109/ICPR.2014.302.

[7] Bebis George et al. Face recognition by fusing thermal infrared and visible imagery. Image and Vision Computing 24.7 (2006): p. 727–742. DOI: https://doi.org/10.1016/j.imavis.2006.01.017.

[8] Huang G.H., Shao H.H. Kernel Principal Component Analysis and Application in Face Recognition. Computer Engineering, Shanghai, 2004. URL: https://www.semanticscholar.org/paper/Kernel-Principal-Component-Analysis-and-Application-Hui-he/61221c884c40f2176c61f5b303222bd0a65b425b (accessed: 06.08.2022).

[9] Xiaogang wang and Xiaoou Tang: Random Sampling for Subspace Face Recognition. International Journal of Computer Vision 70, p. 91–104, 2006. URL: https://mmlab.ie.cuhk.edu.hk/pdf/wangTijcv06.pdf (accessed: 10.08.2022).

[10] Kaur R. and Himanshi E. Face recognition using Principal Component Analysis. IEEE International Advance Computing Conference (IACC). 2015, p. 585–589. DOI: https://doi.org/10.1109/IADCC.2015.7154774.

[11] Turk M.A. and Pentland A.P. Face recognition using eigenfaces Proceedings. IEEE Computer Society Conference on Computer Vision and Pattern Recognition. 1991, p. 586–591. DOI: https://doi.org/10.1109/CVPR.1991.139758.

[12] Loeffler C., Ligtenberg A. and Moschytz G.S. Practical fast 1-D DCT algorithms with 11 multiplications. International Conference on Acoustics, Speech, and Signal Processing. 1989, vol. 2, p. 988–991. DOI: https://doi.org/10.1109/ICASSP.1989.266596.

[13] Ahmed N., Natarajan T. and Rao K.R. Discrete Cosine Transform. IEEE Transactions on Computers. 1974, vol. C-23, no. 1, p. 90-93. DOI: https://doi.org/10.1109/T-C.1974.223784.

[14] Belov N.I., Ermak M.A., Dubinich E.A., Kuznetsov A.Ю. Methods of local features extraction in person authentication task by face thermographic imageю Scientific and Technical Journal of Information Technologies, Mechanics and Optics. 2022, vol. 22, no. 2(138), p. 279–286. DOI: https://doi.org/10.17586/2226-1494-2022-22-2-279-286. – EDN JFLCZJ (in Russian).

Поступила в редакцию – 17 августа 2022 г. Окончательный вариант – 30 августа 2022 г.
Received – August 17, 2022. The final version – August 30, 2022.

Михаил А. Куприяшин[1], Регина Ф. Баязитова[2]
[1,2]*Национальный исследовательский ядерный университет «МИФИ»,*
Каширское ш., 31, Москва, 115409, Россия
[1]*e-mail: rfbayazitova@mail.ru, https://orcid.org/0000-0003-0012-9309*
[2]*e-mail: kmickle@yandex.ru, https://orcid.org/0000-0001-6887-4810*

СОКРЫТИЕ ДАННЫХ В БЛОКАХ ORACLE DATABASE

DOI: http://dx.doi.org/10.26583/bit.2022.3.05

Аннотация. Данная статья посвящена рассмотрению возможности сокрытия сообщения в структуре системы управления базами данных (СУБД) Oracle Database. В качестве контейнера для хранения секретного сообщения используются блоки данных: физические структуры, выделяемые СУБД для хранения данных таблиц и других объектов. В работе рассматривается возможность заполнения таблиц таким образом, чтобы характер фрагментации свободного места являлся носителем информации о секретном сообщении. В частности, фрагменты свободного места соответствуют нулевым битам сообщения, а заполненные фрагменты – единичным. Для формирования контейнера необходимы привилегии на чтение, удаление и добавление новых записей в таблицу. Для извлечения сообщения достаточно права на чтение таблицы. В работе исследуется методика встраивания сообщения, обсуждаются особенности применения методики. Отмечается, что операции удаления и последующего добавления строк приводят к повреждению стеганоконтейнера. Рассмотрены базы данных типов OLAP и OLTP. Подчёркивается, что базы данных, основанные на модели OLAP, существенно лучше подходят для встраивания секретных сообщений описанного вида из-за небольшого числа вышеуказанных операций.
Ключевые слова: стеганография, сокрытие данных, базы данных, системы управления базами данных, Oracle Database.
Для цитирования: КУПРИЯШИН, Михаил А.; БАЯЗИТОВА, Регина Ф. СОКРЫТИЕ ДАННЫХ В БЛОКАХ ORACLE DATABASE. Безопасность информационных технологий, [S.l.], т. 29, № 3, с. 62–71, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1433. DOI: http://dx.doi.org/10.26583/bit.2022.3.05.

Mikhail A. Kupriyashin[1], Regina F. Baiazitova[2]
[1,2]*National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),*
Kashirskaya shosse, 31, Moscow, 115409, Russia
[1]*e-mail: rfbayazitova@mail.ru, https://orcid.org/0000-0003-0012-9309*
[2]*e-mail: kmickle@yandex.ru, https://orcid.org/0000-0001-6887-4810*

Hiding data in blocks of Oracle Database

DOI: http://dx.doi.org/10.26583/bit.2022.3.05

Abstract. In this paper, we explore the possibility of storing a hidden message in the physical data structures of the Oracle Database Management System (DBMS). We consider data blocks, the fundamental Oracle Database storage units for table data and other objects. As a result of normal usage, free space in data blocks gets fragmented. We devised a technique to form the desired fragmentation pattern in a data block. Assuming fragments of free space correspond to “0” bits, and fragments of data corresponding to “1” bits, we may store a secret message inside a block. In order to form the container, we need the object privileges to SELECT, DELETE and INSERT data. The SELECT object privilege is required to retrieve the message at a later time. The paper covers the technique of message embedding in detail. In conclusion we discuss various use causes for the technique. It should be noted that the operations of deleting and then adding rows lead to eventual damage to the steganographic container. In this regard, we studied the OLAP and OLTP database models. We conclude that OLAP databases are better suited for embedding secret messages due to the small number of the operations mentioned before.
Keywords: steganography, data hiding, databases, database management systems, Oracle Database.

For citation: KUPRIYASHIN, Mikhail A.; BAIAZITOVA, Regina F. Hiding data in blocks of Oracle Database. IT Security (Russia), [S.l.], v. 29, no. 3, p. 62–71, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1433. DOI: http://dx.doi.org/10.26583/bit.2022.3.05.

Введение

В настоящее время существует большое количество методов цифровой стеганографии, использующих различные типы контейнеров: от изображений до заголовков пакетов TCP/IP [1, 2].

При этом большое количество таких методов основывается на особенностях структуры самих контейнеров: наличии избыточности, малозаметных областей метаданных. Авторами было замечено, что такими свойствами обладают и файлы систем управления базами данных (СУБД). В качестве объекта исследования была выбрана СУБД Oracle Database, являющаяся наиболее популярной среди всех решений.

На основе анализа современных исследований в области цифровой стеганографии была найдена и разработана методика сокрытия сообщений в метаданных таблиц СУБД.

1. Особенности физической структуры данных

Архитектура СУБД Oracle Database имеет большое количество особенностей, представляющих потенциальную возможность для скрытого хранения данных. Одна из них основана на особенности фрагментации свободного пространства в этой СУБД.

Блок данных, являющийся наименьшей единицей хранения данных в архитектуре Oracle, состоит из заголовка и области для хранения данных. При добавлении данных в таблицу, содержимое строк последовательно добавляется в эту область. Как следствие, данные располагаются в нём в порядке своего появления. При удалении строки новые строки не будут занимать это место до достижения заполнения блока. Поэтому значения ROWID местоположения данных остаются без изменения (рис. 1).

Пользователи и администраторы СУБД могут определить физическое местоположение данных каждой строки, запросив при выборке значения псевдостолбца ROWID. Псевдостолбец ROWID существует во всех таблицах базы данных (БД), но значения ROWID для каждой строки не хранятся, а формируются на основе физического расположения данных этой строки в файлах и блоках данных [3].

Эти особенности можно использовать для встраивания в физическую структуру данных секретного сообщения. Если в последовательности возрастающих ROWID обнаруживаются пропуски, это свидетельствует об удалённых строках базы данных. Сопоставив удалённым строкам значение «0», а присутствующим – значение «1», можно закодировать секретное сообщение.

Предположим, что у нас есть пустой стеганоконтейнер, представляющий собой таблицу, и секретное сообщение длины N. Его можно заполнить следующим образом:

1. Удалить строки таблицы с помощью TRUNCATE или последовательных операций DELETE.
2. Последовательно рассмотреть биты секретного сообщения m1..mi..mn. В случае, если mi равен «1», в новую таблицу добавляется следующая строка из старой. В случае, если mi равен «0», в новую таблицу добавляются случайные данные.
3. Удалить из таблицы все строки, содержащие случайные данные.

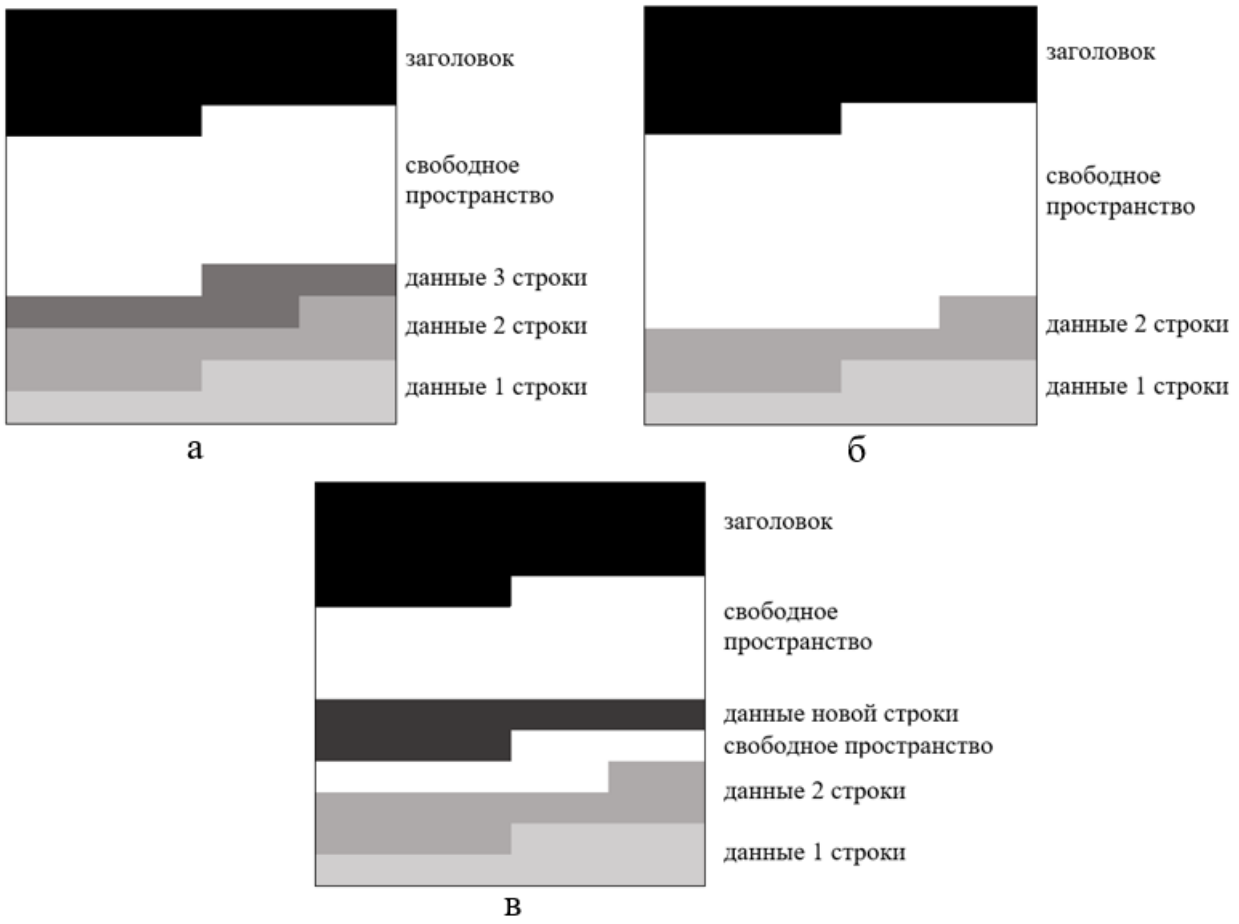

Рис. 1. Графическая иллюстрация заполнения блока строками: а – блок до удаления строки; б – блок после удаления строки; в – блок после добавления новой строки
Fig. 1. Graphic illustration of the process of filling a block with rows: a – the block before deleting; b – the block after deleting a row; c – the block after adding a new row

На шаге 2 всем строкам таблицы должны соответствовать последовательно возрастающие значения ROWID. После удаления данных на шаге 3, пропуски в последовательности ROWID будут соответствовать нулевым битам секретного сообщения. На рис. 2 представлена блок-схема встраивания. На шаге 1, если в таблице строки идут непрерывно в смысле последовательности их ROWID, то для встраивания достаточно вручную удалить каждую существующую строку с помощью DELETE. В противном случае следует очистить таблицу от всех строк с помощью команды TRUNCATE, которая помимо того, что удаляет все строки сразу, также освобождает всё пространство блоков, так, что новые строки вставляются с ROWID, начинающегося с первого в первом блоке объекта. В данном методе это необходимо во избежание встраивания каких-то строк в уже не используемое место в блоке.

На приведённой блок-схеме под удалением всех записей подразумевается использование TRUNCATE, а удалением каждой записи в отдельности — операции DELETE.

На рис. 3 приводится процесс встраивания сообщения в таблицу с данными.

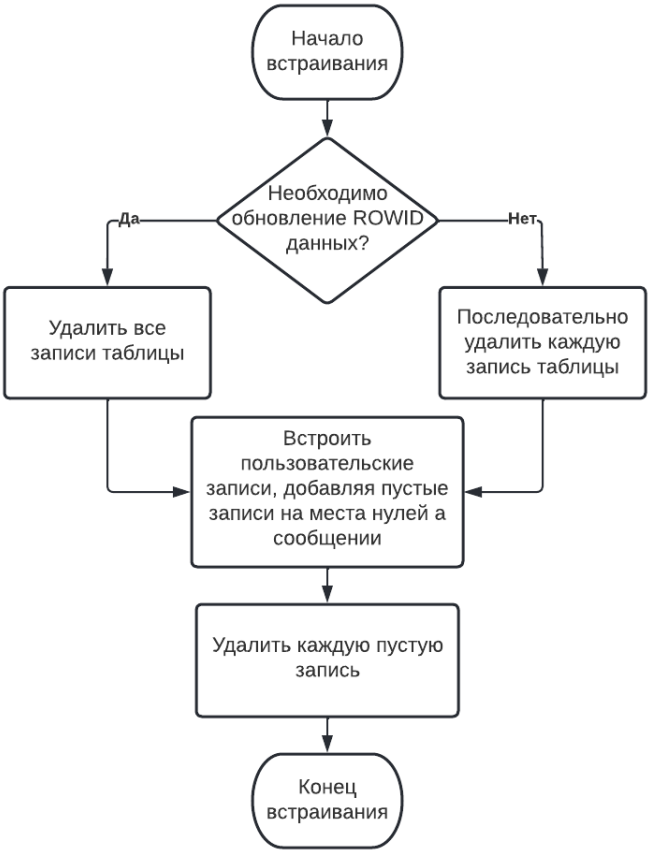

Рис. 2. Блок-схема для встраивания сообщения
Fig. 2. A block diagram for embedding a message

ROWID	SOME_USER_DATA
AAATZEAAMAAAACTAAA	Ufa
AAATZEAAMAAAACTAAB	Kazan
AAATZEAAMAAAACTAAC	Moscow
AAATZEAAMAAAACTAAD	Orel
AAATZEAAMAAAACTAAE	Izhevsk
AAATZEAAMAAAACTAAF	Suzdal

а

ROWID	SOME_USER_DATA
AAATZEAAMAAAACTAAA	Ufa
AAATZEAAMAAAACTAAD	Kazan
AAATZEAAMAAAACTAAF	Moscow
AAATZEAAMAAAACTAAG	Orel
AAATZEAAMAAAACTAAI	Izhevsk
AAATZEAAMAAAACTAAJ	Suzdal

в

ROWID	SOME_USER_DATA
AAATZEAAMAAAACTAAA	Ufa
AAATZEAAMAAAACTAAB	<empty>
AAATZEAAMAAAACTAAC	<empty>
AAATZEAAMAAAACTAAD	Kazan
AAATZEAAMAAAACTAAE	<empty>
AAATZEAAMAAAACTAAF	Moscow
AAATZEAAMAAAACTAAG	Orel
AAATZEAAMAAAACTAAH	<empty>
AAATZEAAMAAAACTAAI	Izhevsk
AAATZEAAMAAAACTAAJ	Suzdal

б

Рис. 3. Изменение вида таблицы и адресов строк в процессе встраивания сообщения: а – строки таблицы перед встраиванием; б – строки таблицы после удаления и встраивания вместе со строками для удаления; в – строки таблицы по окончании встраивания, после удаления соответствующих строк
Fig. 3. A change of the table and addresses of rows during the embedding of the message: a – rows of the table before embedding; b – rows of the table after deleting and adding them with rows for later deletion; c – rows of the table at the end of embedding after deletion of some rows

Для извлечения сообщения необходимо:

1. Выполнить выборку из заполненного стеганоконтейнера.
2. Определить нормальный шаг ROWID на основе размера каждой строки.
3. Просканировать последовательность ROWID по возрастанию. В каждой следующей строке, изменение ROWID на один шаг соответствует биту «1», а на n шагов – (n–1) последовательному биту «0» секретного сообщения.

В табл. 1 приводится описание необходимых привилегий для извлечения сообщения.

Таблица 1. Обязательные привилегии на этапе извлечения сообщения

SQL операция	Описание применения
SELECT	Операция получения содержимого таблиц. Для реализации метода на принимающей стороне требуется наличие этой привилегии на таблицу, выбранную в качестве контейнера.

2. Выбор потенциального контейнера

В рассматриваемой методике ключевыми параметрами для выбора подходящего контейнера являются размер таблицы и имеющиеся у пользователя привилегии на таблицу.

Размер таблицы ограничивает размер сообщения, которое можно в неё встроить. Каждая строка представляет бит данных. Количество строк таблицы должно соответствовать размеру сообщения следующим образом: их должно быть не меньше, чем вес Хэмминга встраиваемого сообщения.

После выбора таблицы с учётом фактора размера, следует изучить текущее положение строк таблицы. Если в таблице строки идут непрерывно в смысле последовательности их ROWID, то для встраивания достаточно вручную удалить каждую существующую строку с помощью DELETE, а затем перезаписать их с соответствующими «пустыми» строками в качестве нулей. Необходимые для встраивания в этом случае привилегии приведены в табл. 2.

Таблица 2. Обязательные привилегии для встраивания сообщения в первом случае

SQL-инструкция	Описание применения
DELETE	Используется во время подготовки таблицы к встраиванию, то есть очищению от строк, а затем при удалении строк, которые выступают в роли нулей во встраиваемом сообщении.
INSERT	Используется при обратном встраивании строк вместе со строками-нулями.
SELECT	Используется на этапе подготовки к встраиванию сообщения для получения текущих значений ROWID строк.

В противном случае следует очистить таблицу от всех строк с помощью команды TRUNCATE, которая помимо того, что удаляет все строки сразу, освобождает блок таким образом, что после этого новые строки вставляются с ROWID, начинающегося с первого в блоке (последний символ в значении ROWID будет снова «A»). В методике это необходимо во избежание встраивания каких-то строк в освобождённое посредством операций удаления место в блоке. Тогда список необходимых привилегий в первом случае пополнится привилегией DROP, которая необходима для выполнения TRUNCATE, согласно [3]. Полный список приведён в табл. 3.

Таблица 3. Обязательный список привилегий для встраивания во втором случае

SQL-инструкция	Описание применения
DROP	Привилегия на удаление одного объекта. Используется для подготовки таблицы к встраиванию сообщения.
INSERT	Используется при обратном встраивании строк вместе со строками-нулями.
DELETE	Используется для удаления строк-нулей при встраивании.
SELECT	Как и в предыдущем случае, необходимо для получения текущих значений ROWID строк при подготовке к встраиванию, а затем при удалении – для выяснения ROWID, по которым требуется его произвести.

3. Оценка пропускной способности канала

Важнейшим аспектом для обеспечения возможности эксплуатации разработанных методик является оценка их характеристик, на которых будут строиться рекомендации по их использованию, на основе которых пользователи смогут принять ряд необходимых решений по выбору контейнера и другим моментам перед непосредственным встраиванием и хранением сообщений. На данный момент существует множество различных характеристик, как общих, так и основывающихся на спецификах контейнеров в конкретных методах. Для осуществления оценки методики можно провести анализ пропускной способности и продолжительности жизни контейнера с сообщением.

Под пропускной способностью в стеганографии понимается максимальный размер секретного сообщения, которое пересылается в одном контейнере – такое описание приводится в [4]. Оценка вместительности встречается в большом количестве современных исследований. В [5] дано аналогичное определение коэффициента использования контейнера или коэффициента эффективности, который определяется как отношение размера наибольшего сообщения к размеру.

В стеганографии сложилось несколько общепринятых подходов к оценке пропускной способности [6]. В данной работе, по аналогии с [7], оценим пропускную способность как количество бит информации в строке таблицы.

На вход перед встраиванием подаются данные в двоичном представлении. При этом на этапе встраивания каждая строка соответствует одному двоичному символу, затем строки, кодирующие нули, удаляются, однако место, выделенное под них в блоке, остаётся. При оценке пропускной способности необходимо учитывать это. Тогда пропускная способность для методики – 1 бит/строка. Приведём пример. Пусть размер пространства, выделяемого в блоке под пользовательские данные, составляет 4096 байт, количество строк пользовательских данных в выбранной таблице равно 100. Средний размер строк таблицы равен 15 байтам. Тогда максимальное количество строк, помещающихся в эту таблицу, будет примерно равно 273. Соответственно, если встраиваемое сообщение будет не соответствовать хотя бы одному критерию: вес Хэмминга не более 100 и размер сообщения не более 273 бит, то встраивание станет невозможным.

После осуществления оценки пропускной способности канала в выбранной методике следует оценить объём пространства, доступного для встраивания, в конкретном выбранном контейнере.

Для методики этот объём будет зависеть, как отмечено выше, от размера блока, значения резервируемого места в блоке, которое будет использовано в случае изменений размеров строк, а также количества строк в таблице. Размер пространства в блоке, которое

выделяется для пользовательских строк, определяется значением PCTFREE. Это параметр, определяемый при создании таблицы, показывает, какой максимальный процент блока может быть заполнен до момента, когда он будет отмечен системой как занятый. Таким образом, для получения оценки необходимо вычислить средний размер строки выбранной таблицы, получить значение PCTFREE для неё и размер блока в табличном пространстве. Окончательное значение будет вычисляться как отношение произведения PCTFREE и размера к средней длине строк.

4. Условия повреждения контейнера

В течение жизненного цикла данные в таблице, как правило, подвергаются различного рода модификациям, которые могут привести к разрушению скрытого сообщения. Такими событиями могут быть следующие:

1. Удаление строк, участвующих в хранении сообщения.
2. Добавление строк в случаях, когда блок помечается системой, как свободный.
3. Удаление таблицы.
4. Перемещение таблицы.

В общем случае, невозможно оценить вероятность наступления вышеперечисленных событий, так как она существенно зависит от режима использования конкретной базы данных. Тем не менее, значительное число баз данных в этом отношении описывается одной из двух широко известных моделей: OLAP или OLTP. Обе основываются на реляционной теории, но используют отличающиеся технические подходы [8]

Первой будет рассмотрена модель OLAP. Хранилища данных преимущественно работают в режиме чтения; данные на запись поступают редко и большими порциями [8]. Ценность в таких СУБД представляет накопленная за достаточно большой промежуток времени историческая информация [9]. Записи, ранее помещённые в хранилище, редко подвергаются модификациям. Из этого следует вывод о том, что при использовании описываемой в этой работе методики сообщение не подвергнется разрушениям в течение длительного времени.

Базы данных OLTP служат источником информации в хранилищах данных. Данные в них обновляются и меняются регулярно, поэтому скорость обработки запросов является важнейшим показателем эффективности работы системы, для обеспечения которой служат транзакции. Они обрабатываются в течение нескольких миллисекунд и нет ничего, что требовало бы больше секунды [10].

Операция чтения, очевидно, не может повлиять на контейнер в разработанной методике, так как не меняют данные, содержащие само сообщение. Изменение строки влияет только на её содержимое, при этом положение строки не меняется (возможно, за исключением случаев так называемых переездов строки: в случае, когда она не помещается в установленные пределы на уровне блоков данных в ней помещается адрес её нового расположения, однако при этом сама строка не перемещается в таблице и продолжает занимать своё место в блоке, поэтому это не повлияет на значение ROWID и не стоит дальнейшего рассмотрения). Так как сообщение встраивается в метаданные таблицы, то эта операция не несёт угрозы его целостности. Наконец удаление строки по описанной выше логике приведёт к потере одного бита сообщения.

В связи с тем, что при встраивании сообщения предполагается использование разности адресов соседних строк для кодирования соответствующего количества нулей между единицами, в случае удаления строки пользователем, не участвующим в секретном общении, единица сообщения будет заменена нулём. Добавление легитимным пользователем строки в случае, если блок помечен системой как свободный, может привести к замене нуля сообщения на единицу.

5. Рекомендации по применению

Для применения методики первым шагом необходимо оценить БД на наличие подходящей таблицы для встраивания. Этот процесс представлен в виде блок-схемы на рис. 4. При наличии возможности выбора между различными БД в данной работе выбрана модель OLAP, в связи с описанными преимуществами.

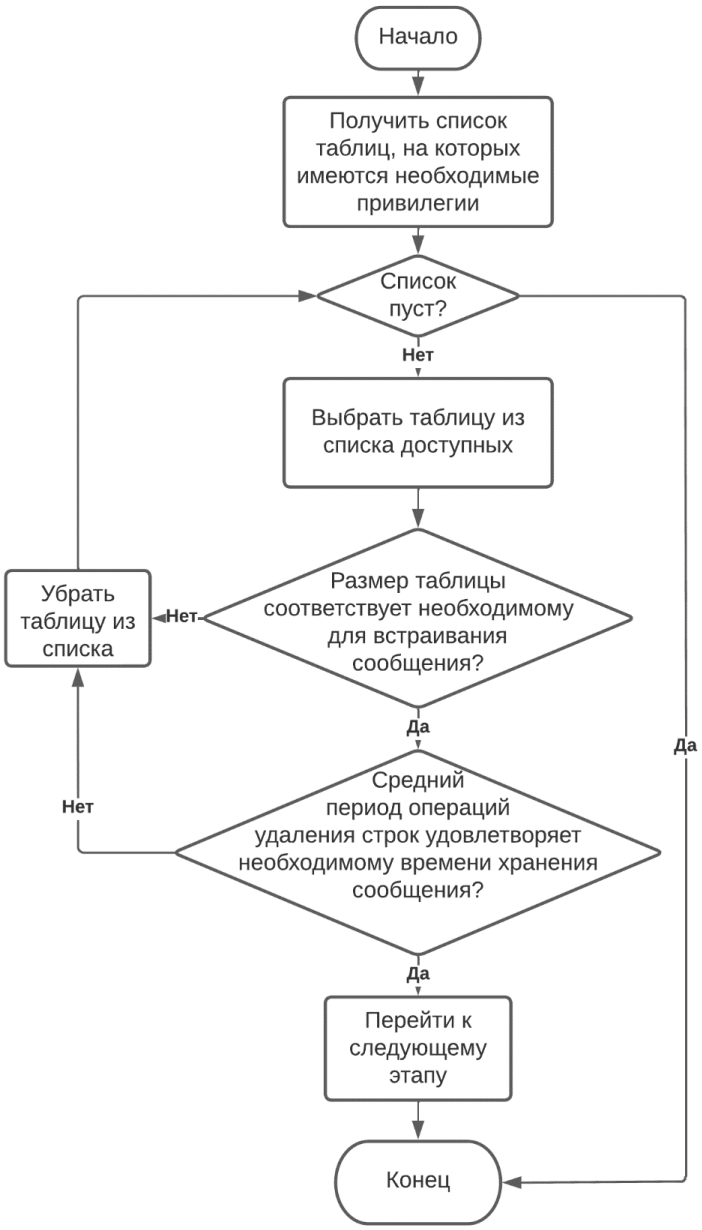

Рис. 4. Блок-схема поиска подходящего контейнера для реализации методики
Fig. 4. A block diagram of the search for eligible container for the technique

Второй этап подготовки к реализации стеганографического канала заключается в модификации сообщения в соответствии с потребностями в достижении максимальной практической устойчивости к внешним факторам. Это особенно важно в случае, если база данных работает в соответствии с моделью OLTP. Для снижения риска повреждения сообщения следует рассмотреть возможность применения корректирующих кодов, например, кодов Хэмминга. На данный момент существует большое множество различных вариантов. Порядок действий при этом представлен на рис. 5.

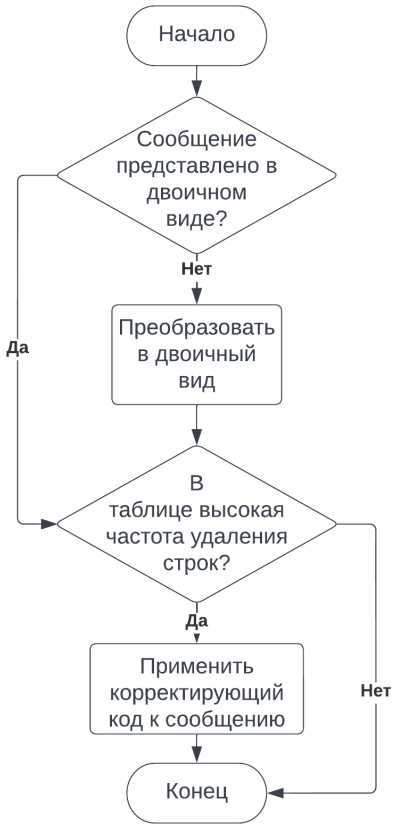

Рис. 5. Блок-схема второго этапа подготовки к встраиванию
Fig. 5. A block diagram of the second part of preparations for the embedding

Заключение

В настоящей работе предложена и исследована методика сокрытия сообщения в структуру СУБД Oracle Database на основе особенности фрагментации свободного места. При встраивании происходит добавление дополнительных строк к пользовательским, таким образом, что первые соответствуют нулям, а вторые – единицам сообщения.

Применение данной методики возможно при соблюдении определённых условий, связанных с привилегиями на выполнение необходимых операций, а также наличием достаточного места в таблице.

Для практического применения методики приведён анализ важных стеганографических характеристик – пропускная способность канала и продолжительность жизни заполненного контейнера. На основе полученных характеристик и описания необходимых предварительных условий предложены рекомендации по эффективной эксплуатации методики на практике.

СПИСОК ЛИТЕРАТУРЫ:

1. Dhobale D.D., Ghorpade V.R., Patil B.S., Patil S.B. Steganography by hiding data in TCP/IP headers. 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE). Chengdu: IEEE. 2010, p. V4-61-V4-65. DOI: http://dx.doi.org/10.1109/ICACTE.2010.5579643.
2. Sergeev A.V., Khorev P.B. Overview on hiding data in microsoft office documents. 3rd International Youth Conference on Radio Electronics, Electrical and Power Engineering, REEPE 2021. M.: IEEE. 2021, p.1–4. DOI: http://dx.doi.org/10.1109/REEPE51337.2021.9388038.
3. Ashdown L., McCormack J., Kyte T. Oracle Database Database Concepts, 18 c. – Oracle Database Documentation. URL: https://docs.oracle.com/en/database/oracle/oracle-database/18/cncpt/ (дата обращения: 5.04.2022).

4. Варновский Н.П., Голубев Е.А., Логачев О.А. Современные направления стеганографии. Материалы конференции "Математика и безопасность информационных технологий" в МГУ 28-29 октября 2004 г. М.: МЦНМО. 2005, с. 32–64. URL: http://www.iisi.msu.ru/UserFiles/File/publications/mabit04.pdf (дата обращения: 30.08.22).
5. Аграновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А. Стеганография, цифровые водяные знаки и стеганоанализ: Монография. М.: Вузовская книга, 2009. – 220 с. URL: https://www.elibrary.ru/item.asp?id=20312731 (дата обращения: 30.08.22) – EDN RCNCEV.
6. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. Киев: МК-Пресс, 2006. – 288 с. URL: https://studfile.net/preview/7379018/ (дата обращения: 30.08.22).
7. Kadhim I.J., Premaratne P., Vial P.J., Halloran B. Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. Neurocomputing. 2019, vol. 335, p. 299–326. DOI: http://dx.doi.org/10.1016/j.neucom.2018.06.075.
8. Plattner H. A common database approach for OLTP and OLAP using an in-memory column database. Proceedings of the 2009 ACM SIGMOD International Conference on Management of data. 2009, p. 1–2. DOI: http://dx.doi.org/10.1145/1559845.1559846.
9. Inmon, W.H. Building the Data Warehouse, Fourth Edition. – 4th ed. м Indianapolis: Wiley Publishing, Inc., 2005. – 576 p. URL: https://ia800202.us.archive.org/9/items/2005BuildingTheDataWarehouse4thEditionWilliamH.Inmon/2005%20-%20Building%20The%20Data%20Warehouse%20%284th%20Edition%29%20%28William%20H.%20Inmon%29.pdf (дата обращения: 30.08.22).
10. Кайт Т. Oracle для профессионалов: архитектура и методики программирования. Т. Кайт, Д. Кун. 3-е изд. М.: И.Д. Вильямс, 2016. – 960 с.

REFERENCES:

[1] Dhobale D.D., Ghorpade V.R., Patil B.S., Patil S.B. Steganography by hiding data in TCP/IP headers. 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE). Chengdu: IEEE. 2010, p. V4-61-V4-65. DOI: http://dx.doi.org/10.1109/ICACTE.2010.5579643.
[2] Sergeev A.V., Khorev P.B. Overview on hiding data in microsoft office documents. 3rd International Youth Conference on Radio Electronics, Electrical and Power Engineering, REEPE 2021. M.: IEEE. 2021, p.1–4. DOI: http://dx.doi.org/10.1109/REEPE51337.2021.9388038.
[3] Ashdown L., McCormack J., Kyte T. Oracle Database Database Concepts, 18c – Oracle Database Documentation. URL: https://docs.oracle.com/en/database/oracle/oracle-database/18/cncpt/ (accessed: 5.04.2022).
[4] Varnovskij N. P., Golubev E. A., Logachev O. A. Sovremennye napravleniya steganografii [Modern Modern directions of steganography]. Materialy konferencii "Matematika i bezopasnost' informacionnyx texnologij" v MGU 28-29 oktyabrya 2004 g. M.: MCNMO. 2005, s. 32–64. URL: http://www.iisi.msu.ru/UserFiles/File/publications/mabit04.pdf (accessed: 30.08.22) (in Russian).
[5] Agranovskij A.V., Balakin A.V., Gribunin V.G., Sapozhnikov S.A. Steganografiya, cifrovye vodyanye znaki i steganoanaliz: Monografiya [Steganography, digital watermarks and steganoanalysis: Monograph]. M.: Vuzovskaya kniga, 2009. – 220 s. URL: https://www.elibrary.ru/item.asp?id=20312731 (accessed: 30.08.22) – EDN RCNCEV (in Russian).
[6] Konaxovich G.F., Puzyrenko A.Yu. Komp'yuternaya steganografiya. Teoriya i praktika. [Computer steganography. Theory and practice]. Kiev: MK-Press, 2006. – 288 s. URL: https://studfile.net/preview/7379018/ (accessed: 30.08.22) (in Russian).
[7] Kadhim I.J., Premaratne P., Vial P.J., Halloran B. Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. Neurocomputing. 2019, vol. 335, p. 299–326. DOI: http://dx.doi.org/10.1016/j.neucom.2018.06.075.
[8] Plattner, H. A common database approach for OLTP and OLAP using an in-memory column database / Proceedings of the 2009 ACM SIGMOD International Conference on Management of data. 2009, p. 1–2. DOI: http://dx.doi.org/10.1145/1559845.1559846.
[9] Inmon, W.H. Building the Data Warehouse, Fourth Edition. – 4th ed. м Indianapolis: Wiley Publishing, Inc., 2005. – 576 p. URL: https://ia800202.us.archive.org/9/items/2005BuildingTheDataWarehouse4thEditionWilliamH.Inmon/2005%20-%20Building%20The%20Data%20Warehouse%20%284th%20Edition%29%20%28William%20H.%20Inmon%29.pdf (дата обращения: 30.08.22).
[10] Kajt T. Oracle dlya professionalov: arxitektura i metodiki programmirovaniya [Expert Oracle, Signature Edition Programming Techniques]. T. Kajt, D. Kun. 3-e izd. M.: I.D. Vil'yams, 2016. – 960 s. (in Russian).

Поступила в редакцию – 01 июля 2022 г. Окончательный вариант – 31 августа 2022 г.
Received – July 01, 2022. The final version – August 31, 2022.

Алексей С. Гераськин[1], Анастасия А. Шуликина[2], Анна А. Лукьянова[3]
Саратовский национальный исследовательский государственный университет им. Н.Г. Чернышевского
ул. Астраханская, 83, Саратов, 410012, Россия
[1]*e-mail: gerascinas@mail.ru, https://orcid.org/0000-0002-3118-1022*
[2]*e-mail: shulikinaanastasia@yandex.ru, https://orcid.org/0000-0003-4285-7873*
[3]*e-mail: redhair.dex6@gmail.com, https://orcid.org/0000-0002-1513-9721*

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПОВЫШЕНИЯ УСТОЙЧИВОСТИ К АТАКАМ МЕТОДА ДИФФЕРЕНЦИАЛЬНОГО ВСТРАИВАНИЯ ЭНЕРГИИ

DOI: http://dx.doi.org/10.26583/bit.2022.3.06

Аннотация. Целью статьи является исследование возможности повышения устойчивости встраивания цифрового водяного знака (ЦВЗ) методом дифференциального встраивания энергии (DEW) к статистическим атакам: медианный фильтр, фильтр Гаусса, пороговое округление, шумоподавление, сжатие; геометрическим атакам: поворот на 90 градусов, незначительная обрезка, масштабирование; атака на повторную запись. Рассматриваются особенности встраивания ЦВЗ методом DEW и возможности повышения надежности этого метода с применением визуальной модели Уотсона. Одной из основных проблем при встраивании ЦВЗ методом DEW является то, что он встраивает информацию в высокочастотные коэффициенты, которые отбрасываются фильтрами, и метод DEW не учитывает, какое влияние на исходное изображение оказывает изменение коэффициентов дискретного косинусного преобразования (ДКП). В качестве решения этих проблем предложена модификация метода, основанная на визуальной модели Уотсона. Модель оценивает максимально допустимым значением, которое можно изменить без визуального воздействия. При сравнении коэффициентов ДКП в алгоритме DEW в соответствии со значениями частотной чувствительности визуальной модели Уотсона уменьшается влияние на визуальное качество изображения. В работе приведена оценка изменений вносимых в изображение при встраивании ЦВЗ с помощью структурного сходства, а устойчивость цифрового водяного знака оценивалась с помощью коэффициента Пирсона. На основании данных представленных в статье проведено сравнение метода DEW и метода DEW с применением модели Уотсона. Согласно проведенному исследованию метод DEW с применением модели Уотсона устойчив к атакам на повторную запись, частично устойчив к геометрической и статистической атаке, тогда как метод DEW к статистическим атака и геометрическим не устойчив.

Ключевые слова: цифровой водяной знак, дискретное косинусное преобразование, метод DEW, модель Уотсона, коэффициент Пирсона, SSIM.

Для цитирования: ГЕРАСЬКИН, Алексей С.; ШУЛИКИНА, Анастасия А.; ЛУКЬЯНОВА, Анна А. ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПОВЫШЕНИЯ УСТОЙЧИВОСТИ К АТАКАМ МЕТОДА ДИФФЕРЕНЦИАЛЬНОГО ВСТРАИВАНИЯ ЭНЕРГИИ. Безопасность информационных технологий, [S.l.], т. 29, № 3, с. 72–81, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1436. DOI: http://dx.doi.org/10.26583/bit.2022.3.06.

Aleksey S. Geraskin[1], Anastasia A. Shulikina[2], Anna A. Lukyanova[3]
Saratov State University
83 Astrakhanskaya Str., Saratov, 410012, Russia
[1]*e-mail: gerascinas@mail.ru, https://orcid.org/0000-0002-3118-1022*
[2]*e-mail: shulikinaanastasia@yandex.ru, https://orcid.org/0000-0003-4285-7873*
[3]*e-mail: redhair.dex6@gmail.com, https://orcid.org/0000-0002-1513-9721*

Investigating the possibility of increasing the resilience to attack of the differential energy watermarking embedding method

DOI: http://dx.doi.org/10.26583/bit.2022.3.06

Abstract. The aim of this paper is to investigate the possibility of increasing the robustness of digital watermark embedding by the differential energy watermarking (DEW) embedding method to static attacks: median filter, Gaussian filter, threshold rounding, noise reduction, compression; to geometric attacks: 90-degree rotation, slight clipping, scaling; attack on rewrite. The peculiarities of digital watermark embedding by DEW method and ways to improve the reliability of this method using Watson's visual model are discussed. One of the main problems in digital watermark embedding by the DEW method is that it embeds information in high-frequency coefficients that are discarded by filters, and the DEW method does not take into account the effect that changes in discrete cosine transform (DCT) coefficients have on the original image. As a solution to these problems a modification of the method based on the Watson visual model has been proposed. The model estimates the maximum allowable value that can be changed without visual influence. Thus, by matching the discrete cosine transform coefficients in the DEW algorithm to the values of frequency sensitivity of Watson's visual model, one refuses to embed the watermark in the area with complex textures in order to reduce the impact on the visual quality and filtering effects. In this paper the changes introduced into the image by digital watermark embedding were evaluated using structural similarity (SSIM), and the stability of the digital watermark was evaluated using Pearson coefficient. Based on the data presented in the paper, a comparison of DEW method and DEW method using Watson's model was carried out. According to this study, the DEW method using Watson's model is resistant to repeated recording attacks, partially resistant to geometric and statistical attacks, while the DEW method is not resistant to static and geometric attacks.

Keywords: digital watermark, discrete cosine transform, DEW method, Watson model, Pearson coefficient, SSIM.

For citation: GERASKIN, Aleksey S.; SHULIKINA, Anastasia A.; LUKYANOVA, Anna A. Investigating the possibility of increasing the resilience to attack of the differential energy watermarking embedding method. IT Security (Russia), [S.l.], v. 29, no. 3, p. 72–82, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1436. DOI: http://dx.doi.org/10.26583/bit.2022.3.06.

Введение

В настоящее время информационных технологий, где обмен данными происходит быстро и комфортно, и вследствие этого становится трудно управлять цифровыми ресурсами. Из-за большого потока разной информации появляется проблема ее достоверности, уникальности [1]. Поэтому возникла необходимость внедрения некоторой авторской информации в передаваемые данные.

Наиболее эффективно для этих целей подходят методы стеганографии, такие как встраивание в мультимедийные файлы цифровые водяные знаки (ЦВЗ). Цифровой водяной знак – скрытно внедряемая метка, с помощью которой можно осуществлять контроль использования различных файлов с целью защиты авторских прав на продукцию [2]. В виде ЦВЗ может быть текст или логотип, которые идентифицируют автора файла.

Таким образом, ЦВЗ предназначен для защиты авторских прав цифровых файлов и подтверждения целостности самого документа. ЦВЗ можно встраивать в документы любого типа. Водяные знаки внедряют в мультимедийные файлы. Их применяют в системах для защиты от копирования цифровых данных. Также стеганография применяет ЦВЗ при обмене секретными сообщениями, внедренными в цифровой сигнал [1].

Существуют разные типы цифровых водяных знаков: видимые и прозрачные, а прозрачные, в свою очередь подразделяются на хрупкие и устойчивые. В зависимости от назначения используют разные типы ЦВЗ.

ЦВЗ используется в идентификации аудио, видео и фотоматериалов, определении незаконной копии материалов. На практике чаще всего используются алгоритмы встраивания ЦВЗ в изображения, тем более с ростом плагиата в сети, это особенно актуально. Существует множество алгоритмов встраивания ЦВЗ в изображение:

– метод WF5, основанный на взвешенном помехоустойчивом коде Хэмминга [3];

- метод Least Significant Bit (LSB), наименьший значащий бит – метод замены значащего бита [3, 4];
- встраивание методом Коча – производит поблочное дискретное косинусное преобразование изображения [4];
- алгоритм Differential Energy Watermarking (DEW), основанный на выборочном отбрасывании части высокочастотных коэффициентов дискретного косинусного преобразования (ДКП) сжатых изображений [5].

Но ЦВЗ, имеют недостатки. ЦВЗ неустойчивы к вредоносным воздействиям, таким как зашумление, фильтрация, изменение размера и яркости [6, 7]. Поэтому перед выбором алгоритма формирования ЦВЗ необходимо разобраться, что может предпринять злоумышленник, чтобы избавиться от ЦВЗ [8], и подобрать наиболее устойчивый алгоритм к атакам злоумышленника.

Например, очень распространен метод LSB – метод встраивания информации в пространственную область изображения [3]. Данный метод встраивания не требует дополнительных вычислений и позволяет скрывать в относительно небольших файлах большой объем секретной информации, но при малейшем искажении изображения приведёт к потере встроенной информации. Его часто заменяют на метод WF5, который позволяет оптимально скрыть ЦВЗ, таким образом, чтобы контейнер визуально не искажался и факт встраивания не был обнаружен [3]. Однако, метод WF5 позволяет легко, при незначительных искажениях контейнера, извлечь встроенную информацию в изображение. Метод Коча обладает рядом преимуществ, однако и у данного метода есть недостатки. Вследствие двукратного применения ДКП к изображению при внедрении и извлечении ЦВЗ, а также применения обратного ДКП для возврата к целочисленным матрицам пикселей после внедрения соотношение коэффициентов частотной матрицы может нарушиться, а это недопустимо, так как от этого напрямую зависит результат работы данного алгоритма [4]. Однако у ДКП большой потенциал устойчивости ЦВЗ, так как алгоритм косинусного преобразования достаточно распространен, большие диапазоны энергетических коэффициентов, позволяют встраивать большое количество информации, что позволяет повысить устойчивость DEW к атакам [9]. Эти недостатки требуют от исследователей продолжать поиски наиболее оптимальных методов алгоритмов встраивания ЦВЗ для защиты данных.

Целью данной работы является исследования возможности повышения устойчивости встраивания ЦВЗ методом DEW к определенным видам атак, таким как статистические, геометрические и атака на повторную запись.

1. Алгоритм DEW

В [10] выдвигается идея дифференциального энергетического водяного знака, представляющего собой метод ЦВЗ, основанный на выборочном отбрасывании части высокочастотных коэффициентов ДКП сжатых изображений и видеоизображений. В основе данного метода лежит дифференциальное встраивание энергии (DEW – Differential Energy Watermarking), под энергией понимается значение коэффициентов ДКП рассматриваемой области изображения.

По методу DEW осуществляется внедрение ЦВЗ в JPGE-изображение – подразумевается, что ЦВЗ состоит из l бит $b_j(j = 0, 1, 2, \dots, l-1)$. Каждый бит ЦВЗ встраивается в выбранную область, состоящую из n блоков по 8×8 коэффициентов ДКП канала яркости изображения каждый. Размер выбранной области определяет скорость встраивания – чем выше n, тем ниже скорость.

Каждый бит ЦВЗ внедряется в выбранную область модификацией разности энергий D между высокочастотными коэффициентами ДКП верхней части этой области (субобласть A) и ее нижней части (субобласть B). Подмножество высокочастотных коэффициентов обозначается $S(c)$.

Энергия субобласти A вычисляется:

$$E_A(c,n,Q) = \sum_{d=0}^{\frac{n}{2}-1} \sum_{i \in S(c)} ([\theta_{i,d}]_Q)^2, \quad (1)$$

где i,d – коэффициент ДКП с индексом i из d-го блока коэффициентов ДКП субобласти A; $[\,]_Q$ – означает, что энергия вычисляется у квантованных коэффициентов.

Энергия субобласти B вычисляется аналогично:

$$E_B(c,n,Q) = \sum_{d=\frac{n}{2}}^{n-1} \sum_{i \in S(c)} ([\theta_{i,d}]_Q)^2. \quad (2)$$

Подмножество $S(c)$ определяется на основе выбранного порога:

$$S(c) = \{h \epsilon \{1,63\} | (h \geq c)\}. \quad (3)$$

Выбором подходящего значения порога определяется стойкость ЦВЗ к удалению и его заметность на изображении. Когда же порог для каждой l_c-области определён, разность энергий определяется как:

$$D(c,n,Q) = E_A(c,n,Q) - E_B(c,n,Q). \quad (4)$$

Значение внедряемого бита определяет знак энергетической разности. Если значение бита «0», то $D > 0$, в противном случае $D < 0$. Следовательно, процедура встраивания информации модифицирует энергии E_A или E_B, чтобы встроить информацию в разность энергий D.

Центральную роль, как в процессе встраивания, так и в процессе извлечения встроенной информации играют энергии субобластей A и B, величина которых определяется четырьмя факторами:

- характером субобластей A и B;
- количеством блоков n на одну выбранную область;
- шагом квантователя;
- размером подмножества $S(c)$.

Если выбранная область однородная, то ее энергия будет содержаться в коэффициенте ДКП. Энергия высокочастотных коэффициентов равна нулю. В случае наличия контуров или текстур значения высокочастотных коэффициентов будут большими. Чем больше блоков n берется на одну выбранную область, тем больше значение содержащейся в ней энергии. Шаг квантователя определяет стойкость ЦВЗ к атаке перекодированием. Размер подмножества $S(c)$ определяется порогом c.

Для увеличения разности энергий необходимо, чтобы в процессе встраивания информации участвовало как можно больше коэффициентов ДКП. Но чрезмерное увеличение размера подмножества $S(c)$ приведет к заметным визуальным искажениям. Это означает, что для каждой выбранной области необходимо найти такое минимальное по размерам подмножество, для которого можно было бы достичь необходимой разницы энергий.

Низкочастотные коэффициенты ДКП модифицировать нежелательно, так как это может ухудшить визуальное качество изображения. Поэтому, порог должен быть не

меньше определенного значения c_{min}. Для определения подходящего c может быть использована следующая формула:

$$c(n, Q, c_{min}) = max\left\{c_{min}, max\left\{\begin{matrix} g \in \{1,63\} | (E_A(g,n,Q) > D) \\ \cap\, (E_B(g,n,Q) > D) \end{matrix}\right\}\right. . \quad (5)$$

Для извлечения встроенного бита получателю снова необходимо найти порог c. Но теперь берется уже максимум по всем порогам для субобластей A и B.

Основными проблемами алгоритма DEW являются:

– Высокочастотные коэффициенты ДКП легко отбрасываются фильтрами, в связи с чем алгоритм DEW, использующий для внедрения ЦВЗ высокочастотные коэффициенты, будет уязвим к этому воздействию на контейнер.
– Алгоритм DEW не учитывает, какое влияние на исходное изображение оказывает отбрасывание коэффициентов ДКП.

2. Модель Уотсона

Для решения приведенных проблем предлагается модификация, основанная на визуальной модели Уотсона [11]. Визуальная модель Уотсона – это одна из моделей, используемых для измерения визуальной точности. Модель восприятия пытается оценить коэффициент разницы JND (Just noticeable difference) между изображениями [12]. Коэффициент JND ДКП является максимально допустимым значением, которое можно изменить без визуального воздействия.

Модель чувствительности Уотсона определяет таблицу частотной чувствительности. Каждое значение в таблице является приблизительным эквивалентом минимума каждого коэффициента ДКП, который не может быть разрешен без маскирования шума [13]. Адаптивный к яркости означает, что, если средняя яркость блока 8×8 имеет больше света, коэффициент ДКП может быть увеличен, и это не привлечет особого внимания. Для каждого небольшого блока Уотсон регулирует размер коэффициентов в соответствии с таблицей чувствительности (табл. 1). Порог маскировки яркости может быть представлен как:

$$t_{ijk}^{L} = t_{ij}\left(\frac{X_k}{\bar{X}}\right)^{a_T}, \quad (6)$$

где t_{ij} – размер пикселей блока 8×8; X_k – размер блока исходного изображения; $\bar{X}$ – средний размер всех коэффициентов DC изображений; a_T – постоянная, рекомендованное значение которой составляет 0,649.

Таблица 1. Таблица частотной чувствительности коэффициентов ДКП

1.40	1.01	1.16	1.66	2.40	3.34	4.79	6.56
1.01	1.45	1.32	1.52	2.00	2.71	3.67	4.93
1.16	1.32	2.42	2.59	2.98	3.64	4.60	5.88
1.66	1.52	2.59	3.77	4.55	5.30	26.28	7.60
2.40	2.00	2.98	4.55	6.15	1.76	8.71	10.17
3.43	2.71	3.64	5.30	7.46	9.62	11.58	13.51
4.49	3.67	4.60	6.28	8.71	11.58	14.50	17.29
6.56	4.93	5.88	7.60	10.17	13.51	17.29	21.15

Свойство маскирования контраста (определенная частотная составляющая энергии превращает другую частотную составляющую в видимое снижение) создает порог маскирования, который определяется следующим образом:

$$S_{ijk} = max\{t_{ijk}^{L}, |X_{ijk}|^{\beta_{ij}} \times (t_{ijk}^{T})^{1-\beta_{ij}}\}, \quad (7)$$

где β_{ij} – это константа от 0 до 1, определяемая Уотсоном как $\beta_{ij} = 0{,}7$. Конечный порог S_{ijk} означает, что если изменение коэффициента ДКП $X_{ijk} > S_{ijk}$, то будут визуальные искажения. Этот алгоритм вычисляет JND_{ijk} для каждого из коэффициентов ДКП в соответствии с моделью Уотсона. В процессе встраивания дифференциальная энергия D может контролироваться путем пересмотра значений E_A и E_B , и поправочное значение каждого коэффициента ДКП X_{ijk} не должно превышать JND_{ijk}. Если $|X_{ijk}| < JND_{ijk}$, то $X_{ijk} = 0$, иначе:

$$\begin{cases} X_{ijk} = X_{ijk} - JND_{ijk}, (X_{ijk} \geq 0) \\ X_{ijk} = X_{ijk} + JND_{ijk}, (X_{ijk} > 0) \end{cases}. \quad (8)$$

Следовательно, водяной знак не будет оказывать заметного влияния на зрительное восприятие, тем самым улучшая прозрачность восприятия водяного знака. Таким образом, соизмерив в алгоритме DEW в соответствии со значением JND на основе визуальной модели Уотсона коэффициенты ДКП, мы отказываемся от встраивания водяного знака в область со сложными текстурами, чтобы уменьшить влияние на визуальное качество. Преимуществами данного метода являются: сложность удаления ЦВЗ, устойчивость к большинству видов атак, возможность снизить влияние на визуальное качество. Недостатки: низкая скорость встраивания ЦВЗ.

3. Оценка схожести изображений и стойкости встроенного ЦВЗ

Одной из важных проблем является количественная оценка качества изображения после внедрения ЦВЗ. Методы оценки качества изображения можно разделить на субъективные и объективные метрики. Субъективные метрики основаны на перцептивной оценке человеком-наблюдателем, в то время как объективные метрики основаны на вычислительных моделях, которые пытаются оценить качество изображения.

В рамках данной работы, оценка качества изображения со встроенным ЦВЗ производится с помощью PSNR (9) – пиковое отношение сигнала к шуму и SSIM – структурное сходство [14]:

$$PSNR = 10 \log_{10}\left(\frac{L^2}{MSE}\right), \quad (9)$$

где L – максимально возможное значение пикселя;

$$MSE = \frac{1}{N}\sum_{i=1}^{N}\left(I(i) - \hat{I}(i)\right)^2 \quad (10)$$

$$SSIM = \left(\frac{\sigma_{XY}}{\sigma_X \sigma_Y}\right)\left(\frac{2\bar{X}\bar{Y}}{(\bar{X})^2+(\bar{Y})^2}\right)\left(\frac{2\sigma_X\sigma_Y}{\sigma_X{}^2+\sigma_Y{}^2}\right), \quad (11)$$

$$\begin{cases} \bar{X} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} x_{ij} \\ \bar{Y} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} y_{ij} \end{cases}, \quad (12)$$

$$\sigma_X^2 = \frac{1}{(M-1)(N-1)}\sum_{i=1}^{M}\sum_{j=1}^{N}(x_{ij} - \bar{X})^2, \quad (13)$$

$$\sigma_Y^2 = \frac{1}{(M-1)(N-1)}\sum_{i=1}^{M}\sum_{j=1}^{N}(y_{ij} - Y)^2, \quad (14)$$

$$\sigma_{XY} = \frac{1}{(M-1)(N-1)}\sum_{i=1}^{M}\sum_{j=1}^{N}(x_{ij} - \bar{X})^2(y_{ij} - \bar{Y})^2, \quad (15)$$

где $X = \{x_{ij}\}$, $Y = \{y_{ij}\}$ – сравнимые изображения; M, N – размеры изображения.

Проверку на стойкость встроенного ЦВЗ будем осуществлять по средствам использования различных видов атак на изображение с ЦВЗ [15].

Для оценки качества извлеченного ЦВЗ будем использовать коэффициент корреляции Пирсона:

$$k = \frac{\sum_{i=1}^{n}(X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum_{i=1}^{n}(X_i - \bar{X})^2 \sum_{i=1}^{n}(Y_i - \bar{Y})^2}}, \quad (16)$$

где $X_i Y_i$ – биты внедренного и извлеченного ЦВЗ соответственно; $\bar{X} = \frac{1}{n}\sum_{t=1}^{n} X_t$, $\bar{Y} = \frac{1}{n}\sum_{t=1}^{n} Y_t$ – среднее значение выборок. Как правило, ЦВЗ считается устойчивым к вредоносному воздействию, если $k \geq 0{,}5$. В противном случае встроенная информация считается уничтоженной.

4. Анализ исследования стойкости алгоритма метода DEW и алгоритма метода DEW с применением модели Уотсона к атакам

В ходе исследования использовались три типа атак: статистические, геометрические и атака на повторную запись [6]. Для анализа была использована база, содержащая более 100 различных изображений. В исследовании проводились следующие виды статистических атак: наложением различных статистических фильтров, сжатие, а также внесение статистических шумов различными методами и их подавление (табл. 2).

Таблица 2. Исследование алгоритмов на предмет устойчивости к статистическим атакам

Атака	Алгоритм метода DEW с применением модели Уотсона		Алгоритм метода DEW	
	Процент побитового совпадения	Коэффициент Пирсона	Процент побитового совпадения	Коэффициент Пирсона
Медианный фильтр	85.638%	0.709	55.214%	0.421
Фильтр Гаусса	83.245%	0.661	43.598%	0.307
Пороговое округление	55.319%	0.177	13.017%	0.005
Шумоподавление	60.904%	0.229	30.105%	0.015
Сжатие quality = 85	94.947%	0.897	64.184%	0.592
Сжатие quality = 75	87.766%	0.75	47.606%	0.501
Сжатие quality = 50	69.415%	0.385	28.784%	0.145

Использовались следующие геометрические атаки: различные комбинации масштабирования и изменения пропорций изображения-контейнера, поворотов изображения-контейнера, сжатия и обрезки (табл. 3).

Таблица 3. Исследование алгоритмов на предмет устойчивости к геометрическим атакам

Атака	Алгоритм метода DEW с применением модели Уотсона		Алгоритм метода DEW	
	Процент побитового совпадения	Коэффициент Пирсона	Процент побитового совпадения	Коэффициент Пирсона
Поворот на 90 градусов	78.456%	0.569	70.821%	0.501
Незначительная обрезка	74.907%	0.509	64.517%	0.487
Масштабирование 85% от измерений	52.66%	0.061	30.156%	0.017

Атака на повторную запись представляет собой несколько последовательных внедрений в частотную область изображения нового ЦВЗ (табл. 4).

Таблица 4. Исследование алгоритмов на предмет устойчивости к атакам на повторную запись

Атака	Алгоритм метода DEW с применением модели Уотсона		Алгоритм метода DEW	
	Процент побитового совпадения	Коэффициент Пирсона	Процент побитового совпадения	Коэффициент Пирсона
Первое внедрение нового ЦВЗ	99.734%	0.995	99.005%	0.921
Второе внедрение нового ЦВЗ	97.074%	0.941	78.032%	0.815
Третье внедрение нового ЦВЗ	91.755%	0.834	67.037%	0.802
Четвертое внедрение нового ЦВЗ	88.032%	0.76	48.587%	0.531

В табл. 5 приведены обобщенные данные по результатам атак на ЦВЗ, внедренные методом алгоритма DEW и методом алгоритма DEW с применением модели Уотсона.

Таблица 5. Обобщенные данные по результатам атак на ЦВЗ

Тип атаки	Алгоритм метода DEW с применением модели Уотсона		Алгоритм метода DEW	
	Коэффициент Пирсона	SSIM	Коэффициент Пирсона	SSIM
Обрезка	≈0.5	–	≈0.4	–
Масштабирование	<0.1	–	<0.1	–
Поворот	≈0.5	–	≈0.5	–
Сжатие	>0.5	>0.7	≤0.5	<0.5
Шумоподавление	>0.3	>0.75	<0.1	–
Внесение шума	>0.5	≈0.5	>0.3	–
Внедрение нового ЦВЗ	>0.5	>0.7	>0.5	>0.6

Заключение

На основании данных проведенных исследований можно заключить, что стойкость метода DEW с применением модели Уотсона к статистическим и геометрическим атакам выше, чем у метода DEW. Из табл. 2 следует, что метод DEW не устойчив к следующим видам статистических атак: медианный фильтр, фильтр Гаусса, пороговое округление, шумоподавление, сжатие, тогда как метод DEW с применением модели Уотсона является устойчивым к данным атакам. Согласно данным табл. 3 метод DEW устойчив к геометрической атаке: поворот на 90 градусов, а метод DEW с применением модели Уотсона устойчив к таким атакам как поворот на 90 градусов и незначительная обрезка. Из табл. 4 видно, что метод DEW и метод DEW с применением модели Уотсона одинаково устойчивы к атакам на повторную запись. Таким образом, можно сделать вывод о том, что метод DEW с применением модели Уотсона устойчив к атакам на повторную запись, частично устойчив к геометрической и статистической атаке, следовательно, он является наиболее подходящим, чем метод DEW для встраивания ЦВЗ в изображения.

СПИСОК ЛИТЕРАТУРЫ:

1. Беззатеев С.В., Волошина Н.В., Минаева Т.А. Метод формирования многоуровневой структуры контейнера при встраивании ЦВЗ в цифровые изображения. Конвергенция цифровых и материальных миров: экономика, технологии, образование: Сборник научных статей международной научной конференции, Санкт-Петербург, 21–22 июня 2018 года. СПб: Санкт-Петербургский государственный экономический университет, 2018, с. 91–99. URL: https://elibrary.ru/item.asp?id=36553660 (дата обращения: 22.06.2022) – EDN SLYMTZ.
2. Завадская Т.В., Крахмаль М.В. Исследование методов цифровой стеганографии для маркировки изображений цифровыми водяными знаками. Современные тенденции развития и перспективы внедрения инновационных технологий в машиностроении, образовании и экономике. 2019, т. 5, № 1(4), с. 97–103. URL: https://elibrary.ru/item.asp?id=39470791 (дата обращения: 22.06.2022) – EDN FXFUXZ.
3. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. Киев: МК-Пресс, 2006. – 286 с. URL: https://studfile.net/preview/7379018/ (дата обращения: 22.06.2022).
4. Гераськин Алексей С., Стрельникова София Ю., Завенягин Максим. П. Исследование возможности улучшения реализации алгоритма метода Коча для встраивания цифровых водяных знаков в изображения. Безопасность информационных технологий, [S.l.], т. 25, № 4, с. 86–94, 2018. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2018.4.08. – EDN YQNKPJ.
5. Setyawan, I., Lagendijk R.L. Extended Differential Energy Watermarking (XDEW) algorithm for low bit-rate video watermarking. The Proceeding of the Seventh Annal Conference of the Advanced School in Computing and Imaging. 2001, p. 202–209. URL: https://citeseerx.ist.psu.edu/messages/downloadsexceeded.html (дата обращения: 22.06.2022).
6. Петелина М.В. Устойчивость цифровых водяных знаков. Сборник трудов молодых ученых и сотрудников кафедры ВТ под ред. д.т.н., проф. Т.И. Алиева. СПб: СПбНИУ ИТМО. 2012, с. 66–69. URL: https://masters.donntu.ru/2018/fknt/shevlyakov/library/article3.htm (дата обращения: 22.06.2022).
7. Шниперов Алексей Н.; Мельников Валерий А. Использование полярных гармонических преобразований при разработке методов маркирования изображений робастным цифровым водяным знаком. Безопасность информационных технологий, [S.l.], т. 28, № 4, с. 90–103, 2021. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2021.4.07. – EDN JDIRVG.
8. Иваненко Виталий Г.; Ушаков Никита В. Защита изображений формата jpeg при помощи цифровых водяных знаков. Безопасность информационных технологий, [S.l.], т. 25, № 2, с. 106–113, 2018. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2018.2.09. – EDN RTJLPN.
9. Голдобин И.А, Климова Е.И. Влияние шумов на алгоритмы цифровой обработки изображений. Сб. статей по материалам научно-технической конференции молодых ученых. Волгоград. 2021, с. 396–402. URL: https://www.elibrary.ru/item.asp?id=46498271 (дата обращения: 22.06.2022) – EDN JVIVOX.
10. Langelaar G.C. and Lagendijk R.L. Optimal differential energy watermarking of DCT encoded images and video. IEEE Transactions on Image Processing. 2001, vol. 10, no. 1, p. 148–158. DOI: http://dx.doi.org/10.1109/83.892451.
11. Watson A.B. DCT quantization matrices visually optimized for individual images, Proc. SPIE 1913, Human Vision, Visual Processing, and Digital Display IV, p. 202-216. (8 September 1993). DOI: http://dx.doi.org/10.1117/12.152694.
12. Yaqing Niua, Matthew Kyanb, Lin Mac, Azeddine Beghdadi, Sridhar Krishnanb, Visual saliency’s modulatory effect on just noticeable distortion profile and it’s application in image watermarking. Signal Processing: Image Communication. 2013, vol. 28, issue 8, p. 917–928. DOI: https://doi.org/10.1016/j.image.2012.07.009.
13. Cox I.J., Miller M.L., Bloom J.A. Digital Watermarking and Steganography, New York: Morgan Kaufmann Publishers, 2008. – 623 p. DOI: http://dx.doi.org/10.1016/B978-0-12-372585-1.X5001-3.
14. Старовойтов В.В. Уточнение индекса SSIM структурного сходства изображений. Информатика. 2018, т. 15, № 3, с. 41–55. URL: https://elibrary.ru/item.asp?id=35618972 (дата обращения: 22.06.2022) – EDN XZOOHR.
15. Batura V.A. Increase of stability at jpeg compression of the digital watermarks embedded in still images. Scientific and Technical Journal of Information Technologies, Mechanics and Optics. 2015, vol. 15, no. 4, p. 708–715. DOI: http://dx.doi.org/10.17586/2226-1494-2015-15-4-708-715.

REFERENCES:

[1] Bezzateev S.V, Voloshina N.V., Minaeva T.A. The method of forming a multi-level container structure when embedding digital watermark in digital images. Konvergenciya cifrovyh i material'nyh mirov: ekonomika, tekhnologii, obrazovanie: Sbornik nauchnyh statej mezhdunarodnoj nauchnoj konferencii, Sankt-Peterburg, 21–22 iyunya 2018 goda. SPb: Sankt-Peterburgskij gosudarstvennyj ekonomicheskij universitet. 2018,

s. 91–99. URL: https://elibrary.ru/item.asp?id=36553660 (accessed: 22.06.2022) – EDN SLYMTZ (in Russian).

[2] Zavadskaya T.V., Krakhmal M.V. Research of digital steganography methods to mark digital watermarks in an image. Sovremennye tendencii razvitiya i perspektivy vnedreniya innovacionnyh tekhnologij v mashinostroenii, obrazovanii i ekonomike. 2019, no. 1(4), s. 97–103. URL: https://elibrary.ru/item.asp?id=39470791 (accessed: 22.06.2022) – EDN FXFUXZ (in Russian).

[3] Konakhovich G.F., Puzyrenko A.IU. Komp'iuternaia steganografiia. Teoriia i praktika. Kiev: MK-Press, 2006. – 286 p. URL: https://studfile.net/preview/7379018/ (accessed: 22.06.2022) (in Russian).

[4] Geraskin Aleksey S.; Strelnikova Sofiia Yu.; Zavenyagin Maxim P. Research of possibility of improvement of realization of algorithm of method of koch for embedding of digital watermarks in images. IT Security (Russia), [S.l.], v. 25, no. 4, p. 86–94, 2018. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2018.4.08. – EDN YQNKPJ (in Russian).

[5] Setyawan I., Lagendijk R.L. Extended Differential Energy Watermarking (XDEW) algorithm for low bit-rate video watermarking. The Proceeding of the Seventh Annal Conference of the Advanced School in Computing and Imaging. 2001, p. 202–209. URL: https://citeseerx.ist.psu.edu/messages/downloadsexceeded.html (accessed 22.06.2022).

[6] Petelina M.V. Ustoichivost' tsifrovykh vodianykh znakov. Sbornik trudov molodykh uchenykh i sotrudnikov kafedry VT pod red. d.t.n., prof. T.I. Alieva. SPb: SPbNIU ITMO. 2012, s. 66–69. URL: https://masters.donntu.ru/2018/fknt/shevlyakov/library/article3.htm (accessed 22.06.2022) (in Russian).

[7] Shniperov Alexey N.; Melnikov, Valeriy A. The use of polar harmonic transformations in the development of methods for robust image watermarking. IT Security (Russia), [S.l.], v. 28, no. 4, p. 90–103, 2021. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2021.4.07. – EDN JDIRVG (in Russian).

[8] Ivanenko Vitaliy G.; Ushakov Nikita V. JPEG digital watermarking for copyright protection. IT Security (Russia), [S.l.], v. 25, no. 2, p. 106–113, 2018. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2018.2.09. – EDN RTJLPN (in Russian).

[9] Goldobin I. A., Klimova E. I. Vliianie shumov na algoritmy tsifrovoi obrabotki izobrazhenii. Sbornik statei po materialam nauchno-tekhnicheskoi konferentsii molodykh uchenykh. Volgograd. 2021, s. 396–402. URL: https://elibrary.ru/item.asp?id=46498271 (accessed 22.06.2022) – EDN JVIVOX (in Russian).

[10] Langelaar G.C. and Lagendijk R.L. Optimal differential energy watermarking of DCT encoded images and video. IEEE Transactions on Image Processing. 2001, vol. 10, no. 1, p. 148–158. DOI: http://dx.doi.org/10.1109/83.892451.

[11] Watson A.B. DCT quantization matrices visually optimized for individual images, Proc. SPIE 1913, Human Vision, Visual Processing, and Digital Display IV, p. 202-216 (8 September 1993). DOI: http://dx.doi.org/10.1117/12.152694.

[12] Yaqing Niua, Matthew Kyanb, Lin Mac, Azeddine Beghdadi, Sridhar Krishnanb, Visual saliency's modulatory effect on just noticeable distortion profile and it's application in image watermarking. Signal Processing: Image Communication. 2013, vol. 28, issue 8, p. 917–928. DOI: https://doi.org/10.1016/j.image.2012.07.009.

[13] Cox I.J., Miller M.L., Bloom J.A. Digital Watermarking and Steganography, New York: Morgan Kaufmann Publishers, 2008. – 623 p. DOI: http://dx.doi.org/10.1016/B978-0-12-372585-1.X5001-3.

[14] Starovoitov V.V. Enhancement of the structural similarity index SSIM. Informatics. 2018, vol. 15, no. 3, p. 41–55. URL: https://elibrary.ru/item.asp?id=35618972 (accessed: 22.06.2022) – EDN XZOOHR (in Russian).

[15] Batura V.A. Increase of stability at jpeg compression of the digital watermarks embedded in still images. Scientific and Technical Journal of Information Technologies, Mechanics and Optics. 2015, vol. 15, no. 4, p. 708–715. DOI: http://dx.doi.org/10.17586/2226-1494-2015-15-4-708-715.

Поступила в редакцию – 12 июля 2022 г. Окончательный вариант – 31 августа 2022 г.
Received – July 12, 2022. The final version – August 31, 2022.

Артём О. Калинкин[1], Светлана А. Голуб[2], Игорь Ю. Коркин[3], Данил Н. Пятовский[4],
Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
[1]*e-mail: kalinkin8884@gmail.com, https://orcid.org/0000-0002-7785-2979,*
[2]*e-mail: glb.svtln@gmail.com, https://orcid.org/0000-0002-2395-0661,*
[3]*e-mail: igor.korkin@gmail.com, https://orcid.org/0000-0001-7640-2792,*
[4]*e-mail: danil.piat@mail.ru, https://orcid.org/0000-0002-7280-9218*

ОБНАРУЖЕНИЕ ПРОГРАММ-ШИФРОВАЛЬЩИКОВ НА ОСНОВЕ ДАННЫХ МЕХАНИЗМА ТРАССИРОВКИ СОБЫТИЙ И ПРИМЕНЕНИЯ МЕТОДА МАШИННОГО ОБУЧЕНИЯ

DOI: http://dx.doi.org/10.26583/bit.2022.3.07

Аннотация. В настоящее время многие аналитические компании отмечают значительный рост компьютерных инцидентов с использованием программ-шифровальщиков. Данный вид вредоносного программного обеспечения частично или полностью изменяет файлы пользователей, вынуждая заплатить выкуп для восстановления файлов. По результатам проведённого в работе сравнительного анализа существующих способов обнаружения программ-шифровальщиков были выявлены их недостатки и принято решение о разработке нового средства обнаружения с использованием аппарата машинного обучения. Анализ недавних атак с использованием программ- шифровальщиков позволил выявить ряд особенностей взаимодействия с файловой системой, присущих только вредоносным программам данного вида. Для сбора информации о таких событиях выбран механизм Windows Event Tracing for Windows (ETW), который предустановлен во все современные сборки Windows и имеет широкие возможности по регистрации различных событий ОС. Для выбора подходящего алгоритма машинного обучения были протестированы следующие алгоритмы: одноклассовый метод опорных векторов (One Class Support Vector Machines), алгоритм изолирующего леса (Isolation Forest) и алгоритм локального уровня выброса (Local Outlier Factor). В качестве основного был выбран алгоритм Isolation Forest. С использованием механизма ETW были получены два набора данных для легитимных программ, и для программ-шифровальщиков. Для безопасной генерации наборов данных, соответствующих программам-шифровальщикам, был разработан демонстрационный прототип ПО, который реализовал основные алгоритмы взаимодействия с файловой системой популярных программ-шифровальщиков. Полученная выборка была поделена в отношении 30% и 70% для обучающего и тестового наборов соответственно. Данные из тестовой выборки не участвовали в процессе обучения. Программная реализация системы обнаружения выполнена на языке Python. Разработанная система была успешно опробована с использованием недавних программ-шифровальщиков WannaCry и TeslaCrypt, а также популярных образцов легитимного ПО VeraCrypt, TrueCrypt, 7z, СУБД Oracle.

Ключевые слова: программы-шифровальщики, машинное обучение, поиск аномалий, Event Tracing for Windows (ETW).

Для цитирования: КАЛИНКИН, Артём О. и др. ОБНАРУЖЕНИЕ ПРОГРАММ-ШИФРОВАЛЬЩИКОВ НА ОСНОВЕ ДАННЫХ МЕХАНИЗМА ТРАССИРОВКИ СОБЫТИЙ И ПРИМЕНЕНИЯ МЕТОДА МАШИННОГО ОБУЧЕНИЯ. Безопасность информационных технологий, [S.l.], т. 29, № 3, с. 82–93, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1437. DOI: http://dx.doi.org/10.26583/bit.2022.3.07.

Artem O. Kalinkin[1], Svetlana A. Golub[2], Igor Y. Korkin[3], Danil N. Pyatovskiy[4]
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31, Moscow, 115409, Russia
[1]*e-mail: kalinkin8884@gmail.com, https://orcid.org/0000-0002-7785-2979,*
[2]*e-mail: glb.svtln@gmail.com, https://orcid.org/0000-0002-2395-0661,*
[3]*e-mail: igor.korkin@gmail.com, https://orcid.org/0000-0001-7640-2792,*

[4]*e-mail: danil.piat@mail.ru, https://orcid.org/0000-0002-7280-9218*

Ransomware detection based on machine learning models and Event Tracing for Windows

DOI: http://dx.doi.org/10.26583/bit.2022.3.07

Abstract. Nowadays ransomware cyberattacks are alarmingly increasing. Ransomware is a form of malicious software that locks users' files by modifying it or it's parts. To get the files back the users are supposed to pay ransom. Ransomware are using different types of cryptography, from modern symmetric ciphers to asymmetric ciphers that require the both public key and a private key. The analysis of existing ransomware detection techniques reveals some drawbacks. It was decided to develop a new ransomware detection tool based on machine learning. The analysis of recent ransomware attacks helps to find the behaviour patterns during interactions with file system, which are typical only for ransomware. To collect related OS events, the Windows built-in mechanism named Windows Event Tracing for Windows (ETW) was used. The following machine learning algorithms were checked: One Class Support Vector Machines, Isolation Forest and Local Outlier Factor. Isolation Forest algorithm shows better results. The ETW helps to gain two datasets for legitimate software programs and for ransomware apps. The whole dataset was divided into two parts, training and testing, with the training part to be around 30% of the dataset and the testing one to be 70%. The Python has been used to program the proposed ransomware detection system. The developed system was successfully tested using WannaCry and TeslaCrypt encryption programs, as well as legitimate VeraCrypt, TrueCrypt, 7z, Oracle DBMS software.

Keywords: ransomware, machine learning, anomaly detection, Event Tracing for Windows (ETW).
For citation: KALINKIN, Artem O. et al. Ransomware detection based on machine learning models and Event Tracing for Windows. IT Security (Russia), [S.l.], v. 29, no. 3, p. 82–93, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1437. DOI: http://dx.doi.org/10.26583/bit.2022.3.07.

Введение

Согласно отчёту, предоставленному SonicWall [1], в 2021 г. было зарегистрировано более, чем в два раза больше атак программ-шифровальщиков чем в 2020 г. и в три раза больше, чем в 2019 г. Можно выделить несколько факторов, способствующих такому резкому росту числа атак программ-шифровальщиков.

Во-первых, появление и активное использование децентрализованных платежных систем с собственными денежными единицами (криптовалют) обеспечили возможность нарушителям получать анонимно выкуп от пользователей, без участия посредников. В результате нарушители получили возможность прямого финансового обогащения.

Во-вторых, появление услуги, в рамках которой разработчики вредоносного ПО предоставляют другим злоумышленникам по подписке программы-шифровальщики и инфраструктуру для управления ими – Ransomware-as-a-Service (RaaS).

Программы-шифровальщики используют самые передовые вредоносные техники для предотвращения обнаружения системой защиты информации, а высокая скорость атаки программ-шифровальщиков значительно затруднят их своевременное обнаружение и удаление.

Можно заключить, что своевременное обнаружение программ-шифровальщиков является актуальной задачей информационной безопасности.

В настоящей работе используется механизм Event Tracing For Windows (ETW), позволяющий получать различные события ОС в режиме реального времени для последующей обработки. Механизм ETW имеет следующие достоинства: переносимость на различные ОС семейства Windows, широкий спектр регистрируемых событий ОС, возможность обработки информации как в режиме реального времени, так и в автономном режиме путём сохранения в файл для последующей обработки.

1. Анализ недавних атак программ-шифровальщиков

Мы провели анализ основных этапов работы программ-шифровальщиков и примеров недавних атак, для установления особенностей программ-шифровальщиков, которые могут быть использованы для их обнаружения.

1.1 Определение программ-шифровальщиков и примеры

Программа-шифровальщик нарушает целостность файла путём изменения файла целиком либо его части. На рис. 1 представлены основные этапы работы программ-шифровальщиков. Далее будет представлен анализ каждого из этапов.

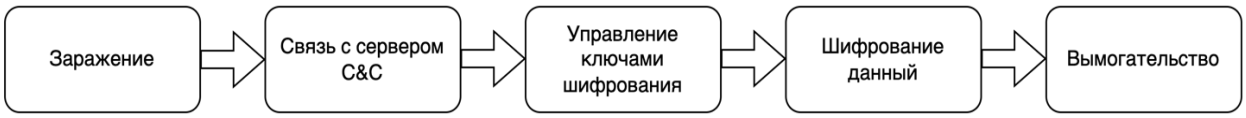

Рис. 1. Этапы атаки программ-шифровальщиков
Fig. 1. Stages of attack of cryptographic programs

I) Этап заражения. На этом этапе происходит доставка и запуск программы-шифровальщика на целевой компьютер пользователя. Нарушители используют следующие векторы атак для заражения [2]:

- рассылка спама и фишинговых писем;
- эксплуатация уязвимостей программных компонентов целевого компьютера пользователя, например веб-браузера;
- распространение вредоносного ПО через веб-сайты.

Наиболее популярным вектором заражения является распространение вредоносного ПО через веб-сайты.

II) Этап связи с управляющим сервером. После этапа заражения программа-шифровальщик обычно связывается через сеть Интернет с командным сервером, называемым Command and Control, C&C, C2 или кластером серверов для передачи и хранения ключей шифрования, а также информации о пользователе и заражённой системе.

Связь с сервером может быть организована с использованием следующих способов:

- статически настроенных IP-адресов;
- статических DNS-адресов (имён);
- динамически создаваемых DNS-адресов (имён).

Некоторые группы программ-шифровальщиков осуществляют работу без связи с сервером, поскольку открытый ключ из ассиметричной пары включен в двоичный файл программы-шифровальщика. Наиболее популярным способом связи является использованием статических DNS-адресов

III) Управление ключами шифрования. На данном этапе происходит генерация криптографических ключей для шифрования файлов пользователя. Криптографические ключи могут быть сгенерированы и сохранены на стороне управляющего сервера, так и локально на стороне программы-шифровальщика.

Для шифрования данных могут использоваться следующие сценарии:

- симметричного шифрования;
- асимметричного шифрования;
- гибридного шифрования, при котором содержимое файлов шифруется с использованием симметричного ключа, затем этот ключ шифруется открытым ключом из ассиметричной пары.

Программы-шифровальщики наиболее часто используют асимметричное и гибридное шифрование.

IV) Шифрование данных. Данный этап является основным для всех программ-шифровальщиков и заключается в блокировке оригинальных документов путём перезаписи их содержимого зашифрованными фрагментами.

Для ускорения этого этапа и сокращения использования ресурсов центрального процессора отдельные примеры программ-шифровальщиков изменяют фиксированное число байт в каждом файле, без изменения оставшейся части файла.

Рабочие документы пользователей, созданные с использованием пакета программ Microsoft Office уязвимы к таким атакам. Соответствующие файловые форматы docx и pptx включают в себя так называемые заголовки, обычно занимающие первые байты файла и хранящие информацию о бинарной структуре файла. Изменение такого заголовка блокирует доступ ко всему файлу, поскольку соответствующие программы-редакторы пакета программ Microsoft Office не могут работать с повреждёнными файлами. В результате пользователь теряет возможность читать и вносить изменения в рабочие файлы. Программы-шифровальщики также могут менять имя файла и изменять его расширение.

V) Этап вымогательства.

На финальном этапе программа-шифровальщик сообщает о выполненных вредоносных манипуляциях в системе и заявляет о требованиях, которые необходимо выполнить пользователю для восстановления изменённых файлов. Как правило, в требованиях указан перевод денежных средств на счета нарушителей с использованием децентрализованных платёжных систем.

Требования нарушителей могут быть предоставлены одним из следующих способов:

- текстовые файлы;
- HTML-документы;
- графические файлы различных форматов.

В ряде случаев программы-шифровальщики создают файлы с требованиями о выкупе в каждом каталоге с зашифрованными файлами [2].

1.1.1 Результаты анализа недавних атак программ-шифровальщиков

В ходе анализа популярных программ-шифровальщиков [3–7], таких как WannaCry, Locky, Ryuk, GandCrab, Coronavirus, Hive были выявлены их основные особенности приведенные в табл. 1.

Таблица 1. Результаты сравнения популярных программ-шифровальщиков

Название, год	**Операционная система**	**Тип заражения**	**Используемый алгоритм шифрования**
WannaCry, 2017	Windows	С помощью уязвимости EternalBlue	AES и RSA
Locky, 2017	Windows	Фишинг	AES
Ryuk, 2018	Кроссплатформенный	С помощью протокола удалённого доступа	AES и RSA
GandCrab, 2018	Кроссплатформенный	Фишинг	AES
CoronaVirus, 2020	Windows	Фишинг	AES и RSA
Hive, 2021	Кроссплатформенный	Фишинг	RSA

1.1.2 Особенность работы программ-шифровальщиков

В ходе анализа популярных программ-шифровальщиков была выявлена следующая особенность их работы. На этапе шифрования программа-шифровальщик совершает значительно большее число файловых операций, чем остальные работающие процессы в ОС за одинаковый промежуток времени. На рис. 2 продемонстрировано, что программа-шифровальщик под условным номером 1 совершает 2954 файловых операций, в то время как остальные легитимные программы генерируют не более 1300 файловых операций. Отмеченный рост файловых операций может быть использован для обнаружения программ-шифровальщиков.

Рис. 2. Количество файловых операций, генерируемых работающими процессами
Fig. 2. The number of files actions generated by running processes

1.2 Индикаторы обнаружения программ-шифровальщиков

Помимо отмеченного роста файловых операций, программы-шифровальщики также могут быть обнаружены с учётом их следующих признаков:

- увеличение числа вновь созданных файлов;
- увеличение числа удаленных файлов;
- увеличение числа переименованных файлов, а также файлов с изменённым расширением;
- увеличение операций чтения и записи для файлов, находящихся в одной папке;
- значительное замедление работы ОС;
- изменение обоев рабочего стола устройства;
- появление на экране явного уведомления о выкупе.

В данной работе использованы индикаторы, связанные с взаимодействием с файловой системой. Также можно выделить четыре общих особенности, которые характеризуют поведение большинства семейств программ-шифровальщиков, табл. 2.

Таблица 2. Примеры взаимодействия с файлами для различных программ-шифровальщиков

Название программ-шифровальщиков	**Примеры взаимодействия с файлами для программ-шифровальщиков**
Cerber, Keypass, Telsacrypt, Gandcrab	Преобразование файла с последующим изменением его имени: файл сначала перезаписывается зашифрованными данными пользователя, затем изменяется имя файла.
Locky	Преобразование файла с предварительным изменением его имени: эта особенность аналогична предыдущей, за исключением того, что сначала файл переименовывается, а затем перезаписывается.
InfinityCrypt, Dharma, Malevich, Sage, Syrk, WannaCry	Копирование исходного файла в новый файл с удалением старого: сначала создаётся новый файл и в него копируются зашифрованные данные исходного файла, после исходный файл удаляется.

1.3 Сравнительный анализ существующих способов обнаружения программ-шифровальщиков

На рис. 3 представлена систематизация существующих способов обнаружения программ-шифровальщиков.

Рис. 3. Систематизация способов обнаружения программ-шифровальщиков
Fig. 3. Systematization of the processes of detecting encryption programs

Способы обнаружения могут быть условно разделены на две группы: с использованием статического анализа и динамического анализа. С помощью статического анализа можно обнаружить программы-шифровальщиков с использованием файловых сигнатур. Динамический анализ позволяет извлекать и обрабатывать информацию о работающей программе [8].

Программы-шифровальщики могут использовать различные приёмы для противодействия своему обнаружению. Например, с помощью техник обфускации программа-шифровальщик может скрыться от сигнатурных средств обнаружения [9].

Обнаружение с помощью динамического анализа лишены таких недостатков и является более перспективным. Способы обнаружения вредоносных программ на основе машинного обучения принимают решение о наличии программ-шифровальщиков с помощью моделей, которые построены с использованием набора аналитических функций. Системы обнаружения программ-шифровальщиков на основе машинного обучения используют структурные особенности программ и их поведенческие особенности.

В данной работе был выбран способ обнаружения на основе машинного обучения с использованием поведенческих особенностей, связанных с взаимодействием программ с файловой системой. Были выбраны следующие индикаторы обнаружения, основанные на увеличении таких файловых манипуляций, как удаление файла, переименование файла, создание нового файла, запись в файл.

2. Обнаружение программ-шифровальщиков с помощью механизма логирования событий ETW

Для сбора информации о файловых операциях в режиме реального времени в ОС Windows можно использовать ряд инструментов:

- Драйвер-фильтр файловой системы.
- Гипервизор на базе аппаратной виртуализации.
- Механизм трассировки событий Windows Event Tracing for Windows (ETW).

Драйвер-фильтр файловой системы добавляется в стек драйверов и получает уведомления о каждом файловом событии. В недавних ОС Windows для установки сторонних драйверов необходима цифровая подпись, что не всегда удобно.

Использование возможностей гипервизоров требует наличия поддержки аппаратной виртуализации, что доступно только в современных компьютерных системах.

Механизм трассировки событий Windows Event Tracing for Windows (ETW) исключает указанные недостатки: не требует установки драйверов, переносим на различные ОС семейства Windows и поддерживает широкий спектр регистрируемых событий ОС [10]. В работе был выбран механизм ETW для сбора информации о файловых событиях в режиме реального времени.

2.1 Анализ возможностей ETW

Механизм трассировки событий Windows Event Tracing for Windows (ETW) был добавлен во все версии ОС Windows, начиная в Windows 2000. ETW был изначально реализован для выявления ошибок и «узких мест» в программе. В настоящее время ETW используется различными средствами защиты информации для получения информации о событиях ОС.

Механизм ETW может регистрировать различные события ОС, такие как: выполненные системные вызовы, операции доступа к реестру Windows и файловой системе, данные о сетевом взаимодействии.

ETW состоит из четырёх компонентов:

- ETW-сессия – это объект ОС создаваемый ETW-контроллером для сбора заданных событий ОС – создание, настройку, запуск и остановку ETW-сессии;
- поставщики событий – это прикладные программы и драйверы, которые создают ETW-события и пересылают информацию потребителям событий;
- потребители событий – это прикладные программы и драйверы, которые получают сгенерированные события.

Например, программа Process Monitor из пакета программ Windows Sysinternals получает события о взаимодействии программ с сетью с использованием ETW. В работе события регистрируются в режиме реального времени [11].

3. Разработка системы обнаружения программ-шифровальщиков

Разработанная система обнаружения использует информацию о новых событиях ОС от механизма ETW и с помощью обработки собранной информации методами машинного обучения принимает решение о присутствии программ-шифровальщиков. Алгоритм работы программы представлен на рис. 4.

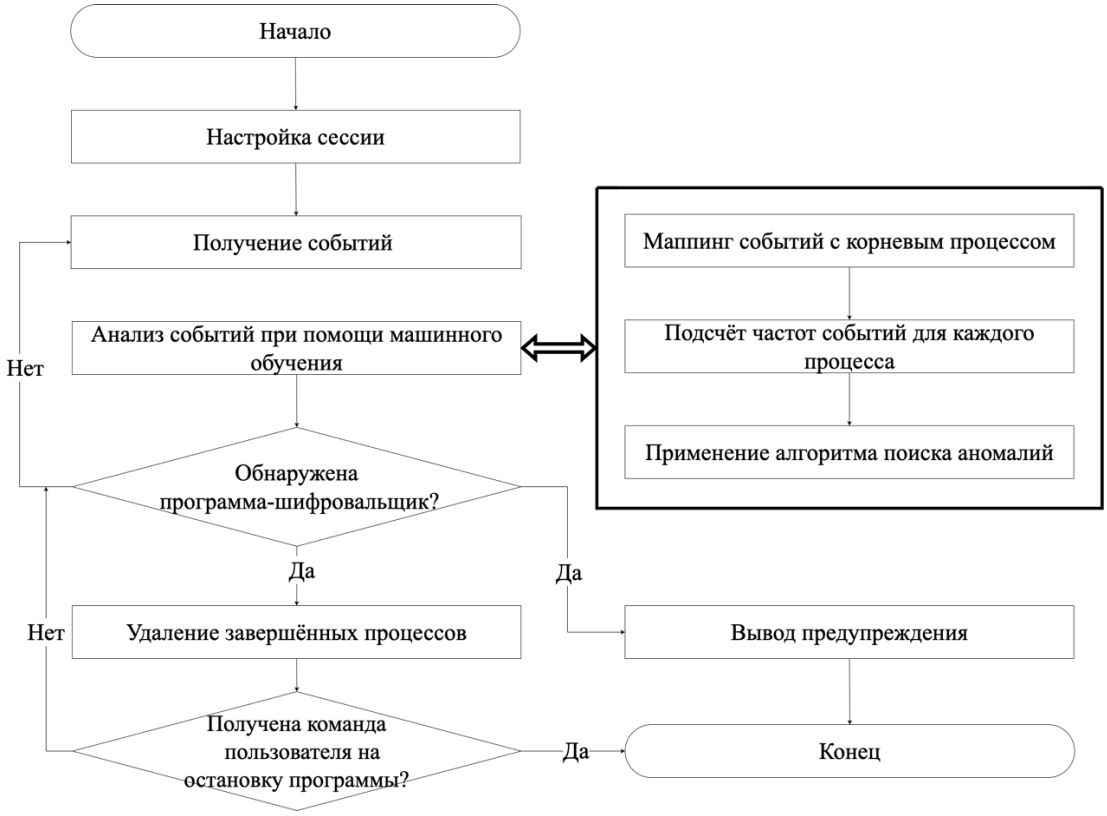

Рис. 4. Алгоритм работы программы
Fig. 4. The algorithm of the program

Для получения информации о файловых событиях были использованы возможности встроенного поставщика событий Microsoft-Windows-Kernel-File. Соответствующая сессия была запущена с использованием библиотеки PyWinTrace, которая предоставляет интерфейс для настройки и управления ETW-сессиями. Отдельные регистрируемые события сохраняются в формате json в файле журнала на жёстком диске, который можно преобразовать в формат csv для удобства дальнейшей обработки массивов данных (выборкой).

3.1 Разработка ПО

Программная реализация разработанного алгоритма была выполнена в среде разработки PyCharm для Windows 10 на языке Python 3 [12].

Для получения обучающей выборки из событий ПО необходимо собрать файловые события, генерируемые программами-шифровальщиками. Для того, чтобы безопасно получить такие события было разработано ПО, реализующее алгоритмы действий с файловой системой, основанное на популярных программах-шифровальщиках. Разработанное демонстрационное ПО осуществляло шифрование файлов только в одной из заданных папок, например, «D:\test». Были реализованы следующие наборы событий, наиболее часто встречающиеся в программах-шифровальщиках:

- переименование исходного файла, запись зашифрованных данных в исходный файл;
- запись зашифрованных данных в исходный файл (без переименования исходного файла);
- создание нового файла, запись зашифрованных данных в новый файл, удаление исходного файла.

3.2 Создание набора данных для классификатора

Для создания набора данных (датасета) последовательно запускались популярные программы-шифровальщики и сборщик событий, в результате работы был получен журнал событий в формате .json. Вручную были помечены ID процессов (pid) для программ-шифровальщиков единицей, для остальных легитимных процессов – нулём. Эти действия повторяются для всех наборов программ-шифровальщиков. Каждая программа-шифровальщик запускалась 16 раз. Фрагмент обучающей выборки представлен на рис. 5.

	pid	label	OPERATIONEND	24	CLOSE	14	CREATE	12	QUERYSECURITY	32	FSCTL	23	QUERYINFORMATION
0	6848 - 0	1.0	1551.0	1551.0	174.0	174.0	154.0	154.0	76.0	76.0	152.0	152.0	343.0
1	4796 - 0	0.0	462.0	462.0	67.0	67.0	67.0	67.0	0.0	0.0	105.0	105.0	150.0
2	27068 - 0	0.0	7.0	7.0	2.0	2.0	2.0	2.0	0.0	0.0	0.0	0.0	1.0
3	22156 - 0	0.0	107.0	107.0	0.0	0.0	8.0	8.0	4.0	4.0	0.0	0.0	40.0
4	20196 - 0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
5	4 - 0	0.0	550.0	550.0	527.0	527.0	1.0	1.0	0.0	0.0	30.0	30.0	0.0
6	3620 - 0	0.0	249.0	249.0	39.0	39.0	51.0	51.0	8.0	8.0	4.0	4.0	79.0
7	9712 - 0	0.0	243.0	243.0	37.0	37.0	43.0	43.0	8.0	8.0	0.0	0.0	34.0
8	23576 - 0	0.0	2.0	2.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	2.0
9	16392 - 0	0.0	86.0	86.0	17.0	17.0	17.0	17.0	0.0	0.0	0.0	0.0	35.0
10	2180 - 0	0.0	6.0	6.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

Рис. 5. Фрагмент обучающей выборки
Fig. 5. Fragment of the training sample

Параметры, необходимые для составления обучающей выборки:

- pid – id процесса;
- 0, 1, 2, … ,15 – номер журнала событий в формате .json;
- label – метка (1– программа-шифровальщик, 0 – обычный процесс);
- данные о файловой активности, полученные от ETW: operationend, close, create, querysecurity, queryinformation, cleanup, read, dirnotify, createnewfile, write, namecreate, setinformation, rename, renamepath, namedelet, setdelet, deletpath, direnum, queryea, flush, setsecurity.

3.3 Обучение классификатора

Для обучения и тестирования использовалось следующее разделение: обучающая выборка (30%), тестовая выборка (70%).

Для обучения модели, было принято решение использовать алгоритмы обнаружения аномалий, что позволило решить задачу классификации на выборках с крайне неравномерным распределением классов. Для обучения классификатора были тестированы следующие алгоритмы:

- OneclassSVM (Метод опорных векторов для одного класса) [13];
- IsolationForest (Изолирующий лес) [14];
- LocalOutlierFactor (Локальный фактор выбросов) [15].

Каждый из алгоритмов запускался по 10 раз, в табл. 3 представлены наилучшие результаты каждого из алгоритмов.

В ходе тестов лучше всего себя показал алгоритм Isolation Forest. Далее эта модель была использована в работе в качестве основной.

Таблица 3. Результаты тестирования алгоритмов машинного обучения

Алгоритмы машинного обучения	**Процессы программ-шифровальщиков (12 процессов)**		**Легитимные процессы (119 процессов)**	
	Precision	Recall	Precision	Recall
One Class Support Vector Machines (одноклассовый метод опорных векторов)	0,31	0,83	0,98	0,82
Isolation Forest (алгоритм изолирующего леса)	1	1	1	1
Local Outlier Factor (алгоритм локального уровня выброса)	0,11	0,17	0,91	0,86

3.4 Тестирование системы обнаружения программ-шифровальщиков

Тестирование происходило в два этапа:

- тестирование с целью проверки обнаружения существующих программ-шифровальщиков;
- тестирование с целью проверки отсутствия ложноположительных срабатываний на легитимных программах.

При обнаружении программы-шифровальщика выводится предупреждение, которое представлено на рис. 6.

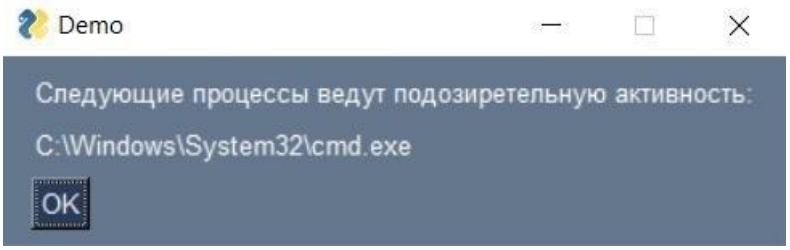

Рис. 6. Вывод предупреждения
Fig. 6. Warning output

В ходе тестирования были успешно обнаружены следующие известные программы-шифровальщики: Wannacry и TeslaCrypt.

Число файлов, зашифрованных программой-шифровальщиком WannaCry до момента обнаружения, составляет 15 файлов. TeslaCrypt до момента обнаружения успевает зашифровать 10 файлов пользователя. Эти результаты являются приемлемыми, так как уменьшение порогового значения числа зашифрованных файлов приведёт к увеличению ложноположительных срабатываний.

Для тестирования с целью проверки отсутствия ложноположительных срабатываний использовалось следующее ПО:

- программы для создания виртуальных дисков и шифрования на «лету»: TrueCrypt и VeraCrypt;
- программные пакеты Microsoft Office;
- система управления реляционными базами данных Oracle;
- файловый архиватор 7z;
- встроенное в ОС Windows средство для дефрагментации диска.

В результате тестирования ложноположительных срабатываний не выявлено.

Все тесты проводились, для операционной системы Windows 10 x64. Также возможна адаптация разработанного средства обнаружения программ-шифровальщиков на Windows 10 x32, Windows 11 x64/x32 и Windows 7 x64/x32.

Заключение

В работе был выполнен анализ популярных программ-шифровальщиков, проведён сравнительный анализ существующих способов обнаружения программ-шифровальщиков. Выявлена особенность работы программ-шифровальщиков, заключающая в резком росте файловых операций, таких как создание, переименование, перезапись и удаление, что позволило разработать систему обнаружения.

Для сбора информации о работающих процессах и их файловых операциях был использован механизм ETW. Собранные данные обрабатывались методами машинного обучения. Разработано ПО, реализующее алгоритмы взаимодействия с файловой системой, основанные на популярных программах-шифровальщиках.

При обучении классификатора решалась задача поиска аномалий. В ходе тестирования алгоритм Isolation Forest (Изолирующий лес) показал высокую точность обнаружения и малое количество ложноположительных срабатываний относительно остальных алгоритмов, и был взят за основу при разработке средства обнаружения программ-шифровальщиков.

В ходе тестирования разработанного средства были успешно обнаружены следующие образцы программ-шифровальщиков: Wannacry и TeslaCrypt. В ходе тестирования ложноположительных срабатываний выявлено не было.

СПИСОК ЛИТЕРАТУРЫ:

1. CYBER THREAT REPORT, 2022. URL: https://www.infopoint-security.de/media/2022-sonicwall-cyber-threat-report.pdf (дата обращения: 20.02.2022).
2. A Survey on Detection Techniques for Cryptographic Ransomware, 2019. URL: http://dataset.tlm.unavarra.es/ransomware/articles/IEEEAccess.pdf (дата обращения: 20.02.2022).
3. Analyzing WannaCry Ransomware Considering the Weapons and Exploits, 2022. URL: https://icact.org/upload/2018/0708/20180708_finalpaper.pdf (дата обращения: 20.02.2022).
4. Threat spotlight: the curious case of Ryuk ransomware, 2019. URL: https://blog.malwarebytes.com/threat-spotlight/2019/12/threat-spotlight-the-curious-case-of-ryuk-ransomware/ (дата обращения: 20.02.2022).
5. RYUK RANSOMWARE, 2021. URL: https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-006.pdf (дата обращения: 20.02.2022).
6. Digital CoronaVirus: Yet Another Ransomware Combined with Infostealer, 2020. URL: https://www.acronis.com/en-us/blog/posts/digital-coronavirus-yet-another-ransomware-combined-infostealer/ (дата обращения: 20.02.2022).
7. Hive Attacks. Analysis of the Human-Operated Ransomware Targeting Healthcare, 2021. URL: https://www.sentinelone.com/labs/hive-attacks-analysis-of-the-human-operated-ransomware-targeting-healthcare/ (дата обращения: 20.02.2022).
8. A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions, 2022. URL: https://arxiv.org/pdf/2102.06249.pdf (дата обращения: 20.02.2022).
9. Advances In Malware Detection-An Overview, 2021. URL: https://arxiv.org/pdf/2104.01835.pdf (дата обращения: 20.02.2022).
10. Peeler: Profiling Kernel-Level Events to Detect Ransomware, 2020. URL: https://ndss21-summer.hotcrp.com/doc/ndss21-summer-paper121.pdf?cap=0121aPNQ0EBTM4to (дата обращения: 12.12.2020).
11. A Comparison of Malware Detection Techniques Based on Hidden Markov Model, 2016. URL: https://www.scirp.org/pdf/JIS_2016042209291406.pdf (дата обращения: 20.02.2022)
12. Kalinkin A. Ransomware detection, 2022. URL: https://github.com/kalinkinartem1/Ransomware-detection (дата обращения: 20.02.2022).

13. Introduction to One-class Support Vector Machines, 2013. URL: http://rvlasveld.github.io/blog/2013/07/12/introduction-to-one-class-support-vector-machines/ (дата обращения: 20.02.2022).
14. Anomaly detection using Isolation Forest – A Complete Guide, 2021. URL: https://www.analyticsvidhya.com/blog/2021/07/anomaly-detection-using-isolation-forest-a-complete-guide/ (дата обращения: 20.02.2022).
15. Anomaly Detection Techniques in Python, 2019. URL: https://medium.com/learningdatascience/anomaly-detection-techniques-in-python-50f650c75aaf (дата обращения: 20.02.2022).

REFERENCES:

[1] CYBER THREAT REPORT, 2022. URL: https://www.infopoint-security.de/media/2022-sonicwall-cyber-threat-report.pdf (accessed: 20.02.2022).
[2] A Survey on Detection Techniques for Cryptographic Ransomware, 2019. URL: http://dataset.tlm.unavarra.es/ransomware/articles/IEEEAccess.pdf (accessed: 20.02.2022).
[3] Analyzing WannaCry Ransomware Considering the Weapons and Exploits, 2022. URL: https://icact.org/upload/2018/0708/20180708_finalpaper.pdf (accessed: 20.02.2022).
[4] Threat spotlight: the curious case of Ryuk ransomware, 2019. URL: https://blog.malwarebytes.com/threat-spotlight/2019/12/threat-spotlight-the-curious-case-of-ryuk-ransomware/ (accessed: 20.02.2022).
[5] RYUK RANSOMWARE, 2021. URL: https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-006.pdf (accessed: 20.02.2022).
[6] Digital CoronaVirus: Yet Another Ransomware Combined with Infostealer, 2020. URL: https://www.acronis.com/en-us/blog/posts/digital-coronavirus-yet-another-ransomware-combined-infostealer/ (accessed: 20.02.2022).
[7] Hive Attacks. Analysis of the Human-Operated Ransomware Targeting Healthcare, 2021. URL: https://www.sentinelone.com/labs/hive-attacks-analysis-of-the-human-operated-ransomware-targeting-healthcare/ (accessed: 20.02.2022).
[8] A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions, 2022. URL: https://arxiv.org/pdf/2102.06249.pdf (accessed: 20.02.2022).
[9] Advances In Malware Detection-An Overview, 2021. URL: https://arxiv.org/pdf/2104.01835.pdf (accessed: 20.02.2022).
[10] Peeler: Profiling Kernel-Level Events to Detect Ransomware, 2020. URL: Режим доступа: https://ndss21-summer.hotcrp.com/doc/ndss21-summer-paper121.pdf?cap=0121aPNQ0EBTM4to (accessed: 12.12.2020).
[11] A Comparison of Malware Detection Techniques Based on Hidden Markov Model, 2016. URL: https://www.scirp.org/pdf/JIS_2016042209291406.pdf (accessed: 20.02.2022).
[12] Kalinkin A. Ransomware detection, 2022. URL: https://github.com/kalinkinartem1/Ransomware-detection (accessed: 20.02.2022).
[13] Introduction to One-class Support Vector Machines, 2013. URL: http://rvlasveld.github.io/blog/2013/07/12/introduction-to-one-class-support-vector-machines/ (accessed: 20.02.2022).
[14] Anomaly detection using Isolation Forest – A Complete Guide, 2021. URL: https://www.analyticsvidhya.com/blog/2021/07/anomaly-detection-using-isolation-forest-a-complete-guide/ (accessed: 20.02.2022).
[15] Anomaly Detection Techniques in Python, 2019. URL: https://medium.com/learningdatascience/anomaly-detection-techniques-in-python-50f650c75aaf (accessed: 20.02.2022).

Поступила в редакцию – 17 июля 2022 г. Окончательный вариант – 01 сентября 2022 г.
Received – July 17, 2022. The final version – September 01, 2022.

Виктор С. Горбатов[1], Дмитрий А. Дятлов[2], Александр Н. Рыжиков[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: Alexander.ryzhikov.work@gmail.com, https://orcid.org/0000-0001-8831-938X

МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ АВТОМАТИЗАЦИИ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ ДЛЯ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

DOI: http://dx.doi.org/10.26583/bit.2022.3.08

Аннотация. В статье рассматривается существующая нормативно-методическая база, определяющая актуальность проблемы тестирования на проникновение, основные методики тестирования значимых объектов критической информационной инфраструктуры (КИИ). Обеспечение безопасности значимых объектов КИИ с целью их устойчивого функционирования является приоритетной задачей государственного регулирования в области информационной безопасности России. В настоящее время сформировано отдельное направление организационно-правового обеспечения безопасности КИИ на основе соответствующей новой нормативно-правовой базы. Значительно меньшее внимание уделяется вопросам инструментального (технического) обеспечения указанного направления, так как объекты КИИ с технологической точки зрения – это традиционные средства информационных технологий. С учетом нынешней сложной, в том числе международной, ситуации, своевременное инструментальное обнаружение и выявление многочисленных уязвимостей позволит улучшить защищенность критической информационной инфраструктуры. Существующие способы проведения аудита безопасности, а также тестирования защищенности объектов КИИ от угроз на проникновение обладают определенными недостатками, такими как трудоемкость, большие временные и материальные затраты, а также острая нехватка квалифицированных специалистов. Достаточно очевидным, хотя и очень сложным, способом решения указанной проблемы является автоматизация процесса тестирования на проникновение как важнейшей составной части мероприятий по обеспечению безопасности значимых объектов КИИ. Методологические аспекты создания автоматизированного программного комплекса тестирования на проникновение являются основной целью проведенных исследований на основе аналитического обзора основных подходов и способов реализации поставленной выше задачи. В результате исследования определены основные методологические аспекты указанной проблемы, в том числе обозначены специфические особенности для объектов КИИ. Полученные результаты могут быть использованы для разработки подобных программных комплексов безопасности для любых объектов информатизации.

Ключевые слова: аудит безопасности, информационная безопасность, критическая информационная инфраструктура, объект, тестирование на проникновение, уязвимость.
Для цитирования: ГОРБАТОВ, Виктор С.; ДЯТЛОВ, Дмитрий А.; РЫЖИКОВ, Александр Н. МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ АВТОМАТИЗАЦИИ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ ДЛЯ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ. Безопасность информационных технологий, [S.l.], т. 29, № 3, с. 94–104, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1439. DOI: http://dx.doi.org/10.26583/bit.2022.3.08.

Victor S. Gorbatov[1], Dmitriy A. Dyatlov[2], Aleksander N. Ryzhikov[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: Alexander.ryzhikov.work@gmail.com, https://orcid.org/0000-0001-8831-938X

Methodological aspects of penetration testing automation for significant objects of critical information infrastructure

DOI: http://dx.doi.org/10.26583/bit.2022.3.08

Abstract. The paper deals with the existing regulatory and methodological framework that determines the importance of the problem of penetration testing as well as the main methods of testing significant objects of critical information infrastructure (CII). Ensuring the security of significant CII facilities for the purpose of their sustainable operation is the high priority task of state regulation in the field of information security of Russia. Currently, a separate direction of organizational and legal support for the safety of CII has been formed on the basis of the corresponding new regulatory framework. Much less attention is paid to the issues of instrumental (technical) support of this direction, since the objects of CII from a technological point of view are traditional means of information technology. Taking into account the current uneasy international situation, timely instrumental detection and identification of numerous vulnerabilities allows improving the security of critical information infrastructure. Existing methods of conducting a security audit, as well as testing the protection of CII objects from penetration threats, have certain drawbacks, such as laboriousness, large time and material costs, as well as an acute shortage of qualified specialists. A fairly obvious, although very complex, way to solve this problem is to automate the penetration testing process as an important part of measures to ensure the safety of significant CII objects. Methodological aspects of creating an automated software complex for penetration testing are the main purpose of the study conducted on the basis of an analytical review of the main approaches and ways to implement the above task. As a result of this study the main methodological aspects of this problem have been determined, including specific features for CII objects. The obtained results can be used to develop similar security software systems for any objects of informatization.

Keywords: security audit, information security, critical information infrastructure, facility, penetration testing, vulnerability.

For citation: GORBATOV, Victor S.; DYATLOV, Dmitriy A.; RYZHIKOV, Aleksander N. Methodological aspects of penetration testing automation for significant objects of critical information infrastructure. IT Security (Russia), [S.l.], v. 29, no. 3, p. 94-104, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1439. DOI: http://dx.doi.org/10.26583/bit.2022.3.08.

Введение

Увеличение компьютерных инцидентов во всем мире в отношении критической информационной инфраструктуры (КИИ) [1] актуализирует проблему обеспечения ее защищенности и устойчивого функционирования, выводя вопросы ее решения на государственный уровень. Законодательное выделение в отдельную категорию объектов КИИ, требующих безусловного обеспечения устойчивости критических процессов в организациях и в производственных отраслях, дало новый импульс в развитие отечественной отрасли информационной безопасности (ИБ) в целом [2], выделив, в то же время, это направление в отдельный важнейший аспект государственного регулирования.

В соответствии с известной методологией [3] реализация угроз безопасности (инцидентов) возможна при наличии тех или иных уязвимостей на объектах информатизации, в том числе и КИИ [2]. Для их выявления нормативно задана необходимость применения нескольких способов[1], одним из которых является тестирование на проникновение. В данной статье рассматриваются общие аспекты этого способа тестирования и его особенности применительно к вопросу обеспечения безопасности объектов КИИ.

За прошедшее пятилетие накоплен существенный отечественный опыт обеспечения безопасности объектов КИИ, прежде всего, по разработке и совершенствованию

[1]Приказ Федеральной службы по техническому и экспортному контролю от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

нормативно-методической базы в этой области [4]. Существующие нормативные требования по обеспечению безопасности значимых объектов КИИ в основном предполагают создание систем менеджмента ИБ на основании различных политик безопасности и дальнейшее выполнение обозначенных требований [5]. В свою очередь политики безопасности разрабатываются, исходя из существующих нормативно-правовых документов и методических рекомендаций, которые регулярно обновляются с учетом вновь обнаруживаемых угроз и выявляемых уязвимостей [6]. Другими словами, обновление и изменение систем безопасности информации, в том числе и КИИ, происходит, как правило, по итогам произошедших инцидентов. Однако, при формировании новых способов выявления уязвимостей КИИ необходимо отдавать предпочтение методам превентивного противодействия компьютерным атакам на основе технических средств защиты информации [7].

Как отмечено выше, одним из нормативно заданных способов противодействия является тестирование на проникновение при аудите безопасности объектов КИИ. В [6, 8] показаны такие достоинства данного способа как:

– выявление уязвимостей до их обнаружения злоумышленником;
– контролирование обновлений программного обеспечения;
– использование более широкого диапазона способов и средств противодействия деструктивному воздействию на объекты КИИ.

На практике при тестировании на проникновение для оценки защищенности информационных ресурсов используются различные методы и модельные представления, не имеющие, однако системного подхода [9]. Кроме этого, там же отмечено, что используемые методики тестирования не ориентированы на формирование базовой модели оценки защищенности информационных ресурсов КИИ.

Поэтому именно выделение отличительных характеристик данного способа выявления уязвимостей для формирования модельного представления тестирования на проникновение в сфере КИИ и является основной целью данной статьи.

Первая и вторая части работы посвящены обзору основной нормативно-методической базы, в том числе рассмотрены методики проведения тестирования на проникновение объектов информатизации в аспекте автоматизации данного процесса.

В третьей части описываются основные термины и определения исследуемой методологии тестирования на проникновение, взаимосвязанные с вопросами безопасности объектов КИИ. Кроме этого, определены основные характерные черты соответствующего модельного представления.

Изложенные результаты показывают значимость тестирования на проникновение на безопасность объектов КИИ и актуальность использования для этой цели автоматизированных инструментальных средств.

1. Уязвимости объектов информатизации

Нормативные требования по обеспечению безопасности объектов КИИ предполагают проведение организационных и технических мероприятий в отношении каждого значимого объекта КИИ на всех этапах жизненного цикла. Наиболее значимым из них является анализ уязвимостей объекта КИИ, на основании которого и выстраивается система защиты в соответствии с присвоенной категорией.

Определение понятия уязвимости дано в стандарте ГОСТ Р 50922–2006[2] как свойство информационной системы, обусловливающее возможность реализации угроз

[2]ГОСТ Р 50922–2006. Защита информации. Основные термины и определения.

безопасности обрабатываемой в ней информации. В ГОСТ Р 56546–2015[3] дается классификация уязвимостей информационных систем по критериям области происхождения уязвимости, по типам недостатков информационных систем и месту возникновения. Анализ указанных «хороших практик» показывает существенную сложность решения задачи поиска уязвимостей из-за большого количества различных типов уязвимостей, отличающихся не только по степени влияния, но и по своей природе.

Как известно [10], любая угроза безопасности информации в общем виде описывается через предполагаемый результат реализации, выраженный в нарушении конфиденциальности, целостности или доступности информации. Таким образом, качество и полнота модели угроз безопасности объекта КИИ и, соответственно, его категория защиты зависят от полноты оценки и анализа уязвимостей в системе защиты информации информационной системы.

Стандарт ГОСТ Р ИСО/МЭК 15408–1–2012[4] напрямую устанавливает необходимость проведения различных мероприятий по выявлению уязвимостей информационной системы для определения уровня информационной безопасности. ГОСТ Р 58143–2018[5] вводит определение тестирования на проникновение, дополняя предыдущий стандарт, и формализуя процесс поиска уязвимостей.

Отсюда следует вывод, что проведение анализа уязвимостей является одной из основных составляющих процесса обеспечения безопасности информационной системы, а тестирование на проникновение можно использовать для реализации данного способа, в том числе и для значимых объектов КИИ.

За основу для исходных данных анализа уязвимостей можно взять банк данных угроз безопасности информации ФСТЭК России, который на настоящее время насчитывает свыше 40 тысяч уязвимостей. Но, тем не менее, очевидным фактором повышения реального уровня защищенности объектов КИИ является применение инструментальных методов и средств тестирования.

2. Методики тестирования на проникновение

Выделим две наиболее известные методики тестирования на проникновение.

Первая представлена американским национальным институтом стандартизации NIST (National Institute of Standards and Technology) в виде технического руководства по тестированию и оценке ИБ NIST SP 800–115[6] Но, по существу данный стандарт надо рассматривать как методологию, предлагающую широкий спектр методов по оценке ИБ, основной частью которой является тестирование на проникновение [11]. Эта часть включает три основные группы техник:

1) техники обзора проверки ИБ;
2) техники идентификации и анализа информационных систем;
3) техники проверки информационных систем на наличие уязвимостей.

[3]ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 19 августа 2015 г. N 1181-ст)

[4]ГОСТ Р ИСО/МЭК 15408-1-2012. Методы и средства обеспечения безопасности. критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

[5]ГОСТ Р 58143–2018. Информационная технология. Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045. Часть 2. Тестирование проникновения.

[6] NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment (NIST SP 800-115). – Computer Security Resource Center, 2008. – 80 p.– URL: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf (дата доступа 20.08.2022).

Техники первой группы собирают и анализируют первичную информацию об информационной системе и могут включать:

– обзор документации (политики безопасности и архитектуры, требования безопасности, планы безопасности, планы реагирования на инциденты и т.п.), результаты которого можно использовать для более точной настройки других методов тестирования;

– обзор сервисных журналов (например, системные журналы или журналы сервера аутентификации, журналы обнаружения и предотвращения вторжений, журналы межсетевого экрана и т.п.), определяющий регистрацию достоверной информации элементами управления безопасностью и соблюдение организацией политики управления журналами (часто для проверки журналов предлагается использование автоматических средств);

– обзор правил (исследование набора правил или сигнатур для сетевого трафика или системной активности, в том числе, списков доступа на маршрутизаторах, правил межсетевого экрана и правил системы обнаружения вторжений), используемый для выявления уязвимостей (слабых мест) устройств безопасности и во всех многоуровневых средствах защиты;

– обзор конфигурации системы (сравнение настроек системы с требованиями безопасности для данной системы, либо с требованиями, определенными в стандартах), применяемый при поиске уязвимостей в элементах управления конфигурацией безопасности;

– анализ сетевой активности (отслеживание потока пользователей, декодирование протоколов, проверка заголовков и полезных данных для отслеживания интересующей информации), используемый для дальнейшего анализа другими методами.

Техники идентификации и анализа информационных систем ориентированы на задание активных устройств и, связанных с ними, портов и служб с целью дальнейшего анализа на предмет потенциальных уязвимостей. Эта информация нужна для дальнейшего исследования информационных систем на наличие уязвимостей. Техники этой группы включают:

– исследование сети (используются различные методы, список которых постоянно пополняется, предполагается использование автоматических средств), в результате чего появляется информация об устройствах сети, которая является входными данными для следующей техники;

– идентификация портов и сервисов позволяет определить открытые порты и службы, запущенные на устройствах сети, выявленные на предыдущих этапах (данная информация может быть получена в рамках других техник, например, в процессе анализ сетевой активности);

– сканирование на уязвимости, предполагающее использование автоматизированных процедур, что являются основными техниками тестирования на проникновение.

Методы тестирования на проникновение представлены в последней группе техник проверки на наличие уязвимостей.

В руководстве NIST тестирование на проникновение определяется, как тестирование безопасности, в ходе которого имитируются реальные атаки с целью определения способов обхода защитных функций объекта информатизации. Тесты на проникновение включают поиск в проверяемой системе нескольких уязвимостей для того, чтобы провести на эту систему большее количество атак, чем в случае использования только одной уязвимости.

Алгоритм тестирования на проникновение по указанной методике, представленный на рис. 1, подразделяется на четыре этапа:

– планирования, на котором определяются правила и устанавливаются цели тестирования (фактические испытания на этом этапе не проводятся);

– обнаружения, состоящий из сбора информации о системе и анализа уязвимостей;

– имитации атаки как основного этапа тестирования, на котором имитируются действия нарушителя и подтверждаются уязвимости, выявленные на предыдущем этапе (при выявлении новой информации о системе, дополнительные данные используются для дальнейшего исследования истинного риска для объекта информатизации);

– составления отчета, которое проходит перманентно с другими этапами на протяжении всего процесса тестирования, по окончании которого оформляется итоговый отчет.

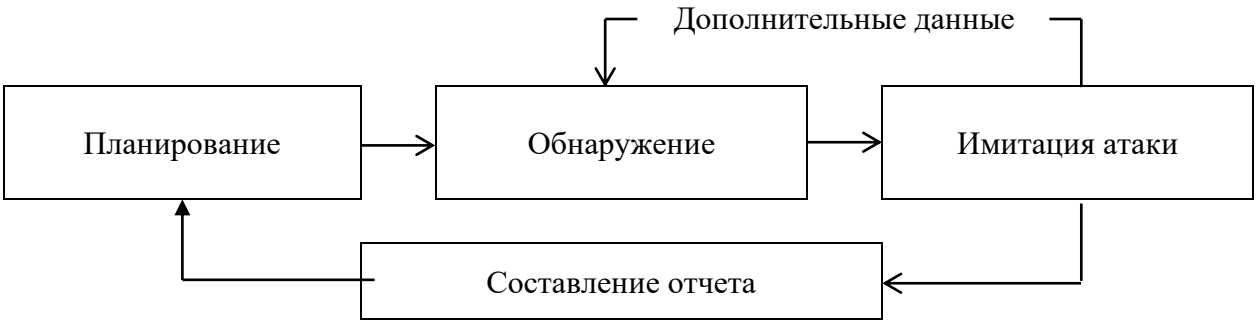

Рис. 1. Схема тестирования на проникновения по методике NIST
Fig. 1. NIST Penetration Testing Scheme

Таким образом, после анализа технического руководства по тестированию и оценке информационной безопасности NIST SP 800–115, можно сделать следующие выводы:

– тестирование на проникновение применяется как основной метод оценки ИБ;

– дополнительные данные, полученные на этапе имитации атаки и используемые в дальнейшем, повышают достоверность проводимых исследований;

– данная методика не является каскадной моделью, нет обязательной последовательности, этапы могут повторяться, а применяемые методы уточняться в рамках тестирования одной системы;

– большую часть тестирования целесообразно проводить с использованием автоматизированных специализированных программных средств.

Недостатком NIST SP 800–115 является то, что она дает общее методологическое представление и предлагает мало практических рекомендаций.

Рассмотрим далее более узконаправленную методику, также общепризнанную и используемую специалистами по тестированию на проникновение – методику тестирования безопасности веб приложений OWASP [12].

В соответствии с данной методикой процесс тестирования описывается в разделах, которые приводят список конкретных этапов тестирования. Каждый этап сопровождается инструкциями, примерами реализации атак, а также специализированными программными средствами для автоматизации процесса тестирования. OWASP также не является каскадной моделью и предполагает циклический процесс исследования. Набор тестов для проверки ИБ [13] представлен в табл. 1.

Таблица 1. Набор тестов методики OWASP

Наименование	Составляющие
Сбор первичной информации	- Сбор информации из открытых источников - Определение веб сервера - Определение структуры каталогов веб приложения - Определение веб межсетевого экрана
Тестирование управления конфигурацией и развертыванием	- Тестирование структуры приложения - Тестирование файлов на наличие чувствительной информации - Анализ резервного копирования и старых версий приложения - Тестирование HTTP методов - Тестирование политики CORS
Тестирование управления идентификацией	- Тестирование процесса регистрации - Определение списка аккаунтов - Тестирование на политику выбора имен пользователей
Тестирование аутентификации	- Тестирование полномочий - Тестирование политики выбора паролей - Тестирование на уязвимости функции смены пароля - Попытка обойти аутентификацию
Тестирование авторизации	- Тестирование на наличие уязвимости «обхода пути» - Попытка обойти авторизацию
Тестирование политики сессий	- Попытка обойти проверку сессии - Тестирование Cookie - Тестирование процедуры выхода из сессии
Тестирование на проверку пользовательского ввода	- Тестирование на XSS уязвимости - Тестирование на уязвимые параметры http запросов - Тестирование на SQL инъекции - Тестирование на инъекции вредоносного кода
Тестирование обработки ошибок	- Анализ кодов ошибок - Анализ стека трассировки
Тестирование на криптографическую устойчивость	- Тестирование на уязвимости протоколов SSL/TLS - Тестирование информации, передающейся по открытому каналу
Тестирование уязвимостей на стороне клиента	- Тестирование HTML инъекций - Тестирование CSS инъекций - Тестирование на уязвимость Clickjacking - Тестирование Local Storage

Отличительными особенностями данной методики являются:

– описание конкретных уязвимостей и инструкции для их обнаружения;

– этапы тестирования структурированы и определяют полную картину тестирования;

– цикличность проводимых этапов, которые имеют входные и выходные данные (выходные данные этапа могут использоваться в качестве входных данных другого этапа);

– большое количество готовых инструментов для автоматизированного тестирования.

Кроме рассмотренных выше стандартов по тестированию на проникновение, существует достаточно большое количество и других, в основном зарубежных, методик, которые имеют как преимущества, так и недостатки [14]. Однако их анализ показывает, что рассмотренные выше «хорошие практики» можно использовать как базовые для разработки

модельного представления соответствующего автоматизированного комплекса программных средств для значимых объектов КИИ.

3. Особенности тестирования значимых объектов КИИ

Как уже указывалось ранее, одним из существенных требований по безопасности, предъявляемых к значимым объектам КИИ, является анализ его уязвимостей, который допускается проводить по известным причинам на макете (полигоне) значимого объекта, то есть в виде имитации проведения в отношении него атаки. Алгоритм выявления уязвимостей значимого объекта включает следующие мероприятия:

1. Анализ проектной, рабочей (эксплуатационной) документации и организационно-распорядительных документов по безопасности.
2. Анализ настроек программных и программно-аппаратных средств, в том числе средств защиты информации.
3. Выявление известных уязвимостей программных и программно-аппаратных средств, в том числе средств защиты информации, посредством анализа состава установленного программного обеспечения и обновлений безопасности с применением средств контроля (анализа) защищенности и (или) иных средств защиты информации.
4. Выявление известных уязвимостей программных и программно-аппаратных средств, в том числе средств защиты информации, сетевых служб, доступных для сетевого взаимодействия, с применением средств контроля (анализа) защищенности.
5. Тестирование на проникновение в условиях, соответствующих принятым моделям угроз и нарушителя, определенных в принятой политике безопасности.

Первые четыре этапа, как правило, могут проводиться работниками сил обеспечения непосредственно субъекта КИИ, однако для наиболее важного последнего этапа, который и рассматривается в данной работе, это является трудно выполнимым условием в силу острой нехватки квалифицированных специалистов.

Среди мер по обеспечению безопасности значимых объектов КИИ, как было уже отмечено выше, тестирование на проникновение входит в состав аудита безопасности. Для его проведения инструментальными методами, например, при разработке программного продукта [15] или оценки безопасности элементов сетевой архитектуры [16], в том числе, тестирования на проникновение, используется большое количество возможных подходов.

Однако в контексте обеспечения безопасности объектов КИИ специфика именно автоматизированного поиска уязвимостей на данный момент рассмотрена недостаточно полно. Кроме этого, надо учитывать установленные повышенные государственные требования к процессу тестирования защищенности объектов КИИ и то, что данная задача имеет ряд отличительных особенностей. В отношении значимых объектов КИИ необходимо учитывать наличие нарушителя, обладающего всем возможным арсеналом информационного деструктивного воздействия. Другими словами, существующие методики аудита ИБ, построенные на типичной модели нарушителя, для значимых объектов КИИ могут быть недостаточно эффективными [17]. Данный вывод можно сделать и для задачи тестирования на проникновение. Результата оценки защищенности объекта КИИ, полученного специализированными программными средствами или на основе существующих методик может быть недостаточно. Необходима инструментальная проверка путем тестирования целенаправленными информационными воздействиями, аналогичными тем, которые будут применяться потенциальным противником. Основой такой проверки является тестирование на проникновение, максимально близко соответствующее действиям квалифицированных нарушителей, обладающих расширенными возможностями по неправомерному проникновению в систему.

Целесообразность введения новых модельных представлений при практической реализации устойчивого функционирования КИИ [2] объясняется многими факторами, важнейшим из которых является специфика самих объектов КИИ. Увеличение объема и функциональности новых прикладных систем приводит к повышению числа непреднамеренных ошибок в них, которые и станут уязвимостями для неправомерных информационных воздействий. Достаточно проследить за увеличением количества уязвимостей в банке данных угроз безопасности информации ФСТЭК России.

При рассмотрении задачи обнаружения компьютерных атак на объекты информатизации в отношении обеспечения безопасности объектов КИИ [18], этот фактор должен быть распространен и на задачу тестирования на проникновения. Основной аргумент в пользу создания специализированного модельного обнаружения уязвимостей значимых объектов КИИ – несоответствие существующих средств обнаружения вторжений реалиям текущей ситуации. Существующие методы хорошо справляются с известными типовыми атаками, однако в специфике защиты объектов КИИ нельзя ограничиваться типовыми шаблонами проведения атак, что значительно усложняет задачу автоматизированного поиска уязвимостей. Воздействие на критическую инфраструктуру может подразумевать и эксплуатацию комбинаций уязвимостей, что еще более усложняет поставленную задачу.

Из вышеизложенного можно выделить следующие характерные черты модельного представления процесса тестирования на проникновение объектов КИИ:

– имитация действий высококвалифицированного нарушителя;
– соответствие нарушителю, обладающему расширенным потенциалом деструктивного информационного воздействия;
– учет максимально расширенного списка уязвимостей;
– имитация эксплуатации комбинаций уязвимостей и уязвимостей нулевого дня.

Заключение

Учитывая важность объектов КИИ для безопасности государства и дальнейшее развитие информационных технологий, обеспечение безопасности данных объектов и предупреждения в отношении них негативных информационных воздействий является актуальным в настоящее время. Различные способы и методики, которые позволят заблаговременно прогнозировать и выявлять возможные уязвимости КИИ, должны рассматривать в качестве первоочередных задач исследований ИБ.

Основу таких способов может составить уже хорошо зарекомендовавшая методология тестирования на проникновение. Ее положительный опыт применения в качестве защитной меры для обеспечения безопасности объектов информатизации с одной стороны, и возможность изменения и адаптации под новые условия информационных систем, с другой стороны, позволяет использовать тестирование на проникновение в качестве базовой методологии при создании инструментальных средств обеспечения безопасности значимых объектов КИИ.

Представленные результаты являются предварительным этапом создания на основе рассмотренных методик NIST и OWASP соответствующего прототипа автоматизированного программного комплекса тестирования на проникновение для выявления уязвимостей значимых объектов КИИ.

СПИСОК ЛИТЕРАТУРЫ:

1. Лапсарь А.П., Назарян С.А., Владимирова А.И. Повышение устойчивости объектов критической информационной инфраструктуры к целевым компьютерным атакам. Вопросы кибербезопасности. 2022, № 2 (48), с. 39–51. DOI: https://doi.org/10.21681/2311-3456-2022-2-39-51.

2. Климов С.М., Поликарпов С.В., Рыжов Б.С., Тихонов Р.И., Шпырня И.В. Методика обеспечения устойчивости функционирования критической информационной инфраструктуры в условиях информационных воздействий. Вопросы кибербезопасности. 2019, № 6 (34), с. 37–48. DOI: https://doi.org/10.21681/2311–3456-2019-6-37-48.
3. Малюк А.А. Основы политики безопасности критических систем информационной инфраструктуры. Курс лекций. Учебное пособие для вузов. М.: Горячая линия-Телеком, 2018. – 314 с.
4. Серёдкин С.П. Безопасность критической информационной инфраструктуры (краткий обзор современных подходов). Информационные технологии и математическое моделирование в управлении сложными системами. 2021, № 4 (12), с. 30–38. DOI: https://doi.org/10.26731/2658-3704.2021.4(12).30-38. – EDN XFOFKY.
5. Ерохин С.Д., Петухов А.Н. Архитектура асимптотического управления безопасностью критических информационных инфраструктур. DSPA: Вопросы применения цифровой обработки сигналов. 2022, т. 12, № 1, с. 18–30. URL: https://www.elibrary.ru/item.asp?id=48402802 (дата обращения: 20.08.2022) – EDN CTANRM.
6. Макаренко С.И. Критерии и показатели оценки качества тестирования на проникновение. Вопросы кибербезопасности. 2021, № 3 (43), с. 43–57. DOI: https://doi.org/10.21681/2311-3456-2021-3-43-57. – EDN UDLKNN.
7. Макаренко С.И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями. Монография. СПб.: Наукоемкие технологии, 2018. – 122 с.
8. Свищёва И.В., Хлоповская А.В. Безопасная разработка программного обеспечения. Тестирование на проникновение. Моя профессиональная карьера. 2022, т. 2, № 36, с. 54–62. URL: https://www.elibrary.ru/item.asp?id=48656896 (дата обращения: 20.08.2022) – EDN CDANIE.
9. Макаренко С.И., Смирнов Г.Е. Модель аудита защищенности объекта критической информационной инфраструктуры тестовыми информационно-техническими воздействиями. Труды учебных заведений связи. 2021, т. 7, № 1, с. 94–104. DOI: https://doi.org/10.31854/1813-324X-2021-7-1-94–104. – EDN UBKIYS.
10. Хвостов Виктор А. и др. Анализ угроз безопасности информации при обработке конфиденциальных данных в мобильных системах. Безопасность информационных технологий, [S.l.], т. 28, № 1, с. 95–105, 2021. ISSN 2074-7136. DOI: https://doi.org/10.26583/bit.2021.1.08. – EDN SEKKBC.
11. Макаренко С.И. Тестирование на проникновение на основе стандарта NIST SP 800–115. Вопросы кибербезопасности. 2022, № 3 (49), с. 44–57. DOI: https://doi.org/10.21681/2311-3456-2022-3-44-57. – EDN JLCAVG.
12. Вульфин А.М. Анализ защищенности веб-приложения для доступа к системе хранения критически важных данных. Моделирование, оптимизация и информационные технологии. 2021, т. 9, № 4 (35). DOI: https://doi.org/10.26102/2310-6018/2021.35.4.038. – EDN MTZGUK.
13. Щекочихин О.В., Синкевич Е.А. Обеспечение информационной безопасности при работе с информационно-поисковыми системами. Информационно-экономические аспекты стандартизации и технического регулирования. 2022, № 2(66), с. 35–40. URL: https://www.elibrary.ru/item.asp?id=48444841 (дата обращения: 20.08.2022) – EDN HNBENM.
14. Макаренко С.И., Смирнов Г.Е. Анализ стандартов и методик тестирования на проникновение. Системы управления, связи и безопасности. 2020, № 4, с. 44–72. DOI: https://doi.org/10.24411/2410-9916-2020-10402. – EDN ZVHQBR.
15. Сенько Л.С. Интеграция аудита информационной безопасности в жизненный цикл разработки программного обеспечения. Инновации. наука. образование. 2020, № 23, с. 903–907. URL: https://www.elibrary.ru/item.asp?id=44488941 (дата обращения: 20.08.2022) – EDN BZPPDH.
16. Бирюков Д.Н., Лебедев С.Л., Самохвалов И.К., Холинов И.А. Построение программного комплекса аудита объектов сетевой инфраструктуры. Труды военно-космической академии имени А.Ф. Можайского. 2021, № 677, с. 135–142. URL: https://www.elibrary.ru/item.asp?id=46635761(дата обращения: 20.08.2022) – EDN AWUEFX.
17. Смирнов Г.Е., Макаренко С.И. Актуальные вопросы развития теории и практики аудита информационной безопасности объектов критической информационной инфраструктуры. Проблемы комплексной безопасности каспийского макрорегиона. Сборник научных статей по материалам международной научно-практической конференции. 2021, с. 148–157. URL: https://www.elibrary.ru/item.asp?id=47250497 – EDN MSQRDC.
18. Шабуров А.С., Никитин А.С. Модель обнаружения компьютерных атак на объекты критической информационной инфраструктуры. Вестник пермского национального исследовательского политехнического университета. электротехника, информационные технологии, системы управления. 2019, № 29, с. 104–117. URL: https://www.elibrary.ru/item.asp?id=37209216 – EDN ZBKJTN.

REFERENCES:

[1] Lapsar A.P., Nazaryan S.A., Vladimirova A.I. Ensuring the resistance of critical information infrastructure objects to advanced persistent threats. Voprosy kiberbezopasnosti. 2022, no. 2 (48), p. 39–51. DOI: https://doi.org/10.21681/2311-3456-2022-2-39-51 (in Russian).

[2] Klimov SM., Polikarpov S.V., Ryzhov B.S., Tikhonov R.I., Shpyrnya I.V. Procedure for Assuring the Continuity of Critical Information Infrastructure under Conditions of Information Influence. Voprosy kiberbezopasnosti. 2019, no. 6 (34), p. 37–48. DOI: https://doi.org/10.21681/2311-3456-2019-6-37-48 (in Russian).

[3] Malyuk A.A. Fundamentals of the security policy of critical information infrastructure systems. A course of lectures. Textbook for universities. M.: Hotline-Telecom, 2018. – 314 p. (in Russian).

[4] Seredkin S.P. An overview of the modern approach of security of critical information infrastructure. Information technologies and mathematical modeling in the management of complex systems. 2021, no. 4 (12), p. 30–38. DOI: https://doi.org/10.26731/2658-3704.2021.4(12).30-38. – EDN XFOFKY (in Russian).

[5] Erokhin S.D., Petukhov A.N. Architecture of asymptotic security management of critical information infrastructures. DSPA: Issues of application of digital signal processing. 2022, vol. 12, no. 1, p. 18–30. URL: https://www.elibrary.ru/item.asp?id=48402802 (accessed: 20.08.2022) – EDN CTANRM (in Russian).

[6] Makarenko S. I. Criteria and parameters for estimating quality of penetration testing. Voprosy kiberbezopasnosti. 2021, no. 3 (43), p. 43–57. DOI: https://doi.org/10.21681/2311-3456-2021-3-43-57. – EDN UDLKNN.

[7] Makarenko S.I. Security audit of critical infrastructure by special information impacts. Monograph. SPb.: Science–intensive technologies, 2018. – 122 p. (in Russian).

[8] Svishcheva I.V., Khlopovskaya A.V. Secure software development. Penetration testing. My professional career. 2022, vol. 2, no. 36, p. 54–62. URL: https://www.elibrary.ru/item.asp?id=48656896 (accessed: 20.08.2022) – EDN CDANIE (in Russian).

[9] Makarenko S.I., Smirnov G.E. Audit model of the security of an object of critical information infrastructure with test information and technical impacts. Proceedings of educational institutions of Communications. 2021, vol. 7, no. 1, p. 94–104. DOI: https://doi.org/10.31854/1813-324X-2021-7-1-94–104. – EDN: UBKIYS (in Russian).

[10] Khvostov Victor A. et al. Analysis of information security threats when processing confidential data in mobile systems. IT Security (Russia), [S.l.], v. 28, no. 1, p. 95–105, 2021. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2021.1.08. – EDN: SEKKBC (in Russian).

[11] Makarenko S.I. Penetration testing in accordance with NIST SP 800-115 standard. Voprosy kiberbezopasnosti. 2022, no. 3 (49), p. 44–57. DOI: https://doi.org/10.21681/2311-3456-2022-3-44-57. – EDN JLCAVG (in Russian).

[12] Vulfin A.M. Security analysis of a web application for accessing the critical data storage system. Optimization and Information Technology. 2021, vol.9, no. 4(35). DOI: https://doi.org/10.26102/2310-6018/2021.35.4.038. – EDN MTZGUK (in Russian).

[13] Shchekochikhin O.V., Sinkevich E.A. The problem of information security when working with information retrieval systems. 2022, no. 2(66), p. 35–40. URL: https://www.elibrary.ru/item.asp?id=48444841 (accessed: 20.08.2022) – EDN HNBENM (in Russian).

[14] Makarenko S. I., Smirnov G. E. Analysis of penetration testing standards and methodologies. Systems of Control, Communication and Security. 2020, no. 4, p. 44–72. DOI: https://doi.org/10.24411/2410-9916-2020-10402. – EDN ZVHQBR (in Russian).

[15] Senko L.S. Integration of information security audit into the software development lifecycle. Innovation. the science. education. 2020, no. 23, p. 903–907. URL: https://www.elibrary.ru/item.asp?id=44488941 (accessed: 20.08.2022) – EDN BZPPDH (in Russian).

[16] Biryukov D.N., Lebedev S.L., Samokhvalov I.K., Kholinov I.A. Building a software complex for auditing network infrastructure objects. Proceedings of the Military Space Academy named after A.F. Mozhaisky. 2021, no. 677, p. 135–142. URL: https://www.elibrary.ru/item.asp?id=46635761 (accessed: 20.08.2022) – EDN AWUEFX (in Russian).

[17] Smirnov G.E., Makarenko S.I. Actual issues of development of theory and practice of information security audit of critical information infrastructure objects. Problems of complex security of the Caspian macroregion. Collection of scientific articles based on the materials of the international scientific and practical conference. 2021, p. 148–157. URL: https://www.elibrary.ru/item.asp?id=4725049747250497 (accessed: 20.08.2022) – EDN MSQRDC (in Russian).

[18] Shaburov A.S., Nikitin A. S. The model for detecting computer attacks on objects of critical information infrastructure. Perm National Research Polytechnic University. 2019, no. 29, p. 104–117. URL: https://www.elibrary.ru/item.asp?id=37209216 (accessed: 20.08.2022) – EDN ZBKJTN (in Russian).

Поступила в редакцию – 20 августа 2022 г. Окончательный вариант – 04 сентября 2022 г.
Received – August 20,2022. The final version – September 04, 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@spels.ru
Сайт журнала: https://bit.spels.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 09.09.2022. Формат 60x84 1/8
Печ. л. 13,5 Уч.-изд. л. 13,5 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