ISSN 2225-5435

Вестник УрФО.

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 1(39) / 2021

УЧРЕДИТЕЛИ

ФГАОУ ВО «ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ООО «ЮЖНО-УРАЛЬСКИЙ ЮРИДИЧЕСКИЙ ВЕСТНИК»

Подписной индекс 73852 в каталоге «Почта России»

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Свидетельство ПИ № ФС77-65765 от 20.05.2016

Издатель: **ООО «Южно-Уральский юридический вестник»**

Адрес редакции и издателя: Россия, 454080, г. Челябинск, пр. Ленина, д. 76.
Тел./факс (351) 267-97-01.

Электронная версия журнала в Интернете:
www.info-secur.ru,
e-mail: urvest@mail.ru

16+

Journal of the Ural Federal District. Information security

ISSN 2225-5435

№ 1(39) / 2021

FOUNDER

SOUTH URAL STATE UNIVERSITY

SOUTH URAL LEGAL NEWSLETTER

CHAIRMAN OF THE EDITORIAL BOARD

CHUVARDIN O. P.,

Head of Department Federal Service for Technical and Export Control of Russia for the Urals Federal District

CHIEF EDITOR

SOKOLOV A.N.,

Ph.D., Associate Professor, Head of Department "Information Protection", South Ural State University (National Research University) (Chelyabinsk city)

PRODUCING EDITOR

SOGRIN E. K.

LAYOUT

SHRABER A. E.

PROOFREADING

FEDOROV V. S.

Subscription index 73852

in the «Russian Post» catalog

The journal is registered by the Federal service in the field of communication, information technology and mass communications.

Certificate
PI No. ФС77-65765 dd. 05/20/2016

Publisher: OOO « South Ural Legal Newsletter»

Editorial and publisher address: Russia, 454080, Chelyabinsk, Lenin Avenue, 76
Phone / fax (351) 267-97-01.

Electronic version of the magazine in the Internet:

www.info-secur.ru,
e-mail: urvest@mail.ru

16+

В НОМЕРЕ

ИССЛЕДОВАНИЕ И ПРОЕКТИРОВАНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ

ПОРШНЕВ С.В., БЕЛЯЕВ Д.О.
Скрытые технические каналы утечки информации, обрабатываемой в средствах вычислительной техники: анализ действующей нормативно-методической базы, терминология. 5

СУББОТИН С. Д., ВОЛЧКОВ Д. Н., ЗАБОКРИЦКИЙ А. А.
Обоснование актуальности разработки тестовой программы для специальных исследований интерфейса Displayport 14

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

ДУХАН Е. И., КНЯЗЕВА Н. С.
Анализ результатов исследования изменений временных отметок файлов. . . . 21

МЕТОДЫ АНАЛИЗА ДАННЫХ

ФЕЛЬДМАН Е. В., РУЧАЙ А. Н., ЧЕРБАДЖИ Д.Ю.
Модель выявления аномальных банковских транзакций на основе машинного обучения 27

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКАЯ И ПРАВОВАЯ ЗАЩИТА ИНФОРМАЦИИ

МУХАЧЕВ С. В., КОБЯКОВ А. В.
Об использовании информационных технологий в условиях борьбы с пандемией 36

АКТУАЛЬНЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ

АБДУЛИН А. А., СОКОЛОВ А. Н.
Исследование программных решений для обеспечения информационной безопасности промышленных сетей автоматизированных систем управления технологическими процессами 43

АСЯЕВ Г. Д., СОКОЛОВ А. Н.
Модель обеспечения информационной безопасности автоматизированной системы управления технологическим процессом на основе метода предиктивной защиты с использованием рекуррентной и полносвязной нейронных сетей 54

RESEARCH AND DESIGN OF TECHNICAL FACILITIES

PORSHNEV S. V., BELYAEV D. O.
Hidden technical channels of information leakage developed in computer equipment: analysis of the regulatory and methodological framework, termi-nology 5

SUBBOTIN S. D., VOLCHKOV D. N., ZABOKRITSKI A. A.
Justification of the relevance of developing a test program for special studies of the displayport interface 14

INFORMATION TECHNOLOGY AND COMPUTER SECURITY

DUHAN E.I., KNYAZEVA N. S.
Analysis of the files timestamps variations investigation results 21

METHODS OF DATA ANALYSIS

FELDMAN E. V., RUCHAY A. N., CHERBADZHI D. Y.
Model for detecting abnormal banking transactions based on machine learning 27

METHODS OF DATA ANALYSIS

MUKHACHEV S. V., KOBYAKOV A. V.
On the use of information technologies in the fight against the pandemic 36

METHODS OF DATA ANALYSIS

ABDULIN A. A., SOKOLOV A. N.
Research of software solutions for providing information security of industrial networks of automated process control systems 43

ASYAEV G. D., SOKOLOV A. N.
A model for ensuring information security of an automated process control system based on the predictive protection method using recurrent and fully connected neural networks 54

УДК 004.056.5

Вестник УрФО № 1(39) / 2021, с. 5–13

Поршнев С.В., Беляев Д.О.

DOI: 10.14529/secur210101

СКРЫТЫЕ ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ В СРЕДСТВАХ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ: АНАЛИЗ ДЕЙСТВУЮЩЕЙ НОРМАТИВНО-МЕТОДИЧЕСКОЙ БАЗЫ, ТЕРМИНОЛОГИЯ

В статье проведен анализ результатов научных исследований скрытых технических каналов утечки информации (СТКУИ, здесь под СТКУИ авторы предложили понимать технические каналы утечки информации (ТКУИ), мер противодействия, которые не предусмотрены действующими нормативными документами в области ТЗИ). Например, ТКУИ, создаваемые линиями электропередач, в которых зависимость потребления электроэнергии от времени определяется нагрузкой центральных процессоров (CPU) средств вычислительной техники (СВТ), управляемых предустановленной специальной программой; акустический ультразвуковой ТКУИ, образованный пассивными колонками и наушниками без использования микрофона; низкочастотные магнитные колебания, возникающие при работе CPU СВТ; радиоизлучение, сопровождающее в процесс ввода информации на смартфоне, которое регистрируется и анализируется на смартфоне нарушителя с помощью FM-тюнера; вариаций теплового излучения корпуса СВТ; акустического излучения, генерируемого дисковыми накопителями в процессе записи и считывания информации; электромагнитного излучения, возникающего в процессе обращения к различным устройствам через порт USB; оптического излучения светодиодных индикаторов СВТ и т.д.

Результаты проведенного анализа свидетельствуют о наличии реальных угроз несанкционированного доступа к информации, обрабатываемой в СВТ, через СТКУИ, а также необходимости проведения целенаправленных исследований данных ТКУИ и дальнейшего совершенствования нормативно-методической базы в области ТЗИ.

В данной статье проведен анализ действующей российской и зарубежной нормативно-методической базы в области технической защиты информации (ТЗИ), науч-

ных публикаций в данной области и обосновано целесообразность дополнения традиционно используемых в области технической защиты информации понятий «технический канал утечки информации (ТКУИ)», «скрытый канал» утечки информации понятием «скрытый технический канал утечки информации (СТКУИ)». Дано определение понятия СТКУИ, а также предложены его структурная схема и классификация СТКУИ.

Ключевые слова: *скрытый технический канал утечки информации, средство вычислительной техники, вредоносное программное обеспечение.*

Porshnev S.V., Belyaev D.O.

HIDDEN TECHNICAL CHANNELS OF INFORMATION LEAKAGE DEVELOPED IN COMPUTER EQUIPMENT: ANALYSIS OF THE REGULATORY AND METHODOLOGICAL FRAMEWORK, TERMINOLOGY

In article, an analysis of the results of scientific research of hidden technical channels of information leakage is carried out (here, under the hidden technical channels of information leakage, the authors proposed to understand technical channels of information leakage, measures to counteract which are not provided for by current regulatory documents in the field of technical information protection). For example, technical channels of information leakage created by power lines, in which the dependence of electricity consumption on time is determined by the load of central processing units (CPUs) of computer equipment controlled by a pre-installed special program; acoustic ultrasonic technical channel of information leakage formed by passive speakers and headphones without the use of a microphone; low-frequency magnetic vibrations that occur during the operation of the cpu of the computer equipment; radio radiation that accompanies the process of entering information on a smartphone, which is recorded and analyzed on the intruder's smartphone using an fm tuner; variations in thermal radiation of the computer equipment body; acoustic radiation generated by disk drives in the process of recording and reading information; electromagnetic radiation that occurs during access to various devices via the USB port; optical radiation of LED indicators of computer equipment, etc.

The results of the analysis indicate the presence of real threats unauthorized access to information processed at the computer device, using a hidden technical channels of information leakage and the need for targeted research of the data leakage channels and further improvement of normative-methodical base in the field of technical protection of information.

This article analyzes the current Russian and foreign regulatory and methodological framework in the field of technical information protection, scientific publications in this field and justifies the expediency of supplementing the traditionally used in the field of technical information

protection concepts of "technical channel of information leakage", "hidden channel" of information leakage with the concept of "hidden technical channel of information leakage". The definition of the concept of a hidden technical channel of information leakage is given, as well as its structural scheme and classification of hidden technical channels of information leakage are proposed.

Keywords: *hidden technical channel of information leakage, computer hardware, malicious software.*

Введение

Техническим каналом утечки информации (ТКУИ) называется совокупность источник информации (передатчик – объект разведки), линия связи (протяженная физическая среда), по которой распространяется информационный сигнал (собственно, канал передачи), а также средство приёма (перехвата) информации [1, 2]. Понятие «ТКУИ» оказывается неразрывно связанным с понятием «фактор, воздействующий на информацию» – «явление, действие или процесс, результатом которых являются утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней» [3]. Печень объективных и субъективных факторов (внутренних и внешних), воздействующих на защищаемую информацию, обрабатываемую средствами вычислительной техники, которые непосредственно формируют ТКУИ выделен в [4].

Отметим, что в отечественной нормативно-методической базе обеспечения информационной безопасности (в части, защиты информации, обрабатываемой с использованием средств вычислительной техники, от утечки по техническим каналам) особое внимание уделено рассмотрению источников угроз безопасности информации и технических каналов утечки, формируемым ввиду наличия факторов таких факторов, как побочные электромагнитные излучения, наводки, наличие акустоэлектрических преобразователей в элементах технических средств [устройств] обработки и передачи информации, а также доступ к защищаемой информации с применением технических средств, съема информации, несанкционированный доступ к защищаемой информации (см., например, [5]).

Однако оказывается, что также существуют ТКУИ, наличие которых обусловлено факторами, не входящими в приведенный выше перечень (например, акустические эманации, возникающие при отображении визуальной информации на экране, параметры которых определяются законом формирования изображения [6] и др.), и которые для краткости будем называть далее «скрытыми техническими каналами утечки информации» (СТКУИ). (Обоснование определения данного термина будет дано ниже.)

Обзор современного состояния открытых зарубежных научных исследований СТКУИ, проведенный авторами данной статьи [7], позволил сделать обоснованный вывод о высокой активности зарубежных ученых в исследованиях СТКУИ, в которых для получения доступа к информации, обрабатываемой средствами вычислительной техники, используются физические поля различной природы, а также о необходимости разработки соответствующей нормативно-правовой и методической базы по противодействию данным СТКУИ, в которой должно быть определено понятие СТКУИ.

В статье дано обоснование определения понятия СТКУИ, предложены его структурная схема и классификация СТКУИ.

Обоснование определения понятия «скрытый технический канал утечки информации»

Впервые понятие «скрытый канал» (covert channels) было введено в научный оборот в 1973 г. Батлером Лэмпсоном [8], под которым автор предложил понимать канал связи (коммуникационный канал), изначально не предназначенный для передачи информации, нарушающий установленную политику безопасности информации.

В соответствие с [9] «скрытый канал – это непредусмотренный разработчиком системы информационных технологий и автоматизированных систем коммуникационный канал, который может быть применен для нарушения политики безопасности информации. В соответствие с ГОСТ Р 53113.1-2008 п. 6.1 угрозы безопасности, которые могут быть реализованы с помощью скрытых каналов, включают в себя:

– внедрение вредоносных программ и данных;

– подачу злоумышленником команд агенту для выполнения;

– утечку криптографических ключей или паролей;

– утечку отдельных информационных объектов.

Понятие «скрытый канал» также используется для систематизации угроз безопасности информации. Например, в банке данных угроз безопасности ФСТЭК России присутствуют следующие угрозы безопасности информации: «УБИ.111: Угроза передачи данных по скрытым каналам» [10], «УБИ.115: Угроза перехвата вводимой и выводимой на периферийные устройства информации» [11], непосредственно связанные с рассматриваемым понятием.

Отметим, что в [12] указано, что «скрытые каналы используются для систематического взаимодействия вредоносных программ (компьютерных вирусов) с нарушителем безопасности при организации атаки на автоматизированные системы, которая не обнаруживается средствами контроля и защиты». Аналогичный алгоритм взаимодействия с потенциальным злоумышленником реализуется посредством разработки и использования вредоносного программного обеспечения формирования скрытого технического канала утечки информации [13]. Отметим, что с обсуждаемой технологией связано понятие «advanced persistent threat» (APT) – «развитая устойчивая угроза», для которой характерно установление и расширение перечня изделий и технологий злоумышленника внутри информационно-технологической инфраструктуры целевой организации для осуществления намерений нарушения политики безопасности информационной системы. Однако этот сценарий извлечения интересующей злоумышленника информации является частным случаем СТКУИ.

К несомненным достоинствам стандартов [9, 12] следует отнести: введение в постановку задачи обеспечения безопасности информации понятия «скрытый канал»; классификацию и систематизацию скрытых каналов; введение требований анализа защищенности информации от утечки по данным каналам и выработки адекватных мер защиты. Также отметим, что в стандартах [9, 12] определена важная особенность скрытого канала, состоящая в невозможности его идентификации применяемыми средствами контроля и средствами защиты информации, а также нейтрализации утечки и последствий этой утечки. В тоже время в них не дано определения термина «скрытый ТКУИ». При этом, очевидно, что понятие «скрытый канал» можно использовать не только применительно к атакам, реализуемых путем несанкци-онированного доступа в информационную систему и использования вредоносного программного обеспечения для нарушения конфиденциальности, целостности и доступности информации, но и к явлениям, связанным с формированием технических каналов утечки информации, однако данный факт упущен разработчиками стандартов [9, 12].

Анализ зарубежной нормативно-методической базы позволяет сделать вывод о том, что в ней не дается определения понятия «скрытый ТКУИ». В тоже время в некоторых зарубежных стандартах по информаци-онной безопасности используется понятие «скрытый канал» (англ. «covert channel»), связанное с нарушениями принятой в организации политики безопасности режимов обработки, хранения и передачи информации с использованием систем информационных технологий и автоматизированных систем, то есть исключительно в задаче обеспечения программно-аппаратной защиты информации.

Например, в стандарте [14], разработанном Национальным центром компьютерной безопасности США в соответствии с директивой 52 51 1 и утвержденном в ноябре 1993 г., определяется понятие «скрытый канал» и описаны некоторые механизмы анализа скрытых каналов. В разделе 2.1 обсуждаемого стандарта приводится четыре определения термина «скрытый канал»:

1. Канал связи является скрытым, если он вообще не предназначен для передачи информации.

2. Канал связи является скрытым (например, косвенным), если он основан на передаче переменных, описывающих ресурсные состояния».

3. Скрытые каналы «определены как такие каналы, которые существуют вследствие реализации политики распределения ресурсов и управления ресурсами.

4. Скрытые каналы – это те каналы, которые «используют объекты, обычно не рассматриваемые как объекты данных, для передачи информации от одного субъекта другому».

С точки зрения целей нашего исследования, наиболее близкими понятию «скрытый технический канал утечки информации» оказываются определения 1 и 4.

В стандарте [14] скрытые каналы классифицируются на:

1. Каналы хранения и синхронизации данных.

2. Зашумленные и незашумленные каналы (канал считается незашумленным, если символы, передаваемые отправителем, совпадают с символами, принимаемыми получателем с вероятностью, равной 1; каналы считаются зашумленными в случае, когда биты, передаваемые отправителем, не могут быть приняты правильно с вероятностью, равной 1, если не используются соответствующие коды исправления ошибок).

3. Агрегированные и неагрегированные каналы (несколько переменных данных, которые могут быть независимо друг от друга использованы для формирования скрытых каналов, могут быть использованы в качестве группы для амортизации затрат на синхронизацию (и, возможно, декодирование) информации. Таким образом, результирующие каналы агрегируются. Каналы могут агрегироваться последовательно, параллельно или в комбинациях последовательного и параллельного агрегирования для получения оптимальной (максимальной) полосы пропускания).

Методами идентификации скрытых каналов, согласно стандарту [14], являются:

1. Синтаксический анализ информационных потоков.

2. Добавление семантических компонентов к анализу информационных потоков.

3. Метод матрицы общих ресурсов (SRM).

4. Метод «невмешательства» (анализ информационных потоков производится с использованием модели информационной системы).

Таким образом, скрытые технические каналы утечки информации, возникающие в процессе функционирования средств вычислительной техники, не рассматриваются стандартом [14].

Среди зарубежных стандартов также отметим стандарт [15] и его обновленную версию [16], известные под аббревиатурами FIPS 140-2 и FIPS 140-3, при этом последний стандарт базируется на стандартах ISO/IEC 19790:2012 и ISO/IEC 24759:2017. Стандарты FIPS 140-2 и FIPS 140-3 относятся к стандартам компьютерной безопасности правительства США, определяющим требования к криптографическим модулям.

Разделы 4.11 стандарта FIPS 140-2, 7.12 стандарта ISO/IEC 19790:2012 и 6.12 стандарта /IEC 24759:2017 (на последних двух стандартах базируется FIPS 140-3), посвящены смягчению последствий других атак на криптографические системы, среди которых выделены:

1. Атаки, основанные на анализе энергопотребления.

2. Атаки по времени (атака по сторонним каналам, в которой атакующий пытается скомпрометировать криптосистему с помощью анализа времени, затрачиваемого на исполнение криптографических алгоритмов).

3. Атаки, использующие ошибки вычислений.

4. Атаки, использующие побочные электромагнитные излучения.

В [17] в дополнение к указанным видам атак авторами предлагается атака с использованием скрытого акустического канала, наряду с побочным электромагнитным излучением сопровождающего функционирование аппаратных средств криптографического преобразования и атака с использованием скрытого канала в оптическом диапазоне электромагнитных волн. Таким образом, в зарубежной нормативно-методической базе и научно-исследовательских трудах встречается также термин, схожий с понятием «скрытый канал» – «side-channel attacks» (атаки по сторонним (или побочным) каналам), который может быть употреблен в контексте проблематики исследования скрытых технических каналов утечки информации.

Отметим, что термин «side-channel attacks» в [17] употребляется исключительно в контексте криптоанализа, исключающего математический анализ шифрующего алгоритма. В качестве примера можно привести идентифицированную уязвимость CVE-2013-4576 из базы данных общеизвестных уязвимостей информационной безопасности [18], обнаруженную в программном обеспечении для шифрования информации и создания электронных подписей GnuPG 1.x и позволяющую осуществить операцию акустического криптоанализа во время дешифрования.

Таким образом, в зарубежной, также как и в отечественной нормативно-правовой базах отсутствуют определения понятия «скрытый ТКУИ».

В этой связи дадим собственное определение понятия «скрытый ТКУИ», принимая при этом во внимание выше изложенное: под скрытым техническим каналом утечки информации, обрабатываемой средствами вычислительной техники, следует понимать паразитный (побочный, вторичный) по отношению к основному (блокированному) техническому каналу утечки информации путь несанкционированного распространения информативного сигнала, представляющий собой совокупность управляемого или неуправляемого злоумышленником источника информации, формирующего информативный сигнал, физической среды распространения этого сигнала, по своей природе происхождения отличной от природы происхождения среды распространения сигнала основного канала утечки, и средства приёма (перехвата) сигнала, управляемого злоумышленником.

Структурная схема СТКУИ, соответствующая данному автором определению, приведена на рисунке 1.2.

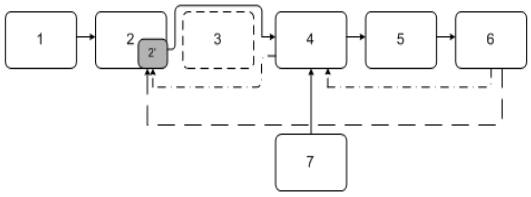


Рис.1. Структурная схема скрытого технического канала утечки информации: 1 – источник информации; 2 – источник информативного сигнала; 2' – источник сигнала в источнике 2, формирующий паразитный (вторичный, побочный) информативный сигнал, не анализируемый в ходе общепринятой методологии защиты информации от утечки по техническим каналам при ее обработке с использованием СВТ; 3 – техническое средство защиты информации (пассивное, активное); 4 – среда распространения информативного сигнала от источника 2'; 5 – техническое средства приёма (перехвата) сигнала от источника 2'; 6 – несанкционированный получатель (злоумышленник); 7 – помехи (физическая природа помех совпадает с физической природой сигнала от источника 2')

Из рисунка 1 видно, что СТКУИ обеспечивает для потенциального злоумышленника возможность дистанционно управлять (в частности, программно) как источником сигнала 2' (в том числе и через среду распространения источника 2') с целью преднамеренного формирования сигнала и извлечения из его параметров информативной составляющей, так и средой распространения с целью воздействия на источник сигнала и обрабатываемые им информационные ресурсы.

В качестве примера СТКУИ, реализованного по схеме, приведенной на рисунке 1, можно привести СТКУИ, описанный в [13]. Здесь специалистами центра кибербезопасности из Университета им. Бен-Гуриона в Негеве (г. Беэр-Шева, Израиль) были исследованы побочные акустические излучения, формируемые накопителями на жестких магнитных дисках (НЖМД) во время процессов поиска, чтения и записи информации и существующие параллельно с побочными электромагнитными излучениями НЖМД, измерение которых регламентируется действующей нормативно-правовой базой в области ТЗИ. Результаты проведенных исследований показали, что законы изменения параметров акустических сигналов определяются особенностями механизмов операций поиска, чтения и записи информации на НЖМД. Для управления акустическими сигналами, генерируемыми НЖМД, авторы разработали программное обеспечение «DiskFiltration», устанавливаемое на скомпрометированном средстве вычислительной техники, которое обеспечивало за счет программного управления движения рычага привода жесткого диска генерацию модулированного информационным сигналом акустического излучения на выбранных звуковых частотах. Генерируемое акустическое излучение перехватывается ближайшим приёмником (например, смартфоном, умными часами, ноутбуком и т. д.) с предустановленным программным обеспечением, позволяющим извлечь информативную составляющую из принятого сигнала. Также программа «DiskFiltration» обеспечивает изменения значения отношения «сигнал/шум» на стороне злоумышленника с помощью реализованного на передающей стороне алгоритма изменения параметров шумоподавления и увеличения интенсивности информативного акустического излучения с параметрами, не позволяющими идентифицировать нестандартное поведение НЖМД) с целью оптимального приёма и дальнейшего анализа.

Классификация СТКУИ

Основываясь на введенном определении понятия СТКУИ, а также обзо-ре результатов исследований скрыты технических каналов утечки информа-ции, обрабатываемой средствами вычислительной техники [7] мы предлагаем следующую классификацию данных каналов, представленную на рисунке 2.

Рис. 2. Классификация скрытых технических каналов утечки информации

Из рисунка 2 видно, что многообразие скрытых ТКУИ ввиду их неочевидности и потенциальной опасности ставит перед специалистами по обеспечению информационной безопасности нетривиальные задачи по выработке оптимальной методологии поиска СТКУИ, анализа защищенности информации от утечки по данным каналам и предложению оптимальных способов и средств защиты.

Заключение

На основе проведенного анализа определений понятия «скрытый канал» в отечественной и зарубежной нормативно-правовой базе обоснована необходимость определения понятия «скрытый технический канал утечки информации» и дано его определение, а также предложена соответствующая классификация СТКУИ.

Литература

1. Бузов, Г. А. Защита информации ограниченного доступа от утечки по техническим каналам: Справочное пособие / Бузов Г.А. – М.: Горячая линия-Телеком, 2015.

2. Зайцев, А. П. Технические средства и методы защиты информации. Учебник для вузов – 7-е изд., испр. / А.П. Зайцев, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая Линия–Телеком, 2018.

3. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.

4. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

5. Специальные требования и рекомендации по технической защите конфиденциальной информации. Утверждены приказом Гостехкомиссии России от 30 августа 2002 г.

6. Daniel Genkin, Mihir Pattani, Roei Schuster, Eran Tromer. Synesthesia: Detecting Screen Content via Remote Acoustic Side Channels. 2019 IEEE Symposium on Security and Privacy (SP), 2019. P. 853-869. – URL: https://ieeexplore.ieee.org/abstract/document/8835386 – (дата обращения: 15.10.2019).

7. Поршнев, С.В., Беляев, Д.О. Обзор результатов исследований скрытых технических каналов утечки информации, обрабатываемой сред-ствами вычислительной техники. 2020, В: Вестник УрФО. Безопасность в информационной сфере.

8. Lampson, B. W.A Note on the Confinement Problem A Note on the Confinement Problem, Communications of the ACM, 16, 10 (Oct. 1973), pp 613-615.

9. ГОСТ Р 53113.1-2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения.

10. Банк данных угроз безопасности информации. – URL: https://bdu.fstec.ru/ubi/threat/view/id/526 – (дата обращения: 25.07.2020).

11. Банк данных угроз безопасности информации. – URL: https://bdu.fstec.ru/ubi/threat/view/id/530 – (дата обращения: 25.07.2020).

12. ГОСТ Р 53113.2-2009. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов.

13. Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici. DiskFiltration: Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard Drive Noise. arXiv preprint arXiv:1608.03431, 2016. – URL: https://arxiv.org/ftp/arxiv/papers/1608/1608.03431.pdf – (дата обращения: 27.03.2020).

14. A Guide to Understanding Covert Channel Analysis of Trusted Sys-tems, National Computer Security Center. NCSC-TG-030. - Ver. 1, 1993 – URL: https://fas.org/irp/nsa/rainbow/tg030.htm – (дата обращения: 10.07.2020).

15. Federal Information Processing Standard Publication 140-2 – URL: https://csrc.nist.gov/publications/fips/140/2/final – (дата обращения: 15.06.2020).

16. Federal Information Processing Standard Publication 140-3 – URL: https://csrc.nist.gov/publications/fips/140/3/final – (дата обращения: 15.06.2020).

17. Yong Bin Zhou, Deng Guo Feng. Side-Channel At-tacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing. State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing, China, 2006. – URL: http://eprint.iacr.org/2005/388.pdf – (дата обращения: 15.06.2020).

18. Common Vulnerabilities and Exposures. – URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4576 – (дата обращения: 12.06.2020).

References

1. Buzov, G. A. Zashchita informacii ogranichennogo dostupa ot utechki po tekhnicheskim kanalam: Spravochnoe posobie / Buzov G.A. – M.: Goryachaya liniya-Telekom, 2015.

2. Zajcev, A. P. Tekhnicheskie sredstva i metody zashchity informacii. Uchebnik dlya vuzov – 7-e izd., ispr. / A.P. Zajcev, R.V. Meshcheryakov, A.A. SHelu-panov. – M.: Goryachaya Liniya–Telekom, 2018.

3. GOST R 50922-2006. Zashchita informacii. Osnovnye terminy i op-redeleniya.

4. OST R 51275-2006. Zashchita informacii. Ob'ekt informatizacii. Faktory, vozdejstvuyushchie na informaciyu. Obshchie polozheniya.

5. Special'nye trebovaniya i rekomendacii po tekhnicheskoj zashchite konfidencial'noj informacii. Utverzhdeny prikazom Gostekhkomissii Rossii ot 30 avgusta 2002 g.

6. Daniel Genkin, Mihir Pattani, Roei Schuster, Eran Tromer. Synesthe-sia: Detecting Screen Content via Remote Acoustic Side Channels. 2019 IEEE Symposium on Security and Privacy (SP), 2019. P. 853-869. – URL: https://ieeexplore.ieee.org/abstract/document/8835386 – (data obrashheniya: 15.10.2019).

7. Porshnev, S.V., Belyaev, D.O. Obzor rezul'tatov issledovanij skrytyh tekhnicheskih kanalov utechki informacii, obrabatyvaemoj sredstvami vychislitel'noj tekhniki. 2020, V : Vestnik UrFO. Bezopasnost' v informacionnoj sfere.

8. Lampson, B. W.A Note on the Confinement Problem A Note on the Confinement Problem, Communications of the ACM, 16, 10 (Oct. 1973), pp 613-615.

9. GOST R 53113.1-2008. Informacionnaya tekhnologiya. Zashchita informacionnyh tekhnologij i avtomatizirovannyh sistem ot ugroz informacionnoj bezopasnosti, realizuemyh s ispol'zovaniem skrytyh kanalov. CHast' 1. Obshchie polozheniya.

10. Bank dannyh ugroz bezopasnosti informacii. – URL: https://bdu.fstec.ru/ubi/threat/view/id/526 – (data obrashheniya: 25.07.2020).

11. Bank dannyh ugroz bezopasnosti informacii. – URL: https://bdu.fstec.ru/ubi/threat/view/id/530 – (data obrashheniya: 25.07.2020).

12. GOST R 53113.2-2009. Informacionnaya tekhnologiya. Zashchita informacionnyh tekhnologij i avtomatizirovannyh sistem ot ugroz informacionnoj bezopasnosti, realizuemyh s ispol'zovaniem skrytyh kanalov. CHast' 2. Rekomendacii po organizacii zashchity informacii, informacionnyh tekhnologij i avtomatizirovannyh sistem ot atak s ispol'zovaniem skrytyh kanalov.

13. Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici. DiskFiltration: Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard Drive Noise. arXiv preprint arXiv:1608.03431, 2016. – URL: https://arxiv.org/ftp/arxiv/papers/1608/1608.03431.pdf – (data obrashheniya: 27.03.2020)

14. A Guide to Understanding Covert Channel Analysis of Trusted Systems, National Computer Security Center. NCSC-TG-030. - Ver. 1, 1993 – URL: https://fas.org/irp/nsa/rainbow/tg030.htm – (data obrashheniya: 10.07.2020).

15. Federal Information Processing Standard Publication 140-2 – URL: https://csrc.nist.gov/publications/fips/140/2/final – (data obrashheniya: 15.06.2020).

16. Federal Information Processing Standard Publication 140-3 – URL: https://csrc.nist.gov/publications/fips/140/3/final – (data obrashheniya: 15.06.2020).

19. Yong Bin Zhou, Deng Guo Feng. Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing. State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing, China, 2006. – URL: http://eprint.iacr.org/2005/388.pdf – (data obrashheniya: 15.06.2020).

17. Common Vulnerabilities and Exposures. – URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4576 – (data obrash-heniya: 12.06.2020).

ПОРШНЕВ Сергей Владимирович, доктор технических наук, профессор, директор Учебно-научного центра «Информационная безопасность», Институт радиоэлектроники и информационных технологий – РтФ, Федеральное государственное автономное образовательное учреждение высшего образования «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина». 620002, г. Екатеринбург, ул. Мира, 19. E-mail: sergey_porshnev@mail.ru

БЕЛЯЕВ Дмитрий Олегович, старший преподаватель Учебно-научного центра «Информационная безопасность», Институт радиоэлектро-ники и информационных технологий – РтФ, Федеральное государственное автономное образовательное учреждение высшего образования «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина». 620002, г. Екатеринбург, ул. Мира, 19. E-mail: belyaev-urfu@yandex.ru

PORSHNEV Sergey, Dr.Sc., Professor, head of Educational and research center «Information security», Institute of radio electronics and information technologies – RTF, Ural Federal University.B. N. Yeltsin. 620002, Ekaterinburg, Mira street, 19. E-mail: sergey_porshnev@mail.ru

BELYAEV Dmitry, Senior Lecturer of Educational and research center «Information security», Institute of radio electronics and information technologies – RTF, Ural Federal University.B. N. Yeltsin. 620002, Ekaterinburg, Mira street, 19. E-mail: belyaev-urfu@yandex.ru

УДК 537.876.2 + 004.056 Вестник УрФО № 1(39) / 2021, с. 14–20

Субботин С.Д., Волчков Д.Н., Забокрицкий А.А. DOI: 10.14529/secur210102

ОБОСНОВАНИЕ АКТУАЛЬНОСТИ РАЗРАБОТКИ ТЕСТОВОЙ ПРОГРАММЫ ДЛЯ СПЕЦИАЛЬНЫХ ИССЛЕДОВАНИЙ ИНТЕРФЕЙСА DISPLAYPORT

Целью исследования, приведённого в статье, является повышения эффективности проведения специальных исследований интерфейса DisplayPort на основе изучения характеристик для разработки тестовых программ. Для этого исследована возможность перехвата побочных электромагнитных излучений данного интерфейса, проведен поиск информативных сигналов от интерфейса и исследовано их затухание на различных расстояниях. Параметры информативного сигнала от интерфейса DisplayPort проанализированы на осциллографе в автоматическом режиме. Обоснована актуальность разработки специальных программ.

Ключевые слова: *побочные электромагнитные излучения, DisplayPort, технический канал утечки информации, специальные исследования, информативные сигналы, электрические сигналы, защита информации.*

Subbotin S.D., Volchkov D.N., Zabokritski A.A.

JUSTIFICATION OF THE RELEVANCE OF DEVELOPING A TEST PROGRAM FOR SPECIAL STUDIES OF THE DISPLAYPORT INTERFACE

The purpose of the research presented in the article is to improve the efficiency of conducting special studies of the DisplayPort interface based on the study of characteristics for further development of test programs. For this purpose, the possibility of intercepting the side electromagnetic radiation of this interface is investigated, the search for informative signals from the interface is carried out, and their attenuation at various distances is investigated. The parame-

ters of the informative signal from the DisplayPort interface are analyzed in the oscilloscope mode. The relevance of the development of special programs is justified.

Keywords: *spurious electromagnetic emissions, DisplayPort, technical channel of information leakage, special research, informative signals, electrical signals, information protection.*

DisplayPort является современным интерфейсом для подключения мониторов и другой мультимедийной техники. Данные устройства могут участвовать в обработке информации ограниченного доступа. В связи с этим возможность наличия технического канала утечки информации (далее – ТКУИ) за счет побочных электромагнитных излучений, возникающих при прохождении сигнала через данный интерфейс, является актуальной проблемой [1].

Для поиска информативных сигналов был собран лабораторный стенд из ноутбука MSI GP73 LEOPARD 8RE (далее – ноутбук) и монитора DELL E2020H 19.5» (далее – монитор), соединенных кабелем HAMA Mini DisplayPort-DisplayPort версией 1.2 [2].

Исследование характеристик излучений интерфейса DisplayPort осуществлялось с помощью поверенных специальных средств измерения внесенных в Государственный реестр средств измерений [3]:

– анализатор спектра «Rohde & Schwarz FSV13» (управление осуществлялось с помощью ноутбука оператора со специальным программным обеспечением «СПО-Навигатор»);

– антенна магнитная активная «АМА-30»;

– антенна дипольная активная «АДА-9»;

– антенна широкополосная рупорная «П6-123» с малошумящим усилителем «ММ 0118. SFSF» из антенного измерительного комплекта «АИК 1-40Б».

Для поиска информативных сигналов измерительные антенны располагались вблизи места подключения интерфейса к монитору, затем измерительные антенны отставлялись на 1 м от исследуемого объекта для фиксирования уровня напряженности электромагнитного поля найденного информативного сигнала. Измерения проводились относительно 1 мкВ/м в полосе пропускания измерительного приемника 1 кГц по магнитной составляющей в диапазоне 0,009…30 МГц антенной «АМА-30», а также в полосе пропускания измерительного приемника 10 кГц по электрической составляющей в диапазоне 0,009…2000 МГц антенной «АДА-9» и диапазоне 900…12000 МГц антенной «П6-123» с малошумящим усилителем «ММ 0118. SFSF» [4].

Рассматриваемый режим обработки информации – вывод информации с ноутбука на экран монитора с разрешением 1600x900, частотой развертки 60 Гц.

Напряженность электромагнитного поля измерялась вблизи интерфейса в два этапа. На первом – был измерен индустриальный шум при выключенных ноутбуке и мониторе. На втором после включения ноутбука и монитора измерялась совокупность «сигнал + шум». В качестве тест-сигналов использовалось включение/выключение монитора от сети [5].

Измерения по магнитной составляющей электромагнитного поля вблизи исследуемого интерфейса антенной «АМА-30» показали большое количество информативных сигналов, которые затухали на расстоянии 30 сантиметров. Напряженность информативных сигналов по магнитной составляющая электромагнитного поля в статье не рассматривалась.

Проведя измерения антенной «АДА-9» вблизи интерфейса, наиболее сильный на фоне индустриального шума информативный сигнал был обнаружен на частоте 172,79 МГц. Измеренные на данной частоте уровень шума и напряженности информативного сигнала составили 26,62 дБ и 47,03 дБ соответственно (см. рис. 1).

Оценивая опасность выявленного сигнала, провели измерения его характеристик на 1 метре от стенда (см. рис. 2).

В данных условиях сигнал был обнаружен. Измеренные уровни шума и напряженности информативного сигнала составили 20,37 дБ и 30,33 дБ соответственно (см. рис. 3).

Аналогичным способом на 1 метре были проведены измерения антенной «П6-123» с малошумящим усилителем «ММ 0118. SFSF» в диапазоне 900…12000 МГц. Результаты измерений представлены в табл. 1.

Условные обозначения, используемые в табл. 1:

$E_{С+Ш}$ – измеренные уровни напряженности электрической составляющей электромагнитного поля от исследуемого технического средства;

$E_{Ш}$ – измеренные уровни напряженности

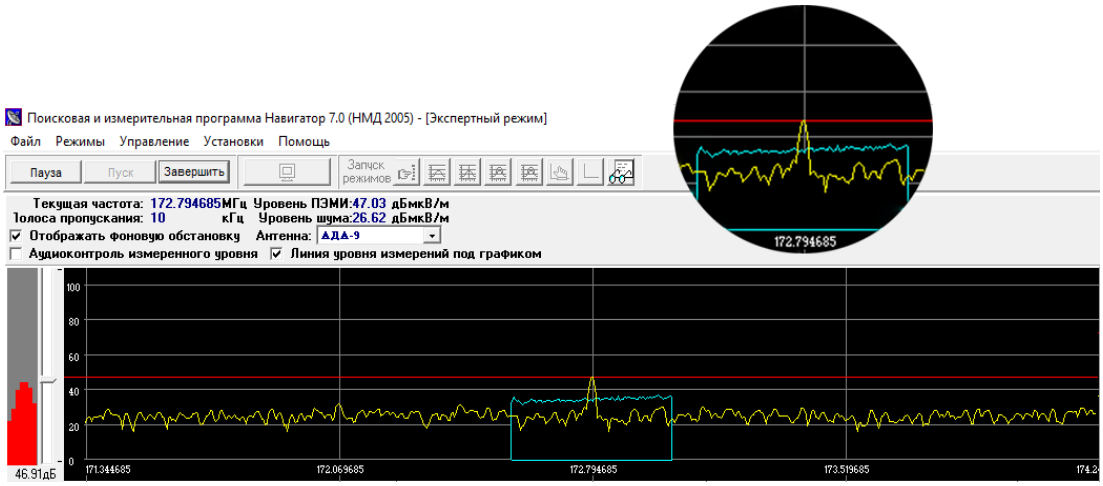


Рис. 1. Спектр информативного сигнала вблизи исследуемого интерфейса

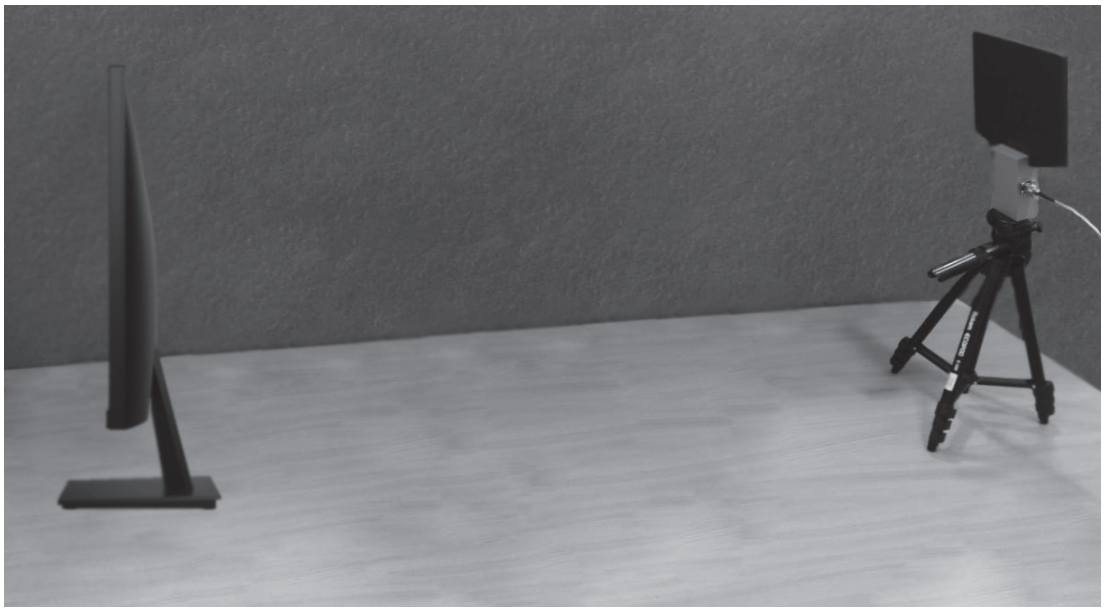


Рис. 2. Измерение информативного сигнала на расстоянии 1 метр

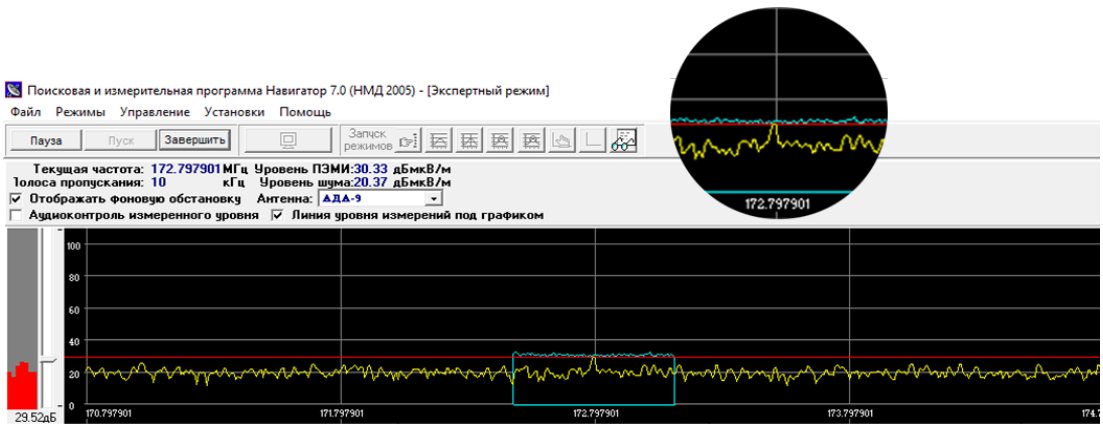


Рис. 3. Спектр информативного сигнала на расстоянии 1 метр от исследуемого интерфейса

Таблица 1

Результаты измерений антенной «П6-123» на 1 метре

№ п/п	Частота, МГц	ЕС+Ш, дБ (мкВ/м)	ЕШ, дБ (мкВ/м)
1	902.030688	26.12	20.80
2	1374.520898	42.97	23.15
3	1546.333069	39.77	19.99
4	1889.969577	30.42	25.05
5	2405.426984	28.31	14.92
6	2749.056084	32.92	19.10
7	2920.863493	33.21	22.21
8	3436.308730	41.80	21.98
9	5154.481746	28.33	23.30

электрической составляющей электромагнитного поля при отключенном исследуемом техническом средстве.

Наибольший уровень напряженности электромагнитного поля информативных сигналов, измеренных антенной «П6-123» с малошумящим усилителем «ММ 0118. SFSF», приведен на рис. 4 и 5.

Полученные данные свидетельствуют об опасности возникновения ТКУИ за счет побочных электромагнитных излучений при использовании интерфейса DisplayPort.

Для исследования амплитудных и временных параметров информативного сигнала от интерфейса DisplayPort использовался цифровой осциллограф «АСК-2203». Измерения проводились во время передачи данных по исследуемому интерфейсу, напрямую подключаясь к проводу (см. рис. 6).

Форма сигала полученная на осциллографе в режиме усреднения приведена на рис. 7.

В результате измерений осциллографом в автоматическом режиме получены следующие временные характеристики информативного сигнала:

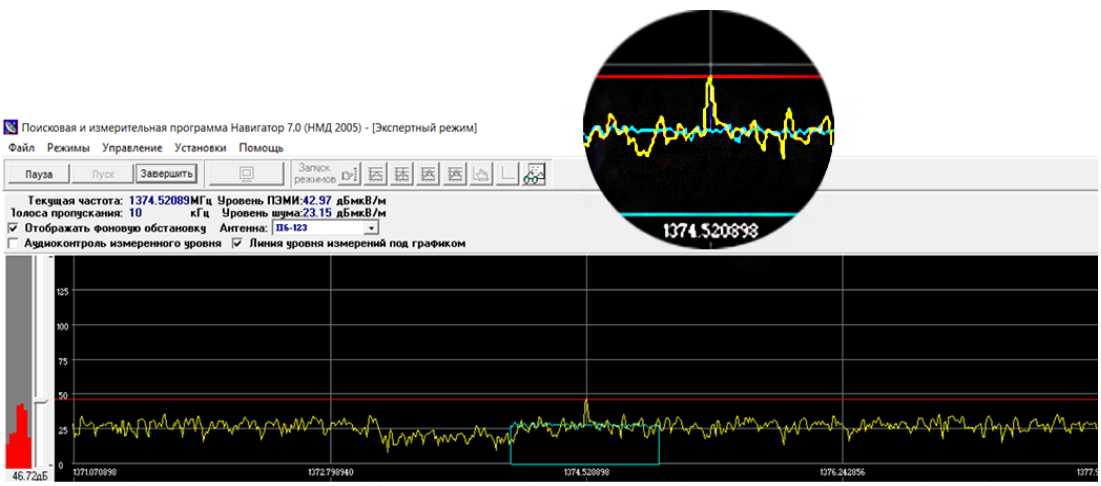


Рис. 4. Уровень напряженности электромагнитного поля информативного сигнала от исследуемого интерфейса на частоте 1374,52 МГц

– длительность импульса 10,50 мкс;

– период импульсов 22,50 мкс.

Данная информация может быть использована для создания специальных тестовых программ, так как их отсутствие затрудняет поиск и исследование характеристик информативных сигналов от данного интерфейса.

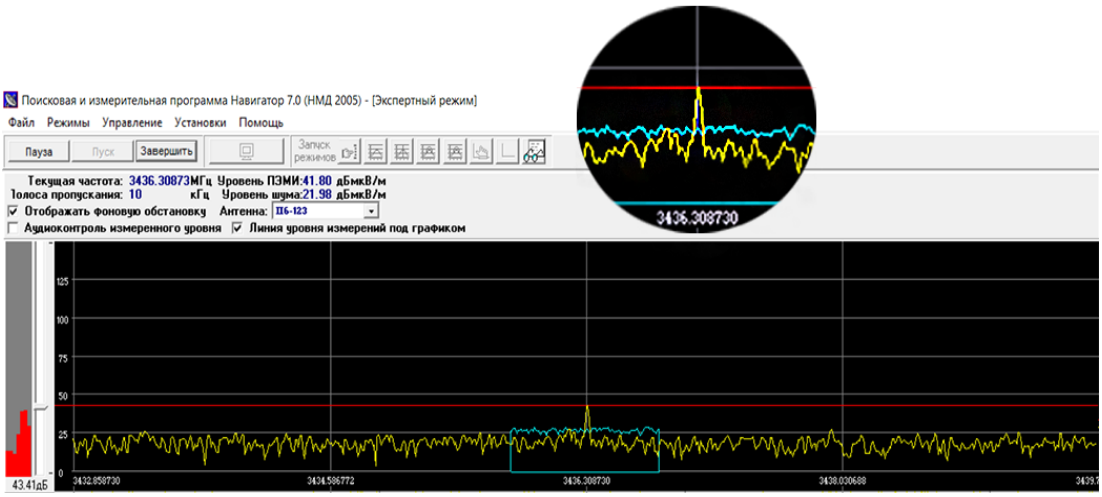


Рис. 5. Уровень напряженности электромагнитного поля информативного сигнала от исследуемого интерфейса на частоте 3436,31 МГц

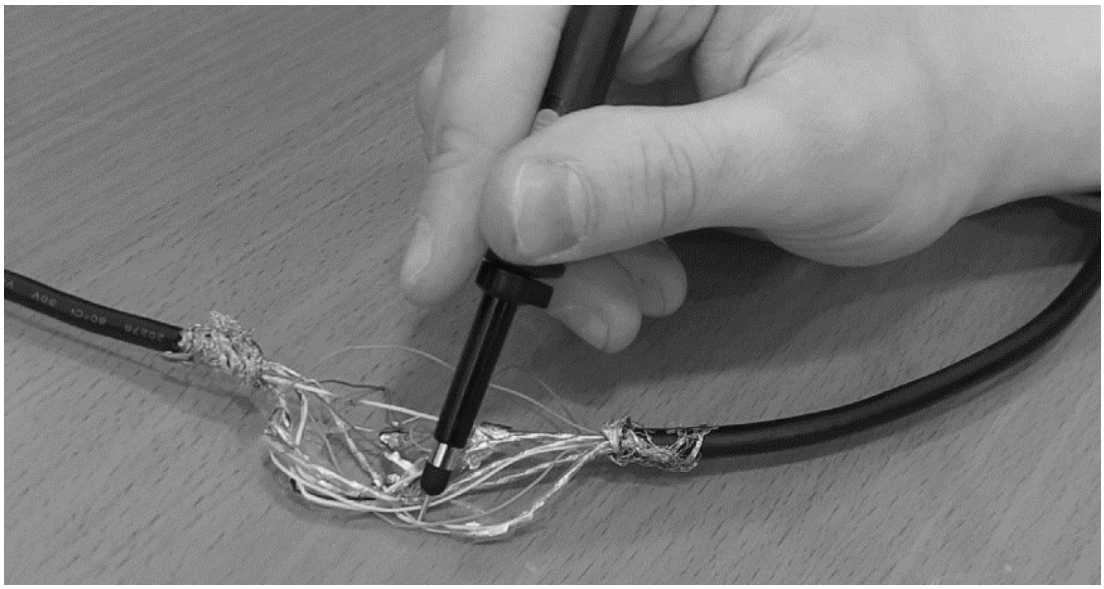


Рис. 6. Подключение к интерфейсу DisplayPort для исследования на осциллографе

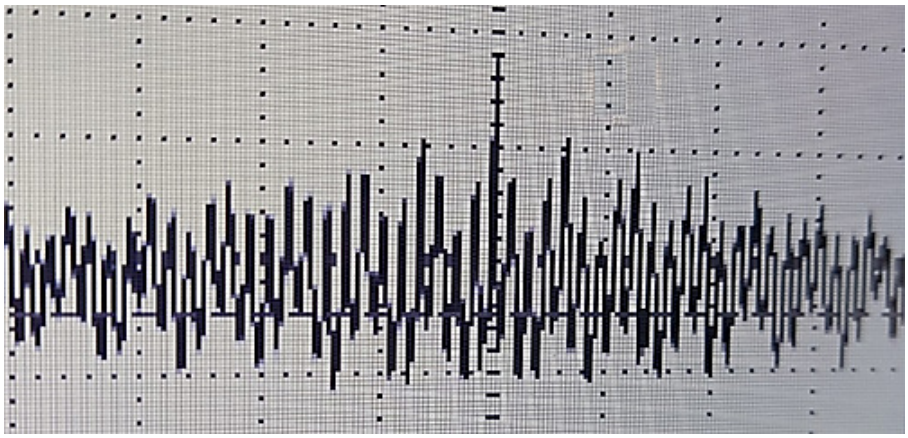


Рис. 7. Осциллограмма исследуемого интерфейса

Таким образом, подводя результаты исследования, можно утверждать о существующем техническом канале утечки информации от исследуемого технического средства с интерфейсом DisplayPort. Об опасности утечки информации по данному каналу можно судить не только по найденному широкому диапазону частот информативных сигналов, но и по их низкому затуханию при удалении от исследуемого устройства. Большинство информативных сигналов были отчетливо видны на расстоянии более одного метра.

Для повышения качества и эффективности проведения специальных исследований интерфейса DisplayPort, актуальной задачей является разработка специальных тестов использующие данные о длительности и периоде импульсов. Именно благодаря специальным тест-программам будет осуществляться корректный поиск и измерение напряженности электромагнитного поля информативных сигналов.

Литература

1. Кондратьев А. В. Техническая защита информации. Практика работ по оценке основных каналов утечки. – М.: Горячая линия – Телеком, 2016. – 304 с. ISBN 978-5-9912-0574-0.

2. VESA DisplayPort Standard Version 1, Revision 2 [Электронный ресурс] Github.com. URL: https://glenwing.github.io/docs/DP-1.2.pdf (дата обращения: 17.02.2021).

3. Государственный реестр средств измерений. [Электронный ресурс] URL: https://fgis.gost.ru/fundmetrology/registry/4 (дата обращения: 17.02.2021).

4. Кондратьев А. В. К вопросу оценки ПЭМИН цифровых сигналов. TFT мониторы. Часть 2 // Официальный сайт группы компаний МАСКОМ. – URL: http://www.mascom.ru/library/statyi/k-voprosu-otsenkipemin-tsifrovykh-signalov-tft-monitory-chast-2.php (дата обращения: 17.02.2021).

5. Кондратьев А. В. К вопросу оценки ПЭМИН цифровых сигналов. TFT мониторы. Часть 3 // Официальный сайт группы компаний МАСКОМ. – URL: http://www.mascom.ru/library/statyi/k-voprosu-otsenkipemin-tsifrovykh-signalov-tft-monitory-chast-3.php (дата обращения: 17.02.2021).

References

1. Kondrat'yev A. V. Tekhnicheskaya zashchita informatsii. Praktika rabot po otsenke osnovnykh kanalov utechki. – M.: Goryachaya liniya – Telekom, 2016. – 304 s. ISBN 978-5-9912-0574-0.

2. VESA DisplayPort Standard Version 1, Revision 2 [Online] Github.com. URL: https://glenwing.github.io/docs/DP-1.2.pdf (accessed: 17.02.2021).

3. Gosudarstvennyy reyestr sredstv izmereniy. [Elektronnyy resurs] URL: https://fgis.gost.ru/fundmetrology/registry/4 (data obrashcheniya: 17.02.2021).

4. Kondrat'yev A. V. K voprosu otsenki PEMIN tsifrovykh signalov. TFT monitory. Chast' 2 // Ofitsial'nyy sayt gruppy kompaniy MASKOM. – URL: http://www.mascom.ru/library/statyi/k-voprosu-otsenkipemin-tsifrovykh-signalov-tft-monitory-chast-2.php (data obrashcheniya: 17.02.2021).

5. Kondrat'yev A. V. K voprosu otsenki PEMIN tsifrovykh signalov. TFT monitory. Chast' 3 // Ofitsial'nyy sayt gruppy kompaniy MASKOM. – URL: http://www.mascom.ru/library/statyi/k-voprosu-otsenkipemin-tsifrovykh-signalov-tft-monitory-chast-3.php (data obrashcheniya: 17.02.2021).

СУББОТИН Станислав Дмитриевич, аспирант ИРИТ-РтФ УрФУ имени первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 19, E-mail: s.d.subbotin@urfu.ru.

ВОЛЧКОВ Дмитрий Николаевич, магистрант ИРИТ-РтФ УрФУ имени первого Президента России Б.Н. Ельцина 620002, г. Екатеринбург, ул. Мира, 19, E-mail: vlc_d.n@mail.ru.

ЗАБОКРИЦКИЙ Александр Александрович, кандидат технических наук, начальник отдела, Управление Федеральной службы по техническому и экспортному контролю по Уральскому федеральному округу. 620078, г. Екатеринбург, ул. Гагарина, 28Б, E-mail fstec@rambler.ru.

SUBBOTIN Stanislav, Postgraduate of Institute of Radio electronics and Information Technologies, Ural Federal University named after first President of Russia B.N. Yeltsin. 620002, Yekaterinburg, Mira str., 19. E-mail: s.d.subbotin@urfu.ru.

VOLCHKOV Dmitry, Undergraduate of Institute of Radio electronics and Information Technologies, Ural Federal University named after first President of Russia B.N. Yeltsin. 620002, Yekaterinburg, Mira str., 19. E-mail: vlc_d.n@mail.ru.

ZABOKRITSKI Alexander, Ph.D of Engineering Sciences., head of department, FSTEC of Russia headquarters in the Urals Federal District. 620078, Yekaterinburg, 28B Gagarin street, E-mail: fstec@rambler.ru.

УДК 004.056.57

Вестник УрФО № 1(39) / 2021, с. 21–26

Духан Е.И., Князева Н.С.

DOI: 10.14529/secur210103

АНАЛИЗ РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЯ ИЗМЕНЕНИЙ ВРЕМЕННЫХ ОТМЕТОК ФАЙЛОВ

В статье рассмотрены работы, посвященные выявлению закономерностей изменения временных отметок при совершении файловых операций. Представлена авторская методика экспериментальных исследований временных отметок файлов. Полученные результаты исследований сведены в таблицу, которая наглядно представляет изменения временных отметок при выполнении пользователем операций над файлами. Систематизированные в виде таблицы данные могут явиться основой для разработки методики восстановления последовательности файловых операций, пригодной для автоматизации.

Ключевые слова: *временные отметки, NTFS, $STANDARD_INFORMATION, $FILE_NAME, файловые операции, компьютерная криминалистика.*

Duhan E.I., Knyazeva N.S.

ANALYSIS OF THE FILES TIMESTAMPS VARIATIONS INVESTIGATION RESULTS

In the article the papers concerning identification of patterns for timestamps variation during file operations being performed are observed. The authors suggest a unique method files timestamps experimental investigation. The obtained research results are summarized in a table that clearly shows the changes in time stamps when the user performs operations over files. Systematized data in the form of a table can be the basis for the development of a method for restoring a sequence of file operations that is suitable for automation.

Keywords: *timestamps, NTFS, $STANDARD_INFORMATION, $FILE_NAME, file operations, computer forensics.*

Современные информационные технологии не только способствуют активному развитию обществу, но и стимулируют рост преступлений, в которых компьютер выступает средством их совершения. Одним из распространенных вопросов, возникающих в ходе расследования компьютерных преступлений, является установление времени создания, изменения и распространения компьютерной информации, хранимой в виде конкретных файлов. Типовой задачей компьютерной криминалистики («Форензики») явля-

ется восстановление последовательности операций, совершенных пользователем над файлами [1]. Для решения криминалистической задачи исследуется служебная информация, регистрируемая в файловой системе (ФС) компьютера. Достоверность и глубина восстановления цепочки файловых операций (ФОп) зависит от объема информации, извлечение и анализ которой требуют большого объема ручной работы и высокой квалификации специалиста.

Файловая система представляет собой структурированное хранилище каталогов и файлов. С точки зрения восстановления файловых операций ФС следует рассматривать как дискретную динамическую систему, которая характеризуется состояниями в некоторые моменты времени. Под воздействием программного обеспечения во время активных действий пользователя компьютера эти состояния изменяются. Таким образом, восстановление последовательности ФОп является задачей системного анализа и сводится к определению траектории движения между начальным и конечным состояниями системы.

Состояниями системы называют совокупность значений некоторых ее характеристик [2]. Применительно к ФС такими характеристиками могут выступать метаданные файлов, а именно временные отметки (ВО). Обычно в ФС для одного файла хранятся три обязательных ВО: создания, последнего изменения и последнего доступа. В ФС NTFS, с которой работают наиболее распространенные операционные системы линейки Windows, для одного файла существуют четыре ВО: создания (**C**), последнего изменения (**M**), последнего доступа (**A**) и последней модификации метаданных (**X**) файла. Два комплекта таких меток хранятся соответственно в атрибутах файловой записи $STANDARD_INFORMATION и $FILE_NAME [3]. При этом одноименные метки, хранящиеся в различных атрибутах файла, при выполнении ФОп меняются поразному и несут информацию о действиях пользователя. Восстановление интересующей следствие хронологии событий возможно на основе тщательного исследования соотношений указанных 8 ВО.

На сегодняшний день существует несколько работ, посвященных изучению процессов изменения ВО. В этих работах используется единый подход к исследованию, который состоит в том, что закономерности в изменениях ВО выявляются экспериментальным путем. Авторы фиксируют и сравнивают значения ВО до и после совершения анализируемой ФОп. Следует добавить, что подобные исследования выполняются вручную и требуют колоссальных временных затрат и высокой квалификации эксперта. Ниже приведен краткий обзор наиболее информативных исследований.

Т. Кнутсон в работе [4] проводил наблюдения только за ВО из атрибута $STANDARD_INFORMATION в ОС Windows XP, 7, 8. Для извлечения и отображения ВО использовалась программа FTK Imager (версия 3.1.1.8). Опция обновления ВО **A** в ОС Windows 7, 8 была выключена1, а в ОС Windows XP — включена. В результате исследований Т. Кнутсон определил, как изменяются ВО при совершении 3 ФОп: копирование, перемещение, редактирование. В работе перемещение и копирование проводилось как в пределах одного тома с ФС NTFS, так и между томами.

В. Матвеева в работе [5] проводила наблюдения за ВО из атрибутов $STANDARD_INFORMATION и $FILE_NAME в ОС Windows XP, 7. Опция обновления ВО **A** была включена. Для извлечения и отображения ВО использовалась команда «istat» в программе TheSleuthKit (TSK). В результате исследований В. Матвеева определила характер изменений ВО при совершении 8 ФОп: переименование, перемещение, копирование, удаление, открытие, изменение файла, просмотр и изменение его атрибутов. Перемещение и копирование проводилось как в пределах одного тома, так и между томами.

GS. Cho в работе [6] проводил наблюдения за ВО из атрибутов $STANDARD_INFORMATION и $FILE_NAME в ОС Windows 7. Опция обновления ВО **A** была выключена. В результате исследований GS. Cho определил, как изменяются ВО при совершении 5 ФОп: переименование, перемещение, копирование, редактирование файла, изменение его атрибутов. Перемещение и копирование проводилось как в пределах одного тома, так и между томами.

[1] В файловой системе NTFS существует возможность отключать обновление времени последнего доступа к файлам. Согласно документации Microsoft, эта возможность предназначалась для увеличения быстродействия. Чтобы активировать эту опцию необходимо параметр HKLM\System\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate установить в значение 0. В ОС Windows 7, 8, 10 данный параметр по умолчанию выключен. В ходе экспериментов выявлено, что характер изменений ВО зависит от состояния этой опции.

Представленные в [4, 5, 6] исследования позволили авторам выявить ряд закономерностей процесса изменения ВО при выполнении над файлами различных операций и предложить частные методики восстановления последовательности ФОп, которые могут оказаться полезными экспертам-специалистам. Однако эти изыскания носят весьма разрозненный, не системный характер и не обеспечивают полноту исследований и широту охвата разнообразия ФОп и вариантов их выполнения, поэтому не могут являться основой для создания автоматизированного инструментария для восстановления последовательности ФОп. Кроме того, для извлечения требуемой информации о ВО файлов авторы использовали программы, не гарантирующие ее полноту.

Тем не менее, вышеописанные результаты исследований позволяют говорить о целесообразности системного подхода к анализу ВО. Авторами статьи была разработана методика проведения исследования ВО [7, 8]. Методика состоит из трех этапов: подготовка совокупности объектов исследования; совершение множества разнообразных ФОп; фиксирование изменений ВО.

Важное преимущество разработанной методики состоит в том, что в качестве объектов исследования используется специальным образом подготовленный набор файлов разных форматов, размеров (обеспечивается хранение содержимого файла как в файловой записи таблицы MFT, так и во внешних кластерах ФС), с установленными атрибутами («архивный», «только чтение», «системный» или «скрытый»). Исследования проводятся в двух возможных режимах: с включенной и выключенной опцией обновления ВО последнего доступа. Перечень ФОп расширен и охватывает вопросы, которые в большинстве случаев задают эксперту-криминалисту при постановке задачи на проведение компьютерного исследования. ФОп выполняются с использованием различных программ, выбор которых обусловлен статистикой их использования обычными пользователями персональных компьютеров. Кроме того, для реализации методики была создана программа, которая извлекает одновременно все ВО с точностью их хранения 10^{-7} с.

В результате исследований процессов изменения ВО по предложенной методике были получены следующие результаты.

1. Подтверждены результаты исследований GS. Cho, T. Кнутсон, B. Матвеевой для ФОп: копирование, перемещение, редактирование, открытие, удаление файла, просмотр и изменение его атрибутов.

2. Уточнены изменения ВО для ФОп: редактирование в пакете MicrosoftOffice и перемещение между томами (из FAT в NTFS).

Ранее T. Кнутсон определил, что при перемещении из FAT в NTFS у файла ВО **A** и **X** синхронно изменяются, а ВО **C** и **M** наследуются от исходного файла. В результате использования представленной методики дополнительно определено, что ВО **M** округляется до секунд (нули в семи младших разрядах точной ВО), ВО **C** округляется до миллисекунд (нули в пяти младших разрядах точной ВО). Это объясняется тем, что в NTFS точность фиксирования ВО равна 10^{-7} с, а в FAT точность фиксирования ВО **M** равна 1 с, ВО C— 10^{-2} с.

GS. Cho при исследовании операции редактировании файла в приложении MicrosoftOffice обнаружил, что у файла синхронно изменяются ВО **M = A = X**. В результате использования методики дополнительно определено, что изменившиеся ВО не абсолютно идентичны, а имеют некоторые отличия в десятых долях секунд. Это объясняется затянутым процессом сохранения файла на основе глобального шаблона Normal.dot.

3. Обнаружены новые значимые комбинации изменения ВО.

Например, при перемещении файла с установленными атрибутами «только чтение», «системный» или «скрытый» в файловом менеджере TotalCommander ВО **C, M, A** из атрибута $FILE_NAME наследуют значения ВО **C, M, A** из атрибута $STANDARD_INFORMATION соответственно, а ВО **X** из обоих атрибутов синхронно изменяются.

В результате исследований был получен большой объем данных, который был систематизирован и представлен в виде сводной таблицы (см. табл. 1), удобной для их дальнейшего анализа.

Для удобства анализа табл. 1 введены следующие обозначения: символами **«C», «M», «A», «X»** отображены соответственно ВО создания, модификации, последнего доступа к файлу и последней модификации метаданных. Символами **«SI»** обозначены ВО, извлеченные из атрибута $STANDARD_INFORMATION, символами **«FN»** — ВО, извлеченные из атрибута $FILE_NAME. Таким образом, например, **«SIA»** обозначает ВО последнего доступа из атрибута $STANDARD_INFORMATION, а **«FNC»** — ВО создания из

атрибута $FILE_NAME. Серые ячейки таблицы указывают на синхронное изменение ВО после выполнения ФОп. Белые ячейки — на отсутствие изменений. Символом Т в ячейках обозначается время выполнения ФОп, аббревиатуры **SIC, SIM, SIA, SIX** — наследование ВО значений из атрибутов $STANDARD_ INFORMATION.

Сформированная обобщенная таблица изменения ВО позволяет восстанавливать последнюю ФОп, совершенную над файлом. Например, если у исследуемого файла ВО **SIM=SIA=SIX**, и они изменились позже ВО **SIC, FNC, FNM, FNA, FNX,** то по таблице можно определить, что данной комбинации ВО соответствует операция «редактирование». Для того, чтобы восстановить цепочку из нескольких ФОп, необходимо знать возможные комбинации ВО, которые могут возникать при последовательном выполнении тех или

Таблица 1

Таблица изменений ВО

Файловая операция	SI				FN			
	C	M	A	X	C	M	A	X
Копированиев ОС Windows 7 (вкл. SIA) (исходный объект[2])			T					
Копирование (выкл. SIA) (исходный объект)								
Копирование в ОС Windows XP, Windows 8, 10 или в файловых менеджерах TotalCommander, FarManager (новый объект[3])	T		T		T	T	T	T
Копирование в ОС Windows 7 (новый объект)	T		T	T	T	T	T	T
Перемещение/переименование (новый объект)				T	SIC	SIM	SIA	SIX
Перемещение/переименование в файловом менеджере TotalCommander для файлов с установленными атрибутами «только чтение», «системный» или «скрытый» (новый объект)				T	SIC	SIM	SIA	T
Перемещение/переименование из файловой системы FAT в файловую систему NTFS (новый объект)			T	T	T	T	T	T
Просмотр атрибутов (вкл. SIA)			T					
Просмотр атрибутов (выкл. SIA)								
Изменение атрибутов				T				
Открытие в ОС Windows XP в оболочке Explorer(вкл. SIA)			T	T				
Открытиев ОС Windows 7, 8, 10 и в ОС Windows XP (не в оболочке Explorer) (вкл. SIA)			T					
Открытиев ОС Windows 7 (выкл. SIA)				T				
Открытие в ОС Windows XP, Windows 8, 10 или в файловых менеджерах TotalCommander, FarManager(выкл. SIA)								
Исполнение (запуск) в ОС WindowsXP в оболочке Explorer(вкл. SIA)			T	T				

[2] файл, над которым выполняли ФОп.

[3] новый файл, который был создан в результате выполнения ФОп над исходным объектом.

Продолжение таблицы 1

Файловая операция	SI				FN			
	C	M	A	X	C	M	A	X
Исполнение (запуск) в ОС Windows 7, 8, 10 и в ОС WindowsXP (не в оболочке Explorer) (вкл. SIA)			T					
Исполнение (запуск) в ОС Windows 7 (выкл. SIA)				T				
Исполнение (запуск) в ОС WindowsXP, Windows 8, 10 или в файловых менеджерах TotalCommander, FarManager								
Удаление (вкл. SIA)			T	T				
Удаление (выкл. SIA)				T				
Редактирование (вкл. SIA)		T	T	T				
Редактирование (выкл. SIA)		T		T				
Редактирование в пакете MicrosoftOffice		T	T	T		T	T	T
Разархивирование (вкл. SIA) (исходный объект)			T					
Разархивирование (выкл. SIA) (исходный объект)								
Разархивирование архиватором 7-Zip и встроенным архиватором Windows файлов с расширением 7z, rar, tar и архиватором WinRAR файлов с расширением zip, 7z, rar, tar, wim(новый объект)	T		T	T	T	T	T	T
Разархивирование архиваторами 7-Zip и встроенным архиватором Windows файлов с расширением zip (новый объект)				T	T	T	T	T

иных ФОп. На основе таблицы изменений ВО с целью сопоставления возможных последовательностей ФОп наблюдаемым вариантам состояний ВО файлов была разработана модель изменения значений ВО при выполнении ФОп [9]. Эту модель целесообразно было строить на основе теории конечных автоматов, которая традиционно используется для представления динамических систем [10]. В модели в качестве входных символов, которые подаются на вход автомата, рассматриваются ФОп, в качестве состояний автомата — комбинации ВО. Функция переходов между состояниями, сформированная на основе таблицы изменений ВО, описывает, каким образом ФОп изменяют состояния ВО. Адекватность модели подтверждена в ходе многочисленных экспериментов.

Результаты экспериментального исследования по специально разработанной методике, их систематизированное представление в виде таблицы и модель изменения значений ВО позволяют автоматизировать проведение компьютерного исследования, задачей которого является восстановление последовательности ФОп.

Литература

1. Федотов Н.Н. Форензика - компьютерная криминалистика. М.: Юридический мир, 2007. 432 с.

2. Гайдук А.Р. Непрерывные и дискретные динамические системы. М.: УМ и ИЦ « Учебная литература», 2004. 252 с.

3. Кэрриэ Б. Криминалистический анализ файловых систем. СПб. : Питер, 2007. 480 с.

4. Knutson T. Filesystem Timestamps: What Makes Them Tick? 2016. [Электронный ресурс]. Режим доступа: https://www.sans.org/reading-room/whitepapers/forensics/filesystem-timestamps-tick-36842. (дата обращения: 21.12.2020)

5. Матвеева В.С. Криминалистический подход к анализу временных атрибутов файлов в операционной системе семейства MicrosoftWindows и файловой системе NTFS // Безопасность информационных технологий. 2013. Вып. 1.

6. Cho GS. A computer forensic method for detecting timestamp forgety in NTFS // Computer & Security. 34 (2013). С. 36-46.

7. Духан Е.И., Князева Н.С. Методика и результаты исследования изменений временных отметок файловых объектов. // Радиотехника. 2020.Том 84, № 2 (4). С. 64-72.

8. Knyazeva N., Khorkov D., Vostretsova E. Building Knowledge Bases for Timestamp Changes Detection Mechanisms in MFT Windows OS. // Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). 2020. С. 553-556.

9. Knyazeva N., Duhan E. Timestamp Change Model in Windows OS. // Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). 2020. С. 623-626.

10. Перегудов Ф.И., Тарасенко Ф.П. Основы системного анализа. Томск: Изд-во НТЛ, 1997.396 с.

References

1. Fedotov N. Forenzika - Computer Forensics [Forenzika —komp'juternajakriminalistika]. M.: Juridicheskij Mir[M.: The Legal World], 2007. 432 p.

2. Gajduk A. Continuous and Discrete Dynamical Systems [Nepreryvnyeidiskretnyedinamicheskiesistemy]. M.:Uchebno-metodicheskijiizdatel'skijcentr «Uchebnajaliteratura»[M.: Educational-Methodical and Publishing Center «Educational Literature»], 2004. 252 p.

3. CarrierB.File System Forensic Analysis, 2007. 480 p.

4. Knutson T. Filesystem Timestamps: What Makes Them Tick? 2016. available at: https://www.sans.org/reading-room/whitepapers/forensics/filesystem-timestamps-tick-36842.(accessed 21December2020)

5. Matveeva V. Forensic Approach to the Analysis of Temporary File Attributes in the Operating System of the Microsoft Windows Family and the NTFS File System [Kriminalisticheskijpodhod k analizuvremennyhatributovfajlov v operacionnojsistemesemejstva Microsoft Windows ifajlovojsisteme NTFS] // Bezopasnostinformacionnyhtehnologij[Information Technology Security]. 2013. no. 1.

6. Cho GS. A Computer Forensic Method for Detecting Timestamp Forgety in NTFS // Computer & Security. 2013. Vol. 34, pp. 36-46.

7. Duhan E., KnyazevaN. Methodology and Results of the Study of Changes in the Timestamps of File Objects [Metodikairezul'tatyissledovanijaizmenenijvremennyhotmetokfajlovyhobektov]. // Radiotehnika[Radio Engineering]. 2020. Vol. 84, no 2 (4). pp. 64-72.

8. Knyazeva N., Khorkov D., Vostretsova E. Building Knowledge Bases for Timestamp Changes Detection Mechanisms in MFT Windows OS. // Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). 2020. pp. 553-556.

9. Knyazeva N., Duhan E. Timestamp Change Model in Windows OS. // Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). 2020. pp. 623-626.

10. Peregudov F., Tarasenko F. Fundamentals of System Analysis [Osnovysistemnogoanaliza]. Tomsk: Izd-vo NTL[Tomsk: Publishing House of Scientific and Technical Literature]. 1997.396 p.

ДУХАН Евгений Изович, доктор технических наук, доцент, доцент учебно-научного центра «Информационная безопасность, Уральский Федеральный Университет им. первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 32. E-mail: eduhan@pm.convex.ru

КНЯЗЕВА Наталия Сергеевна, старший преподаватель учебно-научного центра «Информационная безопасность», Уральский Федеральный Университет им. первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 32. E-mail: npalceva@inbox.ru

DUHAN Evgenij, Doctor of Technology, Associate Professor, Associate Professor of educational and scientific center «Information security», Ural Federal University named after the first President of Russia B.N.Yeltsin, 620002, Yekaterinburg, Mira str., 32. E-mail: eduhan@pm.convex.ru

KNYAZEVA Natalija, Senior lecturer of educational and scientific center «Information security», Ural Federal University named after the first President of Russia B.N.Yeltsin, 620002, Yekaterinburg, Mira str., 32. E-mail: npalceva@inbox.ru

УДК 336.717:004 Вестник УрФО № 1(39) / 2021, с. 27–35

Фельдман Е. В., Ручай А. Н., Чербаджи Д. Ю.

DOI: 10.14529/secur210104

МОДЕЛЬ ВЫЯВЛЕНИЯ АНОМАЛЬНЫХ БАНКОВСКИХ ТРАНЗАКЦИЙ НА ОСНОВЕ МАШИННОГО ОБУЧЕНИЯ

Данная статья посвящена разработке надежной модели выявления аномальных банковских транзакций, которые могут участвовать в схемах отмывания денег и нелегального оборота товаров и услуг. В статье была предложена модель выявления аномальных банковских транзакций на основе машинного обучения. Для обучения и оценки модели используется набор данных CreditCardFraud, состоящий из 284807 транзакций кредитных карт: 492 имеют класс «незаконные», 284315 имеют класс «законные». В предлагаемой модели выявления аномальных банковских транзакций были использованы различные алгоритмы машинного обучения с подбором гиперпараметров. Для оценки предложенной модели использовалась метрика доля верных ответов, точность, полнота, F1 метрика и индекс сбалансированной точности. С помощью алгоритма ресэмплинга в условиях несбалансированности классов удалось повысить надежность классификации аномальных банковских транзакций по сравнению с лучшим известным результатом на наборе данных CreditCardFraud.

Ключевые слова: *банковские транзакции, классификация, выявления аномальных транзакций, машинное обучение.*

Feldman E. V., Ruchay A. N., Cherbadzhi D. Y.

MODEL FOR DETECTING ABNORMAL BANKING TRANSACTIONS BASED ON MACHINE LEARNING

This article is devoted to the development of a reliable model for detecting abnormal banking transactions that may be involved in money laundering and illegal trafficking of goods and services. The article proposed a model for detecting abnormal banking transactions based on machine learning. For training and evaluation of the model, the CreditCardFraud dataset is used, consisting of 284807 Bitcoin transactions: 492 of "illegal" and 284315 of "legal". The pro-

posed model for detecting abnormal bitcoin transactions is based on various machine learning algorithms with the selection of hyperparameters. To evaluate the proposed model, we used the metric of accuracy, precision, recall, F1 score, and index of balanced accuracy. Using the resampling algorithm in conditions of class imbalance, it was possible to increase the reliability of the classification of abnormal banking transactions in comparison with the best-known result on the CreditCardFraud dataset.

Keywords: *transactions, classification, detection of abnormal transactions, machine learning.*

1. Введение

Исходя из отчетов компании Nilson, занимающейся анализом банковских транзакций, общий объем денежных средств, потерянных в результате мошенничества еще в 2016 году, достиг отметки в 22,8 миллиардов долларов, а уже в 2019 году было зафиксировано значение 28,7 миллиардов долларов. Это только подтверждает необходимость того, чтобы банки научились распознавать мошенничество заранее, еще до того, как оно произошло.

Все международные платежные системы (VISA, MasterCard, PayPal и другие) имеют свои системы антифроды, предназначенные для оценки транзакций на предмет их подозрительности с точки зрения мошенничества. Как правило, антифрод состоит из списков, фильтров и правил, по которым проверяются все транзакции. В России тоже используются антифроды для поимки лиц, занимающихся мошенническими действиями в сфере информационных технологий. Но особенно остро стоит вопрос выявления нелегального оборота товаров и услуг. Такой инструмент был бы полезен для выявления незаконных транзакций по обороту товаров и услуг [1].

Данная статья посвящена разработке модели выявления аномальных банковских транзакций на основе машинного обучения. Мы используем набор данных CreditCardFraud [2], состоящий из более чем 200 тысяч банковских транзакций с помощью банковских карт.

В данной статье в предлагаемой модели выявления аномальных транзакций биткоинов были использованы следующие алгоритмы машинного обучения: линейная регрессия, квадратичная регрессия, логистическая регрессия, k-ближайших соседей, деревья решений, случайный лес, наивный байесовский классификатор, метод опорных векторов, классификатор на основе многослойных Персептронов, линейный дискриминантный анализ, квадратичный дискриминантный анализ, адаптивный бустинг. Кроме того, в работе были использованы методы оптимизации гиперпараметров для алгоритмов машинного обучения, что позволило бы повысить надежность классификации.

Было сделано одно важное наблюдение, что набор данных CreditCardFraud является несбалансированным (492 <<незаконные>> и 284315 <<законные>>). Поэтому были выполнены эксперименты по повышению надежности классификации аномальных транзакций биткоинов с помощью алгоритмов ресэмплинга в условиях несбалансированности классов. Благодаря чему удалось повысить надежность классификации аномальных транзакций биткоинов по сравнению с лучшим известным результатом на наборе данных CreditCardFraud [2].

2. Набор данных

Для разработки модели выявления аномальных транзакций необходимо иметь подготовленный большой набор данных для обучения модели. Поскольку дело касается банковских операций, в открытом доступе отсутствуют подходящие наборы данных. Существует единственный набор данных CreditCardFraud, который содержит транзакции, совершенные европейскими держателями кредитных карт в сентябре 2013 года. В этом наборе данных представлены транзакции, которые произошли за два дня. За это время было обнаружено 492 мошенничества из 284 807 транзакций. Набор данных сильно несбалансирован, поскольку на положительный класс (мошенничество) приходится 0,172% всех транзакций.

Набор данных CreditCardFraud содержит только числовые признаки, которые являются результатом преобразования исходных значений признаком методом главных компонент. Из-за проблем с конфиденциальностью невозможно получить исходные функции и дополнительную информацию о данных. Признаки V1, V2, …, V28 являются основными компонентами, полученные с помощью метода главных компонент. Единственными открытыми признаками являются признаки

«Time» и «Amount». Признак «Time» содержит секунды, прошедшие между каждой транзакцией и первой транзакцией в наборе данных. Признак «Amount» отображает сумму транзакции. Признак «Class» является меткой правильного ответа, которая принимает значение 1 в случае мошенничества и 0 в противном случае.

3. Модель выявления аномальных банковских транзакций с помощью машинного обучения

Задачей машинного обучения является поиск целевой функции f: X ⟶ Y, где X — набор входных данных и Y — набор выходных переменных. Процесс поиска этой целевой функции f называется обучением с учителем или построение модели. Целевая функция может быть найдена только при наличии достаточного количества помеченных данных. В выбранном наборе данных все записи являются размеченными.

Так как поиск точной целевой функции является очень сложной задачей, то зачастую на практике она аппроксимируется приближенной функцией. То есть при процессе обучения ищется определенная функция h, наилучшим образом аппроксимирующая неизвестную целевую функцию f. Для обучения модели требуется выборка из исходного набора данных, как правило, составляющая 70% от исходного объема данных. Далее настраиваются параметры модели. Для этого используется валидационный набор, объем которого обычно берется как 20% обучающих данных. Предсказательная способность модели оценивается с использованием тестового набора, которая составляет 30% от набора данных.

В модели выявления аномальных банковских транзакций есть набор данных M, который состоит из n = 284807 транзакций, а также метка ответа, показывающая, является ли данная транзакция незаконной или законной. С каждой транзакцией связан вектор признаков, состоящий из 30 значений. Для целевой функции f требуется определить, является ли конкретная транзакция m незаконной (в этом случае он принимается за 1) или законным (в этом случае принимается значение 0). Целевая функция f может быть найдена с помощью одного из алгоритма машинного обучения для набора из n помеченных транзакций.

Для выявления аномальных банковских транзакций, в работе были использованы следующие алгоритма машинного обучения: линейная регрессия; квадратичная регрессия; логистическая регрессия; k-ближайших соседей; деревья решений; случайный лес; наивный байесовский классификатор; метод опорных векторов; классификатор на основе многослойных персептронов; линейный дискриминантный анализ; квадратичный дискриминантный анализ; адаптивный бустинг; градиентный бустинг.

Поскольку задача сводится к тому, что нужно определить является ли данная транзакция законной или незаконной, то в общем виде это представляется как задача бинарной классификации, где за положительный класс — это набор незаконных транзакций, а за отрицательный — незаконные.

Далее, рассмотрим общие метрики оценки, используемые в моделях машинного обучения.

Доля правильных ответов (Accuracy) — показатель того, как часто классификатор делает правильные предсказания, и равен

$$\frac{TP+TN}{TP+TN+FP+FN},$$

где TP (True Positive) — это число положительных результатов, которые были корректно предсказаны моделью и принадлежат к положительному классу; TN (True Negative) — это число отрицательных результатов, которые были корректно предсказаны моделью и принадлежат к отрицательному классу; FP (False Positive) — это число положительных результатов, которые были некорректно предсказаны моделью и принадлежат к отрицательному классу; FN (False Negative) — это число отрицательных результатов, которые были некорректно предсказаны моделью и принадлежат к положительному классу. Значения FP и FN также часто называют ошибками первого и второго рода.

Точность (Precision) — это показатель

$$\frac{TP}{TP+FP},$$

измеряющий коэффициент правильности классификатора, когда он правильно предсказывает положительную метку класса для положительного класса.

Полнота (Recall) — это показатель

$$\frac{TP}{TP+FN},$$

оценивающий как часто классификатор предсказывает положительную метку для данных, когда данные действительно принадлежат положительному классу.

F1 метрика (F1 Score) — гармоническое среднее точности и полноты, которая рассчитывается следующим образом:

$$F1 = 2\frac{Precision \cdot Recall}{Precision + Recall}.$$

Метрика F1 располагается в отрезке между 0 и 1.

Геометрическое среднее (Geometric mean (Gmean)) — это показатель, равный $\sqrt{TP + TN}$, который используется для того чтобы максимизировать положительные и отрицательные результаты классификаций, предсказанные верно и сохраняя между ними баланс. Нужно помнить о том, что геометрическое среднее сводит негативное влияние перекосов распределения классов к минимуму, но оно не объясняет вклад каждого из классов в общие показатели, потому что дает одинаковый результат для разных комбинаций TP и TN.

Доминирование (Dominance) — это показатель TP – TN, используемый для оценки разницы между TP и TN.

В статье [3] была предложена метрика под названием индекс сбалансированной точности (Index of Balanced Accuracy (IBA)). IBA нужен для оценки бинарного классификатора, в котором данные являются несбалансированными. IBA может быть рассчитан как

$$IBA = (1 + Dominance) \cdot Gmean^2.$$

При замене Dominance и Gmean итоговая формула предоставляет полезную информацию для изучения того, как IBA поддерживает баланс между Dominance и Gmean, также для Dominance можно добавить взвешенный параметр α, который расположен на отрезке $0 \leq \alpha \leq 1$.

$$IBA = (1 + \alpha(TP - TN)) \cdot TP \cdot TN.$$

Однако, если $\alpha = 0$, то IBA равняется $Gmean^2$.

Так как в представленном наборе данных количество незаконных транзакций равняется 492 против 284807 законных, то этот набор является несбалансированным. Класс будем называть миноритарным, когда в наборе данных доля экземпляров некоторого класса слишком мала, а другой класс — мажоритарным, когда он сильно представлен в наборе данных.

Для решения проблемы несбалансированности данных есть несколько подходов. Одним из них является применение различных стратегий ресемплинга (resampling).

Восстановление баланса классов может происходить двумя методами. В первом случае удаляют некоторое количество экземпляров мажоритарного класса (undersampling), во втором — с помощью синтетических данных увеличивают количество экземпляров миноритарного класса(oversampling).

Для решения проблемы несбалансированности данных был выбран алгоритм Tomek Links [4]. Все мажоритарные экземпляры, которые входят в связи Томека, можно удалить из набора данных. Алгоритм Tomek Links направлен на то, чтобы удалить экземпляры, которые можно рассматривать как зашумленные.

4. Результаты экспериментов

Для реализации алгоритма нахождения аномальных транзакций с помощью машинного обучения, использовался язык программирования Python 3, поскольку он больше всего приспособлен для выполнения задач такого рода, а также имеет отличную производительность при обработке данных. Стоит отметить, что в Python есть множество готовых фреймворков и библиотек, которые существенно упрощают процесс написания кода и сокращают время на разработку.

Для работы с данными была выбрана библиотека Pandas, которая использует высокоуровневые структуры данных. Выбор пал именно в пользу Pandas так как в ней есть встроенные методы для группировки, комбинирования и фильтрации данных. Pandas позволяет извлекать данные из различных источников, таких как базы данных SQL, файлы CSV, Excel, JSON для последующей обработки и изучения.

В качестве среды разработки был выбран Google Collab, поскольку в нем уже установлены основные библиотеки, требуемые в разработке. Стоит отметить простоту использования, высокую производительность и отказоустойчивость данного сервера.

Реализация включала в себя несколько этапов:

- Загрузка данных и базовое изучение
- Предобработка данных
- Визуализация
- Обучение

Для обучения данных важно грамотно изучить содержимое исходной таблицы на предмет пропущенных значений. Поэтому в первую очередь было проверено, есть ли в таблицах пропуски. Оказалось, что все значения заданы, значит, их все можно использовать в дальнейшем.

Далее, было решено проверить записи на

предмет уникальности. Оказалось, что не все данные являются таковыми и из 284807 записей уникальными были 283726. Помня небольшое количество аномальных транзакций, было решено узнать, сколько из 1081 транзакции, которые повторяются, являются мошенническими. Был получен следующий результат: не все неуникальные транзакции являются легитимными, 19 из них является аномальными.

Так как набор данных изначально являлся сильно несбалансированным с количеством мажоритарных записей равных 492, важно, что процент их уникальности порядка 96 процентов.

Исходя из вышеописанного, было принято решение исключить неуникальные записи из набора данных и работать с оставшимися 283726 строками. Как в дальнейшем показала практика, именно на этом наборе данных процент точности обучения немного выше.

Таким образом, уже на получившемся наборе данных был испробован метод решения проблемы несбалансированности данных: алгоритм Tomek Links. При помощи этого алгоритма, из полученного набора данных были удалены еще 248 записей из доминирующего класса, которые попадают под условие связи Томека. В дальнейшем использование данного алгоритма позволило повысить процент точности обучения.

Для реализации задачи классификации транзакций было принято решение попробовать различные комбинации алгоритмов машинного обучения из готовых библиотек.

Также для реализации задачи классификации данных, к исходному набору данных были применены различные методы функционального преобразования. Данные методы особенно полезно в машинном обучении, так как различные метрики могут измеряться в разных диапазонах, или значения одного метрики варьируются слишком сильно. Функциональное преобразование можно разделить на нормализацию и стандартизацию данных. Нормализация подразумевает изменение диапазонов в данных без изменения формы распределения, в то время как стандартизация изменяет форму распределения данных. Обычно достаточно нормализовать данные, тогда как стандартизацию стоит применять при использовании алгоритмов, которые основываются на измерении расстояний, например, k-ближайших соседей или метод опорных векторов.

В качестве тестовой и обучающей выборок были отобраны транзакции, помеченные как легитимные или аномальные в соотношении 30:70 соответственно. С помощью выбранных алгоритмов была обучена модель выявления аномальных банковских транзакции транзакций.

Для оценки надежности обученных моделей были рассчитаны метрики: доля верных ответов (accuracy), точность (precision), полнота (recall), F1 метрика (F1 Score) и индекс сбалансированной точности (IBA).

В ходе работы были опробованы следующие вариации обучения модели выявления аномальных банковских транзакций:

1. С удалением повторяющихся исходных данных и без (2 варианта);

2. С оптимизацией данных при помощи алгоритма Tomek Links и без (2 варианта);

3. С нормализаторами данных MinMax Scaler, MaxAbsScaler, StandardScaler, Power Transformer, QuantileTransfomer, Normalizer, FunctionTransformer, PolynomialFeatures, RobustScaler и без (10 вариантов);

4. С различными методами машинного обучения: RandomForest, AdaBoost, K-Neighbors, DecisionTree, LogisticRegression, SVC, CatBoost, XGBoost, LGBM, Tpot, AutoSklearn (11 вариантов);

Всего получается 440 различных комбинаций.

В результаты работы метода машинного обучение RandomForest было замечено, что точность построенной модели увеличилась на 0.0001, если использовать алгоритм Tomek Links. Поэтому в дальнейшем, с каждым из следующих методов применялась эта оптимизация данных. Что касается работы с удалением повторяющихся исходных данных, то их наличие никак не повлияло на точность модели.

В таблице 1 представлены результаты работы метода машинного обучения RandomForest с различными нормализаторами данных. Видно, что лучше всего себя проявили следующие функции масштабирования: StandardScaler, PowerTransformer, QuantileTransformer, Normalizer. Данные нормализаторы показали одинаковую точность, но за счет индекса IBA, лучшим методом масштабирования для данной задачи является QuantileTransformer, подтверждая теоретические тезисы о том, что данный скейлер разработан для задач классификации.

В таблице 2 представлены лучшие резуль-

Таблица 1

Сравнение методов нормализации

Нормализатор	Accuracy	IBA
MinMaxScaler	0.9998	0.9012
MaxAbsScaler	0.9998	0.9111
StandardScaler	0.9999	0.9225
PowerTransformer	0.9999	0.9256
QuantileTransformer	0.9999	0.9306
Normalizer	0.9999	0.9199
RobustScaler	0.9998	0.9056
FunctionTransformer	0.9998	0.9168
PolynomialFeatures	0.9998	0.9044

таты для каждого метода машинного обучения. Стоит отметить, что показатели Precision, Recall и F1 Score считались отдельно для каждого из классов транзакций. Таблица 1 отображает лучшие результаты именно для аномальных незаконных банковских транзакций, так как для оценки эффективности детектирования транзакций в большей степени важно анализировать ошибки для класса незаконных транзакций. Из таблицы 2 видно, что лучшие показатели точности были достигнуты в методах: RandomForest, CatBoost, XGBoost, Tpot, AutoSklearn.

Поскольку методы Tpot и AutoSklearn являются автоматизированными и сами подбирают лучшие гиперпараметры и методы обучения, то в таблице 2 представлены вариации этих методов, которые дали лучший резуль-

Таблица 2

Сравнение методов машинного обучения

Метод	Precision	Recall	F1 Score	Accuracy	IBA
RandomForestClassifier	0.9866	0.9366	0.9610	0.9999	0.9306
AdaBoost	0.8113	0.7273	0.7670	0.9993	0.7073
K-Neighbors	0.6881	0.6773	0.6993	0.9985	0.6885
DecisionTree	0.9129	0.9302	0.9215	0.9997	0.9236
LogisticRegression	0.7047	0.6913	0.6980	0.9990	0.6697
SVM	0.6425	0.6772	0.6328	0.9983	0.6567
CatBoost	0.9799	0.9281	0.9533	0.9998	0.9214
XGBoost	0.9820	0.9239	0.9521	0.9998	0.9168
LGBM	0.5313	0.8161	0.5634	0.9979	0.7997
Tpot	0.9888	0.9366	0.9620	0.9999	0.9306
AutoSklearn	0.9930	0.9006	0.9446	0.9998	0.8917

тат. Для Tpot это оказался метод XGBClassifier с параметрами: learning_rate=0.5, max_depth=7, min_child_weight=1, n_estimators=100, n_jobs=1, subsample=0.8, а для AutoSklearn это был метод RandomForest с параметрами: learning_rate=0.5, max_depth=10, min_child_weight=1, n_estimators=100, n_thread=1, subsample=0.7

Заметив, что параметры получаются примерно одинаковые, было принято решение не заниматься перебором гиперпараметров, а обучать модели на различных методах с этими же гиперпараметрами.

основе машинного обучения. Аномальными являются банкоские транзакции, которые могут быть использованы в схеме отмывания денег или незаконного оборота товаров и услуг. Для обучения и оценки данной модели был использован набор данных, состоящий из 284807 транзакций, из которых 492 являются нелегальными, а остальные входят в класс легитимных. В предложенной модели обнаружения аномальных транзакций использовались различные алгоритмы машинного обучения. С помощью алгоритма пересчета Tomek Links в условиях несбалансиро-

Таблица 3

Сравнение результатов с другими работами

Метод	Precision	Recall	F1 Score	Accuracy	IBA
RandomForestClassifier	0.9866	0.9366	0.9610	0.9999	0.9306
CatBoost	0.9799	0.9281	0.9533	0.9998	0.9214
XGBoost	0.9820	0.9239	0.9521	0.9998	0.9168
Tpot	0.9888	0.9366	0.9620	0.9999	0.9306
AutoSklearn	0.9930	0.9006	0.9446	0.9998	0.8917
LogisticRegression[5]	0.99	0.90	0.94	0.94	-
K-Neighbors[5]	0.99	0.86	0.92	0.93	-
SVM[5]	0.99	0.88	0.93	0.93	-
LogisticRegression[6]	0.9226	0.9184	-	0.9315	-
Autoencoders[7]	0.84	0.74	0.79	0.8341	-
IsolationForest[8]	-	-	-	0.8049	-

В таблице 3 отображены лучшие результаты, достигнутые в ходе данной работы и в других статьях. С этой целью были взяты результаты из работ [5], [6], [7], [8], в которых так же строились модели выявления аномальных транзакций на этом же наборе данных. Метрики Precision, Recall, F1 Score, IBA указаны для аномальных транзакций, если же они не подсчитаны, то стоит прочерк. Видно, что полученные в ходе данного исследования результаты, являются точнее, чем ранее полученные.

5. Заключение

В данной была предложена модель выявления аномальных банковских транзакций на

ванных классов и различных методов функционального преобразования удалось повысить достоверность классификации. В результате, надежность предложенной модели обнаружения аномальных транзакций на основе алгоритмов Tpot и RandomForest составляет 0,9999. Это значение на порядок выше, чем в проводимых на этом же наборе данных исследованиях [5], [6], [7], [8].

Литература

1. Фельдман Е.В. Противодействие совершению бесконтактных преступлений с использованием цифровых технологий // Вестник УрФО. Безопасность в информационной сфере. 2020. № 2 (36). С. 49-55.

2. Набор данных CreditCardFraud [Электронный ресурс] // Kaggle, Inc. URL: https://www.kaggle.com/mlg-ulb/CreditCardFraudfraud

3. Garcia V., Mollineda R.A., Sanchez J.S. Index of Balanced Accuracy: A Performance Measure for Skewed Class Distributions. Pattern Recognition and Image Analysis. IbPRIA 2009. Lecture Notes in Computer Science, vol 5524. Springer, Berlin, Heidelberg.

4. Tomek I. Two modifications of CNN // IEEE Trans. Syst. Man Cybern., vol. 6, 1976, 769–772.

5. In depth skewed data classif [Электронный ресурс] // Kaggle, Inc. URL: https://www.kaggle.com/joparga3/in-depth-skewed-data-classif-93-recall-acc-now

6. Semi Supervised Classification using AutoEncoders [Электронный ресурс] // Kaggle, Inc. URL: https://www.kaggle.com/shivamb/semi-supervised-classification-using-autoencoders

7. Выявление мошенничества с помощью алгоритмов случайного леса, нейронного автокодировщика и изолирующего леса [Электронный ресурс] // Habr, Inc. URL: https://habr.com/ru/company/nix/blog/478286/

8. 9 подходов для выявления аномалий [Электронный ресурс] // Habr, Inc. URL: https://habr.com/ru/post/477450/

References

1. Fel'dman E.V. Protivodejstvie sovershheniyu beskontaktnyh prestuplenij s ispol'zovaniem cifrovyh tekhnologij // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. 2020. № 2 (36). S. 49-55.

2. CreditCardFraud // Kaggle, Inc. URL: https://www.kaggle.com/mlg-ulb/CreditCardFraudfraud

3. Garcia V., Mollineda R.A., Sanchez J.S. Index of Balanced Accuracy: A Performance Measure for Skewed Class Distributions. Pattern Recognition and Image Analysis. IbPRIA 2009. Lecture Notes in Computer Science, vol 5524. Springer, Berlin, Heidelberg.

4. Tomek I. Two modifications of CNN // IEEE Trans. Syst. Man Cybern., vol. 6, 1976, 769–772.

5. In depth skewed data classif // Kaggle, Inc. URL: https://www.kaggle.com/joparga3/in-depth-skewed-data-classif-93-recall-acc-now

6. Semi Supervised Classification using AutoEncoders // Kaggle, Inc. URL: https://www.kaggle.com/shivamb/semi-supervised-classification-using-autoencoders

7. Vyyavlenie moshennichestva s pomoshch'yu algoritmov sluchajnogo lesa, nejronnogo avtokodirovshchika i izoliruyushchego lesa // Habr, Inc. URL: https://habr.com/ru/company/nix/blog/478286/

8. 9 podhodov dlya vyyavleniya anomalij // Habr, Inc. URL: https://habr.com/ru/post/477450/

ФЕЛЬДМАН Елена Васильевна, старший преподаватель кафедры компьютерной безопасности и прикладной алгебры; Челябинский государственный университет. 454001, Россия, Челябинск, ул. Братьев Кашириных, 129. E-mail: mila008.is@gmail.com

РУЧАЙ Алексей Николаевич, кандидат физико-математических наук, доцент, заведующий кафедрой компьютерной безопасности и прикладной алгебры. Челябинский государственный университет. 454001, Россия, Челябинск, ул. Братьев Кашириных, 129.; доцент кафедры защиты информации, Южно-Уральский государственный университет (национальный исследовательский университет). 454080, Россия, г. Челябинск, пр. им. В.И. Ленина, 76. E-mail: ran@csu.ru

Чербаджи Дмитрий Юрьевич, студент математического факультета, Челябинский государственный университет. 454001, Россия, Челябинск, ул. Братьев Кашириных, 129. E-mail: enorot@gmail.com

FELDMAN Elena, Senior Lecturer of the Department of Computer Security and Applied Algebra; Chelyabinsk State University. 454001, Russia, Chelyabinsk, st. Brothers Kashirins, 129. E-mail: mila008.is@gmail.com

RUCHAY Alexey, PhD in Physics and Mathematics, Associate Professor, Head of the Department of Computer Security and Applied Algebra; Chelyabinsk State University. 454001, Russia, Chelyabinsk, st. Brothers Kashirins, 129.; Associate Professor, Department of Information Security, South Ural State University (National Research University). 454080, Russia, Chelyabinsk, etc. them. IN AND. Lenin, 76. E-mail: ran@csu.ru

CHERBADZHI Dmitry, student of the Faculty of Mathematics, Chelyabinsk State University. 454001, Russia, Chelyabinsk, st. Brothers Kashirins, 129. E-mail: enorot@gmail.com

УДК 004.056.5:61

Вестник УрФО № 1(39) / 2021, с. 36–42

Мухачев С. В., Кобяков А. В.

DOI: 10.14529/secur210105

ОБ ИСПОЛЬЗОВАНИИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В УСЛОВИЯХ БОРЬБЫ С ПАНДЕМИЕЙ

В статье рассматриваются особенности применения информационных технологий в условиях борьбы с пандемией в России. Рассмотрены основные направления использования таких технологий для борьбы с пандемией и профилактике заболеваемости. Обсуждаются особенности их применения и изменение способов использования с течением времени; отмечены региональные особенности. Обращено внимание на возникшие правовые сложности применения информационных технологий, связанные с вопросами информационной безопасности.

Делается вывод об эффективности применения информационных технологий в борьбе с пандемией.

Ключевые слова: *информационные технологии, пандемия, covid-19, информационная безопасность, оповещение, цифровой пропуск, правовое регулирование.*

Mukhachev S. V., Kobyakov A. V.

ON THE USE OF INFORMATION TECHNOLOGIES IN THE FIGHT AGAINST THE PANDEMIC

The article discusses the features of the use of information technologies in the fight against the pandemic in Russia. The main directions of using such technologies to combat the pandemic and prevent morbidity are considered. The features of their application and changes in the ways of use over time are discussed; regional features are noted. Attention is drawn to the legal difficulties that have arisen in the application of information technologies related to information security issues.

The conclusion is made about the effectiveness of the use of information technologies in the fight against the pandemic.

Keywords: *information technology, pandemic, covid-19, information security, notification, digital pass, legal regulation.*

Пандемия Covid-19 стала одним из наиболее значимых общемировых явлений последнего года. Она повлияла на все стороны жизни населения земного шара. Пожалуй, еще никогда не предпринимались столь масштабные меры по борьбе с заболеванием и его распространением.

Россия не стала исключением. Фактически все сферы деятельности государственных структур подверглись испытанию на прочность: управление, медицина, правоохранительные органы, информационное обеспечение и другие.

Цифровые информационные технологии стали эффективным инструментом для организации борьбы с пандемией, противодействия распространению новой инфекции. Задействованы все виды информационных систем: государственные, муниципальные, а также иные информационные системы [1]. Они продемонстрировали эффективность в оповещении населения, управлении силами и средствами, реализации ограничительных мер. Вместе с тем, выявились и определенные сложности, связанные с некоторыми аспектами информационной безопасности, нормативно-правовым регулированием применения информационных технологий в особых условиях пандемии.

Можно перечислить основные направления работы государственных органов в информационном пространстве в условиях пандемии: информирование населения; контроль за перемещением здорового населения; контроль за инфицированными гражданами; моделирование и прогнозирование развития эпидемиологической обстановки.

Остановимся на них подробнее.

Информирование населения должно происходить при помощи средств массовой информации и иных каналов информации [2]. Для решения этой задачи привлекается Федеральное автономное учреждение ОКСИОН [3] с целью использования общероссийской комплексной системы информирования и оповещения населения в местах массового пребывания людей (ОКСИОН). Она представляет собой организационно-техническую систему, объединяющую аппаратно-программные средства обработки, передачи и отображения аудио и видеоинформации. ОКСИОН изначально создана для решения задач в области гражданской обороны, а также для защиты от чрезвычайных ситуаций, обеспечения пожарной безопасности, безопасности на водных объектах и охраны общественного порядка, своевременного оповещения и оперативного информирования граждан о ЧС и угрозе террористических акций, мониторинга обстановки и состояния правопорядка в местах массового пребывания людей на основе использования современных технических средств и технологий. Система предназначена для эффективного решения задач информирования граждан. Согласно методическим рекомендациям Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий[4], основными каналами для информирования населения являются: СМС-рассылка сообщений; информирование абонентов операторов фиксированной телефонной связи; информирование через средства массовой информации; информирование в местах массового пребывания; информирование на наземном общественном транспорте; подвижные средства информирования.

Исходя из сложившейся ситуации, следует отметить, что наиболее хорошо зарекомендовали себя каналы информирования через СМС-рассылку сообщений и средства массовой информации. Связано это с тем, что были введены ограничения, связанные с местонахождением граждан вне мест постоянного проживания, что затруднило обращение их к другим каналам информирования. СМС-рассылка использовалась и до пандемии. СМС-сообщения использовались МЧС, Росгидрометом и иными государственными органами для информирования граждан о возможных опасностях, иных важных событиях. Данный канал показал свою эффективность и во время пандемии. И такая эффективность обусловлена, прежде всего, наличием мобильной связи практически у всех граждан.

Однако следует обратить внимание и некоторые недостатки и сложности в организации СМС-рассылки в условиях пандемии Covid-19. Например, отсутствовало широкое и понятное информирование о введении обязательного режима самоизоляции для граждан всех возрастов, когда таковой вводился в том или ином регионе; о правилах нахождения на улице; о введении дополнительных требований, таких как обязательное использование лицевых масок; об официальной статистике заражений. Такое информирование было бы крайне полезно и удалось бы избежать ряда негативных явлений. На-

пример, одна из проблем – распространение недостоверной информации среди населения (а порой и откровенной дезинформации). И в этой ситуации следует опереться на каналы ведомств, которым население безусловно доверяет. Согласно опросам населения в г. Москве, уровень доверия населения в вопросах безопасности наиболее высок у МЧС [5]. Информация, полученная через каналы МЧС, воспринимается как максимально достоверная.

Еще одна сложность связана с многократным дублированием информации в рассылках. Хотя понятно, что диктуется это стремлением достичь повышенного внимания, но может приводить к противоположному результату. Повторное отправление сообщений может негативно влиять на восприятие информации, распространяемой по данному каналу, так как психологически это ассоциируется со спамом. Часть получателей могут блокировать сообщения на своих мобильных устройствах. Данная тенденция опасна и может привести к сокращению количества граждан, охватываемых через этот канал информирования.

Информирование через средства массовой информации (в том числе социальные сети) можно рассмотреть на примере информирования населения Свердловской области. Здесь информирование претерпело в своем развитии несколько различных условных периодов.

Для начального периода было характерно следующее: количество информации об инфекции, распространяемой через СМИ и социальные сети, чрезмерно, источники часто недостоверны, интерес граждан к данной теме максимален. Эти обстоятельства обусловили стремление к перепроверке полученной информации. В борьбу с недостоверной информацией включился Роскомнадзор [6]. Надежные каналы взаимодействия власти с населением Свердловской области были неустойчивы. Этот период условно длился с 2 марта (когда оперативный штаб сообщил, что у гражданина России, вернувшегося на родину из Италии, подтвердился коронавирус) по 5 апреля 2020 года. Завершение данного периода связано с выступлением президента России В. В. Путина, в котором разъяснялись меры борьбы с пандемией, текущее состояние, и, в частности, говорилось о том, что нерабочие дни продлены по 30 апреля.

Следующий период – промежуточный. Количество информации об инфекции, поступающей через СМИ и социальные сети, велико. Однако появляются более надежные каналы взаимодействия власти с населением. Интерес населения к тематике, связанной с пандемией, по-прежнему велик. Количество недостоверной информации быстро сокращается. К официальным и надежным источникам информации можно отнести чат Оперативного штаба по Свердловской области, инстаграм-аккаунт губернатора (https://www.instagram.com/evgenykuyvashev/) и специальные разделы на интернет-ресурсах средств массовой информации, связанные с инфекцией и проходящие модерацию. Данный период длился по 16 апреля. Окончание этого периода можно связать с заявлением губернатора Свердловской области Е. В. Куйвашева о введении режима обязательной самоизоляции до особо распоряжения.

И, наконец, завершающий, третий период. Количество информации об инфекции в СМИ и социальных сетях постепенно уменьшается. Происходит потеря интереса у населения к тематике, связанной с пандемией, в связи с насыщением информацией. В этот период население обращается к региональным новостям, что связано ссамостоятельностью принятия решений об изменение режима самоизоляции губернатором. Региональные СМИ преимущественно ссылаются на региональные министерства и сообщения губернатора (например, на инстаграм-аккаунт губернатора, где он постоянно отвечает на вопросы населения Свердловской области). Устанавливается устойчивый канал информирования о пандемии, что повышает достоверность информации. Начало этого периода – середина мая, и он продолжается по настоящее время.

Следующее направление – контроль за перемещением здорового населения.

Один из главных факторов, снижающих заболеваемость в период пандемии, максимальное сокращение физических контактов с инфицированными людьми. Были разработаны ограничительные меры, направленные на длительное нахождение граждан дома. Данные ограничения были названы «самоизоляцией». Вначале обязательная самоизоляция распространялась только на граждан старше 65 лет, а для иных возрастов она носила лишь рекомендательных характер. Но с 30 марта 2020 года в Москве ввели обязательную самоизоляцию для всех возрастов. Передви-

гаться вне жилищ допускалось только по неотложным причинам и к месту работы. На следующий день режим обязательной самоизоляции ввели ещё в 26 регионах России. На 2 апреля режим обязательной самоизоляции был введён в 79 регионах, а к 27 апреля во всех регионах был введен режим повышенной готовности. Появилась острая необходимость контроля за перемещением граждан.

Каждый регион решал проблему контроля в соответствии со своими техническими возможностями. В большинстве регионов использовались цифровые пропуска, что позволило избежать скопления людей при выдаче бумажных документов. Однако в нескольких регионах использовались бумажные пропуска, процесс получения которых стал причиной массовых скоплений людей [7,8].

Наиболее развитая в техническом и организационном отношении система цифровых пропусков была применена в Москве. Для получения пропуска служили веские причины: необходимость нахождение гражданина на рабочем месте, посещение медицинской организации или иные. Алгоритм получения был изложен официальном сайте мэра Москвы [9]. Срок действия определялся в соответствии с целью поездки. Получить пропуск можно несколькими способами: с помощью интернет-портала mos.ru или звонка по специальному номеру, а также через СМС-сообщение. После подачи заявления принимается решение о выдаче или невыдаче пропуска, о чем заявитель уведомляется через сайт, СМС-сообщением или письмом на электронную почту (в соответствии со способом оформления заявки). Контроль за перемещением в городе был организован жестко. Пропуск прикрепляется к транспортным картам и государственным номерам автомобиля, что исключает самовольное перемещение на общественном или личном транспорте в черте города. При проведении проверки гражданин обязан предъявить специальный буквенно-цифровой или QR-код своего пропуска.

При использовании цифровых пропусков в Москве возникли некоторые трудности. На стадии бета-тестирования приложения «Социальный мониторинг» были отмечены недоработки, связанные с информационной безопасностью. Приложение при установке на мобильное устройство запрашивало права на доступ ко всей информации, имеющейся в памяти устройства, передавало собранную информацию на серверы мэрии Москвы в открытом виде, без шифрования, и использовало зарубежные системы для распознавания лиц [10]. Это вызвало общественный резонанс, одна из политических партий отправила жалобу в Роскомнадзор [11].

После официального введения системы цифровых пропусков также вскрылись недостатки. Например, выяснилось, что в начале внедрения системы можно было указать любую из работающих компаний и получить свой пропуск, не являясь сотрудником указанной фирмы. Спустя некоторое время такие пропуска были аннулированы [12], а система доработана.

На первоначальном этапе существовала проблема с организацией проверкой пропусков. С этим связана, например, ситуация, когда 15 апреля на входе в метро Москвы скопились огромные очереди [13]. В дальнейшем система цифровых пропусков была подключена к автоматизированным средствам видео фиксации и нарушения стали регистрироваться в автоматическом режиме.

Следует отметить некоторые правовые коллизии, возникшие при реализации системы цифровых пропусков. Прежде всего, они связаны с обработкой и передачей персональных данных без прямого выражения согласия граждан.

Следует также отметить, что ситуация с пропускным режимом различных регионах России сильно различается. В некоторых пропускная система отсутствует (г. Санкт-Петербург, Свердловская обл., Ленинградская область); в других нет системы цифровых пропусков и они выдаются исключительно в бумажном виде (Краснодарский край, Челябинская обл., Пермской обл. и др.). Имеются регионы, в которых реализованы цифровые пропуска собственной разработки (Красноярский край, Нижегородская область, Республика Татарстан и др.). Реализованы цифровые пропуска, построенные на платформе Минкомсвязи России (Забайкальский край, Костромская область, Тульская область и др.). В регионах, где внедрена система цифровых пропусков, основной принцип работы состоит в том, что гражданину нужно отправить СМС-сообщение на специальный номер и получить в ответ буквенно-цифровой код или заполнить анкету на официальном интернет-ресурсе администрации региона.

Оповещение граждан о статистике пандемии, режиме ограничения передвижения,

особенностях заболевания, мерах профилактики было организовано с применением различных информационных технологий: телерадиовещание, интернет-ресурсы, рассылка СМС-сообщений. Основной системой для оповещения граждан считается телерадиовещание, которое позволяет охватить большую часть населения. Телерадиовещание было задействовано для трансляции обращений главы государства, информационных сводок и разъяснения решений органов власти.

Другой канал информирования – интернет-ресурсы. Перечислим основные.

Портал Правительства Российской Федерации Стопкоронавирус.рф [14] содержит официальную информацию о коронавирусе в России. Имеет рубрики: «О коронавирусе», «Меры правительства», «Что предпринять», «Вопросы и ответы», «Полезная информация». Из названия рубрик следует, что публикуется исчерпывающая информация о коронавирусе и развитии пандемии.

Другой ресурс «Коронавирус: статистика», созданный Интернет-порталом Яндекс. Здесь публикуется следующая статистическая информация: динамика пандемии по регионам России, России в целом, в других странах, в мире в целом; уровень активности на текущую дату в мегаполисах мира по сравнению с самым оживлённым днем февраля-марта[15].

Таким образом, информационные технологии нашли широкое применение в условиях борьбы с пандемией. Оповещение населения о пандемии и мерах борьбы с ней, организация различных мер, предотвращающих ее распространение, информирование о количестве инфицированных – вот далеко не полный перечень областей применения современных информационных технологий. Конечно, обозначились определенные проблемы и сложности, связанные с широким применением таких технологий – начиная с психологических особенностей восприятия информации населением и заканчивая проблемами информационной безопасности и нормативно-правового регулирования этой сферы.

Литература

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»//СПС КонсультантПлюс.

2. Федеральный закон от 21.12.1994 № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера»// СПС КонсультантПлюс.

3. ФАУ «ИЦ ОКСИОН» [Электронный ресурс]. – Режим доступа: URL:https://www.mchs.gov.ru/ministerstvo/uchrezhdeniya-mchs-rossii/federalnye-avtonomnye-uchrezhdeniya/fau-ic-oksion(дата обращения 18.01.2021).

4. Методические рекомендации по созданию системы информирования и оповещения населения[Электронный ресурс]. – Режим доступа: URL:https://06.mchs.gov.ru/deyatelnost/napravleniya-deyatelnosti/grazhdanskaya-zashchita/5-preduprezhdenie-chrezvychaynyh-situaciy/metodicheskie-rekomendacii-po-zn-i-t-ot-chs/metodicheskie-rekomendacii-po-sozdaniyu-sistemy-informirovaniya-i-opoveshcheniya-naseleniya(дата обращения 18.01.2021).

5. Материалы социологических исследований и опросов общественного мнения в 2019 году[Электронный ресурс]. – Режим доступа: URL:https://www.mos.ru/dsmir/documents/socio/view/233095220/(дата обращения 18.01.2021).

6. Роскомнадзор потребовал у СМИ и социальных сетей удалить ложную информацию о коронавирусе [Электронный ресурс]. – Режим доступа: URL:https://rkn.gov.ru/news/rsoc/news72366.htm(дата обращения 18.01.2021).

7. Толпы россиян скопились в очередях за пропусками для автомобилей[Электронный ресурс]. Режим доступа: URL:https://www.mk.ru/auto/2020/04/03/tolpy-rossiyan-skopilis-v-ocheredyakh-za-propuskami-dlya-avtomobiley.html(дата обращения 18.01.2021).

8. Жители Зеленогорска выстроились в огромные очереди за пропусками из города[Электронный ресурс]. Режим доступа: URL:https://www.enisey.tv/news/post-21292/(дата обращения 18.01.2021).

9. Цифровые пропуска: как будет работать пропускная система в городе[Электронный ресурс]. – Режим доступа: URL:https://www.mos.ru/mayor/themes/2299/6434050/(дата обращения 18.01.2021).

10. Приложение для слежки за москвичами «Социальный мониторинг» убрали из GooglePlay [Электронный ресурс]. – Режим доступа: URL:https://habr.com/ru/news/t/495088/(дата обращения 18.01.2021).

11. Роскомнадзор обещал проверить «Социальный мониторинг» при появлении в открытом

доступе[Электронный ресурс]. Режим доступа: URL:https://www.interfax.ru/russia/702003(дата обращения 18.01.2021).

12. Мэрия Москвы объяснила аннулирование рабочих пропусков с верным ИНН [Электронный ресурс]. Режим доступа: URL:[Электронный ресурс]. – Режим доступа:URL:https://www.rbc.ru/society/21/04/2020/5e9f1f079a794793df375f02(дата обращения 18.01.2021).

13. Собянин назвал очереди в метро из-за проверок пропусков критичными [Электронный ресурс]. – Режим доступа: URL:https://ria.ru/20200415/1570065653.html(дата обращения 18.01.2021).

14. Стопкоронавирус.рф. [Электронный ресурс]. – Режим доступа: URL:https://xn--80aesfpebagmfblc0a.xn--p1ai/(дата обращения 18.01.2021).

15. Коронавирус: статистика[Электронный ресурс]. – Режим доступа: URL:https://yandex.ru/covid19/stat(дата обращения 18.01.2021).

References

1. Federal'nyy zakon ot 27.07.2006 № 149-FZ «Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii»//SPS Konsul'tantPlyus.

2. Federal'nyy zakon ot 21.12.1994 № 68-FZ «O zashchite naseleniya i territoriy ot chrezvychaynykh situatsiy prirodnogo i tekhnogennogo kharaktera»// SPS Konsul'tantPlyus.

3. FAU «ITS OKSION» [Elektronnyy resurs]. – Rezhim dostupa: URL:https://www.mchs.gov.ru/ministerstvo/uchrezhdeniya-mchs-rossii/federalnye-avtonomnye-uchrezhdeniya/fau-ic-oksion(data obrashcheniya 18.01.2021).

4. Metodicheskiye rekomendatsii po sozdaniyu sistemy informirovaniya i opoveshcheniya naseleniya[Elektronnyy resurs]. – Rezhim dostupa: URL:https://06.mchs.gov.ru/deyatelnost/napravleniya-deyatelnosti/grazhdanskaya-zashchita/5-preduprezhdenie-chrezvychaynyh-situaciy/metodicheskie-rekomendacii-po-zn-i-t-ot-chs/metodicheskie-rekomendacii-po-sozdaniyu-sistemy-informirovaniya-i-opoveshcheniya-naseleniya(data obrashcheniya 18.01.2021).

5. Materialy sotsiologicheskikh issledovaniy i oprosov obshchestvennogo mneniya v 2019 godu[Elektronnyy resurs]. – Rezhim dostupa: URL:https://www.mos.ru/dsmir/documents/socio/view/233095220/(data obrashcheniya 18.01.2021).

6. Roskomnadzor potreboval u SMI i sotsial'nykh setey udalit' lozhnuyu informatsiyu o koronaviruse [Elektronnyy resurs]. – Rezhim dostupa: URL:https://rkn.gov.ru/news/rsoc/news72366.htm(data obrashcheniya 18.01.2021).

7. Tolpy rossiyan skopilis' v ocheredyakh za propuskami dlya avtomobiley[Elektronnyy resurs]. Rezhim dostupa: URL:https://www.mk.ru/auto/2020/04/03/tolpy-rossiyan-skopilis-v-ocheredyakh-za-propuskami-dlya-avtomobiley.html(data obrashcheniya 18.01.2021).

8. Zhiteli Zelenogorska vystroilis' v ogromnyye ocheredi za propuskami iz goroda[Elektronnyy resurs]. Rezhim dostupa: URL:https://www.enisey.tv/news/post-21292/(data obrashcheniya 18.01.2021).

9. Tsifrovyye propuska: kak budet rabotat' propusknaya sistema v gorode[Elektronnyy resurs]. – Rezhim dostupa: URL:https://www.mos.ru/mayor/themes/2299/6434050/(data obrashcheniya 18.01.2021).

10. Prilozheniye dlya slezhki za moskvichami «Sotsial'nyy monitoring» ubrali iz GooglePlay [Elektronnyy resurs]. – Rezhim dostupa: URL:https://habr.com/ru/news/t/495088/(data obrashcheniya 18.01.2021).

11. Roskomnadzor obeshchal proverit' «Sotsial'nyy monitoring» pri poyavlenii v otkrytom dostupe[Elektronnyy resurs]. Rezhim dostupa: URL:https://www.interfax.ru/russia/702003(data obrashcheniya 18.01.2021).

12. Meriya Moskvy ob"yasnila annulirovaniye rabochikh propuskov s vernym INN [Elektronnyy resurs]. Rezhim dostupa: URL:[Elektronnyy resurs]. – Rezhim dostupa:URL:https://www.rbc.ru/society/21/04/2020/5e9f1f079a794793df375f02(data obrashcheniya 18.01.2021).

13. Sobyanin nazval ocheredi v metro iz-za proverok propuskov kritichnymi [Elektronnyy resurs]. – Rezhim dostupa: URL:https://ria.ru/20200415/1570065653.html(data obrashcheniya 18.01.2021).

14. Stopkoronavirus.rf. [Elektronnyy resurs]. – Rezhim dostupa: URL:https://xn--80aesfpebagmfblc0a.xn--p1ai/(data obrashcheniya 18.01.2021).

15. Koronavirus: statistika[Elektronnyy resurs]. – Rezhim dostupa: URL:https://yandex.ru/covid19/stat(data obrashcheniya 18.01.2021).

МУХАЧЕВ Сергей Валентинович, кандидат физико-математических наук, доцент, доцент кафедры «Информационные технологии и защита информации», Уральский государственный университет путей сообщения. 620034, г. Екатеринбург, ул. Колмогорова, 66. E-mail: msv62@yandex.ru

КОБЯКОВ Антон Васильевич, студент, Уральский государственный университет путей сообщения. 620034, г. Екатеринбург, ул. Колмогорова, 66. E-mail: ant-kobyakov-2k@yandex.ru

MUKHACHEV Sergey, candidate of physical and mathematical Sciences, associate Professor, associate Professor of the Department of information technology and information security, Ural State University of Railway Transport. 620034, Yekaterinburg, st. Kolmogorov, 66. E-mail: msv62@yandex.ru

KOBYAKOV Anton, student, Ural State University of Railway Transport. 620034, Yekaterinburg, st. Kolmogorov, 66. E-mail: ant-kobyakov-2k@yandex.ru

АКТУАЛЬНЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ

УДК 004.056.5

Вестник УрФО № 1(39) / 2021, с. 43–53

Абдулин А. А., Соколов А. Н.

DOI: 10.14529/secur210106

ИССЛЕДОВАНИЕ ПРОГРАММНЫХ РЕШЕНИЙ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ СЕТЕЙ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ[1]

В статье представлены исследования современных программных решений обеспечения информационной безопасности промышленных сетей. Функциональные возможности выбранных продуктов классифицированы в соответствии с требованиями архитектуры адаптивной безопасности: обнаружение угроз, реагирование на инциденты, прогнозирование возникновения инцидентов, предотвращение возникающих угроз. Проведен сравнительный анализ выбранных систем обеспечения информационной безопасности промышленных сетей. Выделены универсальные программные решения обеспечения информационной безопасности промышленных сетей, а так программные продукты, наиболее подходящие для тех или иных направлений обеспечения информационной безопасности.

Ключевые слова: *Автоматизированная система управления технологическим процессом, система контроля уязвимостей, SCADA-система, оркестровка безопасности, система обнаружения угроз.*

[1] Исследование выполнено при финансовой поддержке гранта РФФИ и Челябинской области в рамках научного проекта № 20-47-740006

RESEARCH OF SOFTWARE SOLUTIONS FOR PROVIDING INFORMATION SECURITY OF INDUSTRIAL NETWORKS OF AUTOMATED PROCESS CONTROL SYSTEMS

The article presents studies of modern software solutions for information security of industrial networks. The functionality of the selected products is classified according to the requirements of the adaptive security architecture: threat detection, incident response, incident prediction, prevention of emerging threats. A comparative analysis of the selected information security systems for industrial networks was carried out. The universal software solutions of information security of industrial networks are distinguished, and also the software products which are the most suitable for these or those directions of information security.

Keywords: *Automated process control system, vulnerability control system, SCADA system, security orchestration, threat detection system.*

С началом периода внедрения вычислительной техники в системы управления связано появление термина «автоматизированная система управления» (АСУ). Будучи задействованными в критической инфраструктуре промышленных сетей, автоматизированные системы управления технологическими процессами (АСУ ТП) строятся на основе отказоустойчивой, высоконадежной вычислительной техники. Это техника промышленного исполнения, созданная специально для долговременной, круглосуточной эксплуатации на индустриальных объектах. Последствия сбоя или отказа работы систем представляет серьезную угрозу для оборудования, а также для жизни и здоровья людей.

АСУ ТП имеет стандартную трехзвенную структуру, и какой бы ни была ее отказоустойчивость, средний её уровень — SCADA-системы, — является наиболее уязвимым, и позволяет злоумышленнику производить ряд манипуляций с технологическим процессом, в том числе вопреки отказоустойчивости.

Безопасность АСУ ТП – это практика защиты сетей диспетчерского управления и сбора данных (SCADA), общей структуры систем управления, используемых в промышленных операциях. Эти сети отвечают за автоматическое, дистанционное управление необходимыми товарами и услугами, такими как вода, природный газ, электричество и транспорт для миллионов людей. SCADA является одним из наиболее распространенных типов систем управления производством (ICS).

Эти сети, как и любая другая сеть, находятся под угрозой кибератак, которые могут быстро и с тяжелыми последствиями разрушить любую часть критической инфраструктуры, если не будет обеспечена надлежащая безопасность. Капитальные затраты – еще одна ключевая проблема: системы SCADA могут стоить организации от десятков тысяч до миллионов долларов. По этим причинам важно, чтобы организации внедряли надежные меры безопасности SCADA для защиты своей инфраструктуры, которые могут потенциально пострадать от сбоев, вызванных внешней атакой или внутренней ошибкой [1, с. 4].

За последние годы подходы к обеспечению безопасности АСУ ТП значительно изменились. До появления компьютеров единственным способом мониторинга сети SCADA была группа из нескольких человек на каждой станции для подготовки отчетности о состоянии каждой системы. На более загруженных станциях постоянно работали технические специалисты для ручного управления сетью и связи по телефонным линиям.

Только после появления локальных сетей (LAN) и достижений в направлении миниатюризации систем, стали видимыми достижения в развитии АСУ ТП, такие как, например, распределенная сеть SCADA. Позже появились сетевые системы, которые смогли обмениваться данными через глобальную сеть (WAN) и соединять вместе множество других компонентов.

Начиная с местных компаний и заканчивая федеральными правительствами, каждая организация, которая работает с системами SCADA, уязвима. Эти угрозы могут иметь далеко идущие последствия, как для экономики, так и для общества. Угрозы для сетей SCADA можно разбить на несколько групп:

• **Хакеры** – отдельные лица или группы лиц со злым умыслом. Получив доступ к ключевым компонентам SCADA, хакеры могут развязать хаос в организации, который может варьироваться от перебоев в обслуживании до кибервойны.

• **Malware** – вредоносное ПО, включая вирусы, шпионское и вымогательское ПО, которое представляет опасность для систем SCADA. Несмотря на то, что вредоносное ПО может специально не предназначаться для самой сети, оно все же может представлять угрозу для ключевой инфраструктуры, которая помогает управлять сетью SCADA. Это включает в себя мобильные приложения, которые используются для мониторинга и управления системами SCADA.

• **Террористы** – в отличие от «хакеров», целью которых является получение денег, руководствуются стремлением создать хаос и причинить как можно ущерба.

• **Сотрудники** – могут создавать внутренние угрозы, которые могут быть не менее разрушительными, чем внешние (от ошибки, связанной с человеческим фактором, до недовольного сотрудника или подрядчика). Важно, чтобы безопасность SCADA устраняла эти риски.

Управление современными сетями SCADA без принятия надлежащих мер безопасности может создавать серьезные риски. Многие сети по-прежнему не имеют необходимых систем обнаружения и мониторинга, и это делает их уязвимыми для атак. Поскольку сетевые атаки SCADA используют как киберфизические, так и физические уязвимости, необходимо соответствующим образом согласовать меры кибербезопасности [2].

Системы контроля уязвимостей — один из эффективных методов противодействия промышленным киберугрозам. Это узкопрофильные программы, разработанные специально для промышленных систем автоматизации. Они позволяют определить целостность внутренней среды устройства, зафиксировать все попытки изменить прикладную программу контроллера, изменения в конфигурации сетевых устройств защиты и управления в энергосетях.

В ходе исследования были выбраны ключевые пункты, представленные в таблице 1, такие как:

1) обнаружение угроз нулевого дня, уязвимость нулевого дня;

2) возможность интеграции с центром обеспечения безопасности, с системами управления информационной безопасностью;

3) анализ и обнаружение аномалий сетевого трафика;

4) возможность инвентаризации устройств;

5) оркестровка безопасности — это стек решений программ, собирающий данные об угрозах безопасности из нескольких источников и реагировать на события безопасности низкого уровня без помощи человека;

6) наличие функции пассивного мониторинга сети;

7) формирование журналов учета событий;

8) отображение топологии сети и возможность ее сегментации;

9) возможность мультиместного и безагентонго развёртывания и т.д.

Исследование представленных программных решений позволило сделать следующие выводы.

Nozomi Networks предлагает единое решение для контроля рисков в режиме реального времени. Высокая точность и минимальность ложных срабатываний достигается за счет инновационного использования искусственного интеллекта и машинного обуче-

Таблица 1

Программные решения обеспечения информационной безопасности промышленных сетей

Возможности	NOZOMI (NG)	CLAROTY	CYBERX Platform	DRAGOS ICP	Forescout PLATFORM	INDEGY ICS	Kaspersky (KICS)
1. Обнаружение угроз							
Обнаружение аномалий	Yes	Yes	Yes	Yes			Yes
Автоматическое обнаружение активов	Yes		Yes	Yes	Yes	Yes	
Обнаружение потока				Yes			Yes
Обнаружение PLC- и RTU-устройств			Yes	Yes		Yes	Yes
Отображение топологии сети	Yes	Yes	Yes	Yes		Yes	Yes
Инвентаризация устройств	Yes	Yes	Yes	Yes		Yes	
Фильтры просмотра	Yes	Yes	Yes	Yes		Yes	Yes
Обнаружение мошеннических устройств	Yes		Yes		Yes	Yes	Yes
Обнаружение угроз нулевого дня	Yes		Yes			Yes	Yes
Обнаружение угроз с контекстом	Yes	Yes	Yes	Yes	Yes		
ICS анализ угроз			Yes	Yes		Yes	Yes
Глубокий анализ пакетов (DPI)			Yes	Yes	Yes	Yes	Yes
Сегментация сети	Yes				Yes		
Зеркалирование портов			Yes	Yes		Yes	Yes
2. Реагирование на инциденты							
Смягчение событий безопасности	Yes			Yes	Yes	Yes	
Оповещения Data Historian	Yes		Yes	Yes		Yes	
Контроль приложений	Yes	Yes		Yes	Yes	Yes	Yes
3. Прогнозирование возникновения инцидентов							
Анализ трафика	Yes		Yes	Yes		Yes	Yes
Оркестровка безопасности			Yes	Yes	Yes	Yes	
Мониторинг изменений	Yes	Yes		Yes		Yes	

Продолжение таблицы 1

Отчет об оценке уязвимости	Yes		Yes	Yes	Yes	Yes	Yes
Постоянный мониторинг		Yes	Yes			Yes	Yes
Журнал событий		Yes				Yes	Yes
4. Предотвращение угроз							
Смягчение событий безопасности	Yes			Yes	Yes	Yes	
Оповещения Data Historian	Yes		Yes	Yes		Yes	Yes
Контроль периметра	Yes	Yes		Yes	Yes	Yes	Yes

ния. Интегрированная инфраструктура безопасности включает встроенные интеграции для систем управления активами и идентификацией, SIEM [3].

Основные функциональные возможности системы Nozomi Networks (рис. 1):

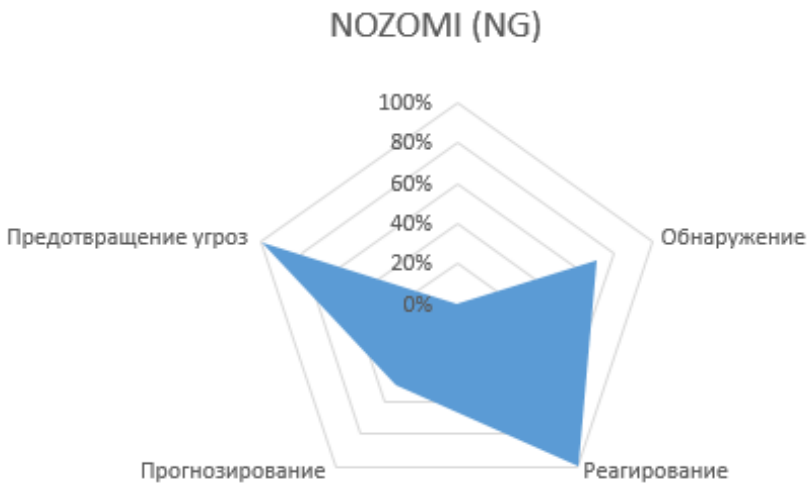


Рис. 1. Функциональные возможности NOZOMI (NG)

1. Обнаружение:
• обнаружение аномалий на основе поведения;
• правила и сигнатурное обнаружение;
• продвинутая корреляция для детального понимания и быстрое восстановление;
• OT ThreatFeed для существующих угроз и уязвимостей.
2. Реагирование:
• автоматический захват пакета;
• снимки системы TimeMachine.
3. Прогнозирование:
• мониторинг изменений;
• отчет об оценке уязвимости.
4. Предотвращение угроз:
• смягчение событий безопасности;
• оповещения Data Historian;
• контроль периметра.

Claroty Platform предоставляет группам безопасности исключительную видимость в промышленных сетях управления и мониторинг в режиме реального времени. Мониторинг способен распознать продвинутые угрозы и вовремя выявить уязвимости сети. Платформа позволяет сегментировать сеть, контролировать и предоставлять безопасный удаленный доступ, составлять детализированные политики доступа и записывать сеансы [4].

Основные функциональные возможности системы Claroty Platform (рис. 2):

1. Обнаружение:
• постоянный мониторинг (обнаружение угроз с контекстом, мониторинг изменений);
• обнаружение вредоносной активности и рискованных изменений в течение всей атаки «kill-chain».

2. Реагирование:

• контекстные оповещения для быстрой сортировки и расследования;

• формирование автоматизированного ответа на основе существующей сетевой инфраструктуры.

3. Прогнозирование:

• превентивно выявляет и устраняет уязвимости, неверные конфигурации и незащищенные соединения.

4. Предотвращение угроз:

• точные периодические запросы активов ОТ и ИТ;

• безопасный запрос ресурсов ICS и не-ICS для улучшения видимости конфигураций активов;

• расширенный контекст для предупреждений и уязвимостей.

Платформа **CyberX** обеспечивает непрерывный мониторинг угроз ICS и обнаружение активов, объединяя глубокое понимание промышленных протоколов, устройств и приложений с определением поведенческих аномалий, специфичным для ICS, анализом угроз, анализом рисков и автоматизированным моделированием угроз.

Безагентная платформа безопасности CyberX ОТ позволяет клиентам автоматически обнаруживать ИТ-активы, видеть топологию сети, выявлять критические уязвимости и векторы атак. Решение дает возможность постоянно отслеживать ОТ сети на предмет разрушительных кибератак [5].

Основные возможности системы CYBERX Platform (рис. 3):

1. Обнаружение:

• непрерывный мониторинг;

• поведенческая аналитика с самообучением;

• запатентованные алгоритмы с поддержкой ICS.

2. Реагирование:

• возможности глубокой криминалистической экспертизы, расследования и поиска угроз;

• полноценные PCAP для анализа детализации;

• встроенная интеграция на уровне приложений с IBM QRadar, Splunk и ServiceNow.

3. Прогнозирование:

• автоматизированное моделирование угроз для прогнозирования наиболее вероятных путей векторов атак;

• определение базовых моделей поведения и конфигураций;

• собственный специфический для ICS анализ угроз (нулевые дни, вредоносные программы, злоумышленники).

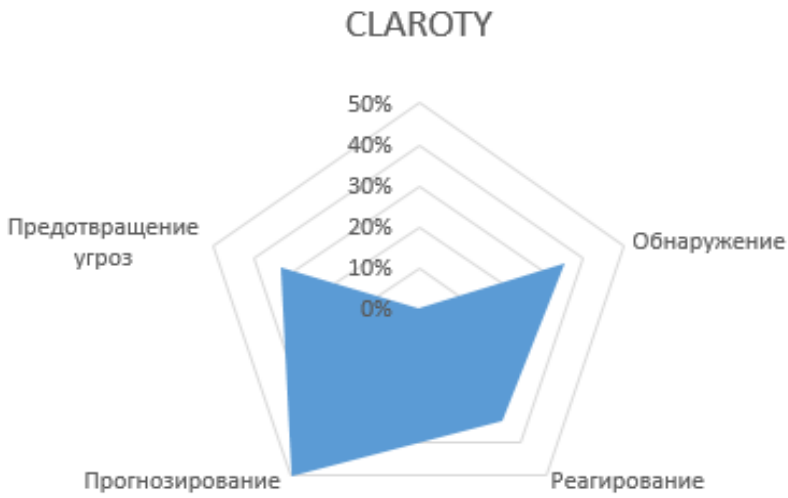


Рис. 2. Функциональные возможности CLAROTY Platform

4. Предотвращение угроз:

• запатентованные оценки рисков и уязвимостей, характерные для ICS, включая обнаружение активов;

• упреждающая, основанная на оценке риска приоритизация действий по смягчению последствий для защиты критических активов;

• интеграция с ведущими технологиями предотвращения, включая межсетевые экраны следующего поколения, однонаправленные шлюзы и безопасный удаленный доступ, защита привилегированных учетных записей.

Dragos Industrial Cybersecurity Platform — это защитное решение для промышленных сетей, которое автоматически находит и идентифицирует активы сети. Программа сканирует активы, находя неправильные настройки, возможности улучшения конфигурации. В случае выявления подозрительной активности, платформа предоставляет пошаговое руководство к расследованию и реагированию на инцидент и инструменты для устранения неполадок [6].

Forescout Platform — единая платформа, позволяющая применять адаптивные, детализированные политики и быстро просматривать результаты, используя существующую физическую и виртуальную сетевую инфраструктуру [7]. Основные функциональные возможности Forescout Platform (рис. 5):

1. Обнаружение:
- автоматическое обнаружение активов;
- обнаружение мошеннических устройств;
- обнаружение угроз с контекстом;

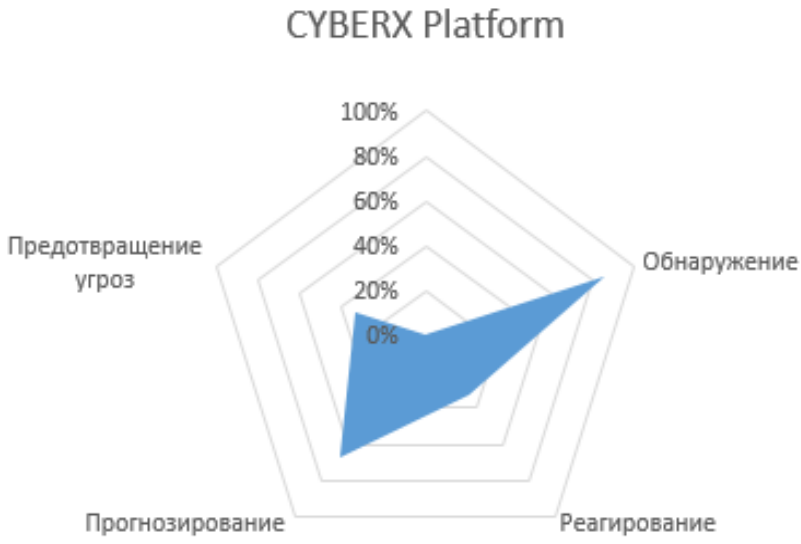


Рис. 3. Функциональные возможности CYBERX Platform

Основные возможности системы Dragos Industrial Cybersecurity Platform (рис. 4):

1. Обнаружение:

Сложные характеристики тактик, методов и процедур противника с помощью анализа поведения угроз выявляют злонамеренную активность в сетях ICS и предоставляют подробный контекст для предупреждений.

2. Реагирование:
- смягчение событий безопасности;
- оповещения Data Historian;
- контроль приложений.

3. Прогнозирование:

Глубокая проверка пакетов (DPI) протоколов ICS, характеристик трафика и активов, возможность использования журналов узлов и событий контроллера, а также интеграция с активами ICS, такими как исторические данные, обеспечивают полное представление о средах ICS.

4. Предотвращение угроз:
- смягчение событий безопасности;
- оповещения Data Historian;
- контроль периметра.
- глубокий анализ пакетов (DPI);
- зеркалирование портов.

2. Реагирование:
- смягчение событий безопасности;
- контроль периметра.

3. Прогнозирование:
- оркестровка безопасности;
- отчет об оценке уязвимости.

4. Предотвращение угроз:
- смягчение событий безопасности;
- контроль периметра.

Indegy Industrial Cybersecurity Suit обеспечивает отслеживание активов, обнаружение и смягчение угроз, управление уязвимостями и обеспечение целостности устройства. Она способна защитить сеть не только от зловредного вмешательства, но и от непреднамеренных человеческих ошибок [8].

Основные возможности Indegy Industrial Cybersecurity Suit (рис. 6):

1. Обнаружение:
- автоматическое обнаружение пакетов;
- пассивный мониторинг сети.

2. Реагирование:

Рис. 4. Функциональные возможности DRAGOS ICP

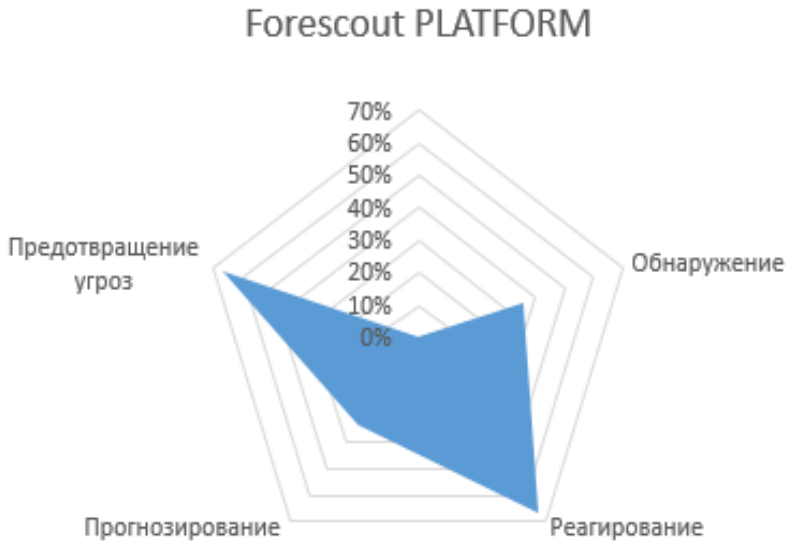


Рис. 5. Функциональные возможности Forescout Platform

• смягчение событий безопасности;
• оповещения Data Historian;
• контроль периметра.
3. Прогнозирование:
• анализ трафика;
• оркестровка безопасности;
• мониторинг изменений;
• отчет об оценке уязвимости;
• постоянный мониторинг;
• журнал событий.
4. Предотвращение угроз.

Kaspersky Industrial CyberSecurity – это набор технологий и сервисов, призванный защитить промышленные системы всех уровней (включая серверы SCADA, панели HMI, инженерные рабочие станции, ПЛК, сетевые соединения и персональное оборудование), сохраняя при этом стабильность и непрерывность технологических процессов. Каждая промышленная среда уникальна, поэтому решение адаптируемо под конкретную отрасль – например, нефтегазовый сектор, энергетические сети, производство. При этом решение не влияет на непрерывность технологических процессов [9].

Основные возможности Kaspersky Industrial CyberSecurity (рис. 7).

1. Обнаружение:
• обнаружение аномалий;
• обнаружение потока;
• обнаружение PLC- и RTU-устройств;
• отображение топологии сети;

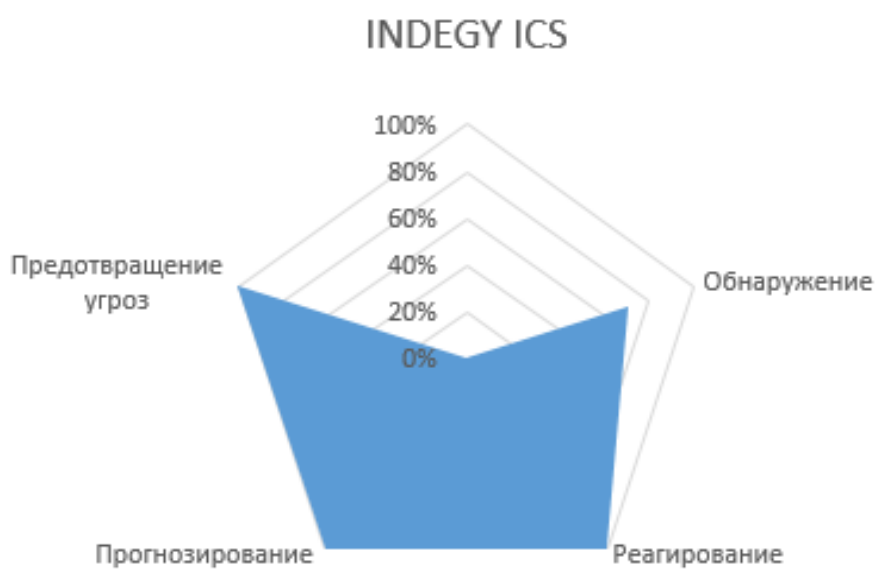


Рис. 6. Функциональные возможности INDEGY ICS

Рис. 7. Функциональные возможности Kaspersky (KICS)

- инвентаризация устройств;
- фильтры просмотра;
- обнаружение мошеннических устройств;
- обнаружение угроз нулевого дня;
- ICS анализ угроз;
- глубокий анализ пакетов (DPI);
- сегментация сети;
- зеркалирование портов.

2. Реагирование:
- контроль приложений.

3. Прогнозирование:
- анализ трафика;
- оркестровка безопасности;
- мониторинг изменений;
- отчет об оценке уязвимости;
- постоянный мониторинг;
- журнал событий.

4. Предотвращение угроз:
- оповещения Data Historian;
- контроль периметра.

На основе проведенных исследований можно сделать вывод, что наиболее полным функционалом для обеспечения всех четырех требований архитектуры адаптивной безопасности, обладают продукты DRAGOS ICP и INDEGY ICS.

Полученные результаты позволяют выбрать подходящие решения для конкретной

ситуации. Если, например, необходима система только для обнаружения угроз, наиболее подходящим вариантом является CYBERX Platform, которая обладает возможностями автоматического обнаружения устройств, топологии сети, аномалий, мошеннических устройств и т.д.

NOZOMI (NG) и Forescout Platform специализируются на предотвращении и реагировании на возникающие угрозы. Эти программные продукты имеют возможности контроля периметра и приложения, а так же систему оповещения Data Historian, что позволяет наиболее эффективно бороться с возникающими угрозами.

Kaspersky Industrial CyberSecurity имеет наиболее полный функционал в области обнаружения, предотвращения и прогнозирования угроз. Для эффективного прогнозирования будущих угроз, Kaspersky Industrial CyberSecurity имеет систему постоянного мониторинга трафика, его глубокого анализа, обнаружение аномалий.

Литература

1. Абдулин А.А. Методы оценки уязвимостей автоматизированных систем управления технологическими процессами /Абдулин А.А., Соколов А.Н. //Сборник трудов XVII Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых «Безопасность информационного пространства», г. Челябинск, 2018, с 4 – 9.

2. Кибербезопасность АСУ ТП. Обзор специализированных наложенных средств защиты [Электронный ресурс] – https://www.anti-malware.ru/analytics/Market_Analysis/ICS-security-review (дата обращения: 03.11.2020).

3. Industrial Strength OT and IoT Security and Visibility [Электронный ресурс] – https://www.nozominetworks.com/downloads/US/Nozomi-Networks-Guardian-Data-Sheet.pdf (дата обращения: 19.11.2020).

4. Continuous Threat Detection [Электронный ресурс] – https://cdn2.hubspot.net/hubfs/2553528/CTDdatasheet.pdf (дата обращения: 14.01.2021).

5. Learn why industrial control systems are soft targets for adversaries [Электронный ресурс] – https://cyberx-labs.com/resources/risk-report-2019/ (дата обращения: 03.02.2021).

6. Industrial Control Threat Intelligence Whitepaper [Электронный ресурс] – https://www.dragos.com/resource/industrial-control-threat-intelligence-whitepaper/ (дата обращения: 15.12.2020).

7. The Forescout Platform Complete Situational Awareness for the Extended Enterprise [Электронный ресурс] – https://www.forescout.com/platform/ (дата обращения: 01.12.2020).

8. The Indegy IndustrialCybersecurity Suite [Электронный ресурс] – https://cdn2.hubspot.net/hubfs/2755567/The%20Indegy%20Industrial%20Cybersecurity%20eBook%202019.pdf (дата обращения: 11.02.2021).

9. Kaspersky Industrial CyberSecurity [Электронный ресурс] –www.dialognauka.ru URL: https://www.dialognauka.ru/products/KICS/ (дата обращения: 10.11.2020).

References

1. Abdulin A.A., Methods of vulnerability assessment of automated control systems of technological processes / A.A. Abdulin, A.N. Sokolov // Proceedings of the XVII All-Russian scientific-practical conference of students, graduate students and young scientists "Security of Information Space", Chelyabinsk 2018, pp. 4-9.

2. Cybersecurity of APCS. Review of specialized superimposed protection tools [Electronic resource] - https://www.anti-malware.ru/analytics/Market_Analysis/ICS-security-review (date of reference: 03.11.2020).

3. Industrial Strength OT and IoT Security and Visibility [Electronic resource] - https://www.nozominetworks.com/downloads/US/Nozomi-Networks-Guardian-Data-Sheet.pdf (accessed 19.11.2020).

4. Continuous Threat Detection [Electronic resource] - https://cdn2.hubspot.net/hubfs/2553528/CTDdatasheet.pdf (accessed 14.01.2021).

5. Learn why industrial control systems are soft targets for adversaries [Electronic resource] - https://cyberx-labs.com/resources/risk-report-2019/ (accessed 03.02.2021).

6. Industrial Control Threat Intelligence Whitepaper [Electronic resource] - https://www.dragos.com/resource/industrial-control-threat-intelligence-whitepaper/ (accessed 15.12.2020).

7. The Forescout Platform Complete Situational Awareness for the Extended Enterprise [Electronic resource] - https://www.forescout.com/platform/ (accessed 01.12.2020).

8. The Indegy IndustrialCybersecurity Suite [Electronic resource] - https://cdn2.hubspot.net/hubfs/2755567/The%20Indegy%20Industrial%20Cybersecurity%20eBook%202019.pdf (accessed 11.02.2021).

9. Kaspersky Industrial CyberSecurity [Electronic resource] -www.dialognauka.ru URL: https://www.dialognauka.ru/products/KICS/ (access date: 10.11.2020).

АБДУЛИН Артур Ахмадулович, аспирант кафедры защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: arthyrw@gmail.com

СОКОЛОВ Александр Николаевич, кандидат технических наук, доцент, заведующий кафедрой защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: sokolovan@susu.ru

Abdulin Arthur Akhmadulovich, postgraduate student of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: arthyrw@gmail.com

SOKOLOV Alexander Nikolaevich, Ph.D., Associate professor, Head of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: sokolovan@susu.ru

УДК 004.89 Вестник УрФО № 1(39) / 2021, с. 54–61

Асяев Г.Д., Соколов А.Н.

DOI: 10.14529/secur210107

МОДЕЛЬ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ НА ОСНОВЕ МЕТОДА ПРЕДИКТИВНОЙ ЗАЩИТЫ С ИСПОЛЬЗОВАНИЕМ РЕКУРРЕНТНОЙ И ПОЛНОСВЯЗНОЙ НЕЙРОННЫХ СЕТЕЙ [1]

В статье проанализированы основные причины роста количества успешно реализованных кибератак, связанные с особенностями функционирования автоматизированных систем управления технологическими процессами (АСУ ТП). Показано, что традиционные подходы, связанные с разработкой моделей угроз и применением стандартных сертифицированных решений для обеспечения информационной безопасности АСУ ТП не всегда эффективны. На основе нового критерия защищенности автоматизированной системы и метода предиктивной защиты предложена модель на основе двух искусственных нейронных сетей, позволяющая по косвенным признакам (параметрам) системы определить возможность наступления кибератаки и спрогнозировать время, через которое она наступит, а также выбрать соответствующие меры защиты. В результате работы модели формируется перечень действий при обнаружении новых видов угроз, связанных с деструктивными воздействиями на объект, исходя из приемлемости прогнозируемых последствий работы АСУ ТП.

Ключевые слова: *автоматизированная система управления технологическим процессом (АСУ ТП), деструктивное воздействие, инцидент информационной безо-*

[1] Исследование выполнено при финансовой поддержке гранта РФФИ и Челябинской области в рамках научного проекта № 20-47-740006

пасности, искусственная нейронная сеть (ИНС), кибератака, конкатенация функций, критическая информационная инфраструктура, предиктивная защита.

Asyaev G.D., Sokolov A.N.

A MODEL FOR ENSURING INFORMATION SECURITY OF AN AUTOMATED PROCESS CONTROL SYSTEM BASED ON THE PREDICTIVE PROTECTION METHOD USING RECURRENT AND FULLY CONNECTED NEURAL NETWORKS

The article analyzes the main reasons for the growth in the number of successfully implemented cyberattacks related to the functions of functioning of automated process control systems (APCS). It is shown that the traditional approaches associated with the development of threat models and standard certified solutions for information security of ICS are not always effective. On the basis of a new criterion for the security of an automated system and a method of predictive protection, a model based on two artificial networks has been proposed, which makes it possible, by indirect signs (parameters), to determine the possibility of a cyber attack and predict the time after which it will come, as well as to select appropriate protection measures. As a result of the operation of the model, a list of actions is formed upon detection of new types of threats associated with destructive effects on the object, based on the acceptability of the predicted consequences of the operation of the APCS.

Keywords: *automated process control system (APCS), destructive impact, information security incident, artificial neural network (ANN), cyberattack, function concatenation, critical information infrastructure, predictive protection.*

1. Введение

Развитие информационных технологий сопровождается постоянным пополнением арсенала средств, используемых злоумышленниками для реализации кибератак, в том числе на объекты критической информационной инфраструктуры. При этом, несмотря на то, что на большинстве объектов используются средства защиты, количество успешно проведенных кибератак возрастает [1]. Вероятной причиной этого роста является несовершенство применяемых моделей информационной безопасности на основе традиционных подходов, связанных с разработкой моделей угроз и применением стандартных сертифицированных решений по защите информации.

Одним из подходов, связанных с обеспечением защиты информации в автоматизированной системе управления технологиче-

ским процессом (АСУ ТП), является подход, основанный на постоянном мониторинге трафика всех действий системы. Анализ трафика позволяет вовремя выявить аномальное поведение системы и сформировать меры по нейтрализации деструктивных воздействий. К аномальным относятся редкие данные, события или наблюдения, которые вызывают подозрения ввиду существенного отличия от большей части данных. Аномальным поведением называют нестандартное поведение системы, отличное от нормального, влекущее за собой отклонение от технологического процесса [2].

Важными особенностями функционирования АСУ ТП являются [3]:

• различная степень критичности выхода из строя отдельных элементов АСУ ТП в зависимости от технологического процесса;

• промышленные информационные системы могут работать годами, их остановка недопустима или невозможна. Это затрудняет установку обновлений для программного обеспечения для устранения уязвимостей, а также другое регулярное вмешательство в сам процесс работы [4];

• многие АСУ ТП используют закрытые проприетарные протоколы. Их производители, как правило, не реализуют адекватные политики поиска и исправления уязвимостей [4].

Перечисленные особенности приводят к выводу о необходимости постоянного аудита и оценки рисков для предотвращения инцидентов информационной безопасности АСУ ТП [5].

В [3] был сформулирован новый критерий защищенности автоматизированной системы (АС), используемой в замкнутом контуре управления объектом (функциональной подсистемой): система является защищённой, если под воздействием факторов, влияющих на информацию, передаточная функция АС меняется таким образом, что качество управления объектом управления остаётся в заданных пределах. При этом под передаточной функцией подразумевается зависимость сигнала, подаваемого вход объекта управления, от структуры управляющего информационного трафика, поступающего на вход АС. Деструктивное воздействие кибератаки приводит к изменению управляющего трафика и самой управляющей функции, в результате чего на объект поступает искажённый сигнал управления. Последствия деструктивного воздействия можно считать приемлемыми, если качество управления объектом управления при этом остаётся в заданных пределах.

На основании критерия защищенности АС в [1] сформулировано понятие предиктивной защиты как деятельности, позволяющей по косвенным признакам (параметрам) системы определить возможность наступления кибератаки и спрогнозировать время, через которое она наступит, а также выбрать соответствующие меры защиты.

С точки зрения предиктивной защиты весь процесс обеспечения безопасности можно представить в виде модели из трех блоков, связанных между собой, для каждого из которых характерны свои специфичные угрозы (рис. 1).

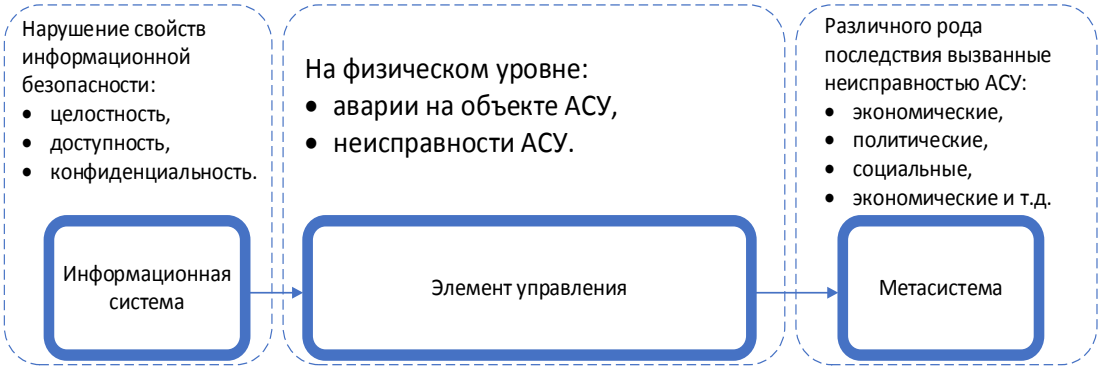


Рис. 1. Угрозы информационной безопасности на различных уровнях управления автоматизированной системы

Стоит также заметить, что модель, представленная на рис. 1, носит последовательный характер: нарушение свойств информации на уровне информационной системы АСУ приводит к определенным последствиям на уровне объекта управления и метасистемы. Для информационной системы АСУ ТП наиболее важными свойствами с точки зрения обеспечения безопасности информации

являются её целостность и доступность. Обеспечение конфиденциальности технологической информации при этом не является первоочередной задачей [1]. При выявлении нарушений каких-либо свойств безопасности на уровне управляющего устройства наступает нарушение работы на физическом уровне (сбои, аварии, отказ в обслуживании и т.д.). После этого рассчитываются последствия для системы при нарушении работы соответствующего управляющего блока.

Информационные потоки подразделяются на:

• поток данных, генерируемый функцией или элементом управления;

• поток данных, формируемый командами используемого программного обеспечения;

• набор данных, хранящихся непосредственно на элементе управления.

Потоки информации предназначены для обмена между различными элементами управления технологическим процессом или для реализации элементами контроля их внутренних функций. Элемент управления представляет собой промышленный контроллер или автономное устройство, принимающее сигналы от контролируемых функций. При этом верхний уровень управляется с помощью программного обеспечения, которое обеспечивает координацию всего технологического процесса, в то время как функции автоматизации нижнего уровня управляются посредством программного обеспечения исполнительных устройств и средств, которые управляют ими. Современные средства защиты информации представляют собой систему фильтрации трафика в соответствии с созданными черными и белыми списками, которые запрещают или разрешают выполнять соответствующие команды, пропускать трафик [6]. Стоит отметить, что списки разграничения доступа формируются из некой эвристической модели, составляемой администратором безопасности. Именно к новым типам кибератак (которые еще неизвестны или не были проведены) большинство современных средств защиты информации, как правило, неустойчивы.

Относительно недавно стали применяться интеллектуальные системы управления, основанные на использовании искусственных нейронных сетей (ИНС) [7]. Подобные системы могут обучаться на определенной выборке известных событий информационной безопасности и распознавать менее известные или абсолютно новые кибератаки [1]. Основной сложностью при создании таких систем является формирование обучающей выборки исходных данных требуемого объёма. В условиях постоянного изменения модели угроз информационной безопасности и вариативности характеристик объектов управления сформировать такую выборку за достаточно короткое время далеко не всегда возможно. Даже не смотря на то, что системы на основе ИНС позволяют классифицировать кибератаки на ранних стадиях, этого не всегда бывает достаточно.

2. Модель «раннего» обнаружения инцидентов информационной безопасности на основе метода предиктивной защиты. Постановка задачи и ее решение с использованием искусственных нейронных сетей

Целью представленного исследования является построение модели обеспечения информационной безопасности АСУ ТП на основе метода предиктивной защиты, отличительной особенностью которой является способность «раннего» обнаружения инцидентов информационной безопасности, то есть прогнозировать инциденты, влекущие негативные последствия, до их появления. Поскольку в этой постановке задачи модель должна прогнозировать время, через которое возможно наступление кибератаки (в том числе ее временные и числовые характеристики) и формировать соответствующую стратегию защиты, для обучения использована нейронную сеть «с подкреплением» (с созданием «агента») [8]. В качестве такой сети выбрана рекуррентная нейронная сеть с сетью смеси распределений на выходе (Recurrent Neural Network with Mixture Density Network output, MDN-RNN). Такая сеть обладает особенностью – «мышлением наперед», важной с точки зрения поставленной задачи (рис. 2). Для рекуррентной нейронной сети долгосрочной памяти (LSTM) достаточно 256 слоев, чтобы выявить общие паттерны для прогнозирования и в то же время не переобучиться под конкретную выборку. Recurrent Neural Network фиксирует внутреннее текущее состояние безопасности управляющего объекта в своем окружении с целью предсказывать последующее состояние на основе предыдущего и совершённого действия.

Следующим шагом в рассматриваемой архитектуре представленной модели является выбор стратегии защиты. Этот механизм

реализован с помощью контроллера на основе полносвязной нейронной сети (рис. 3): на вход подается текущее состояние *z* и скрытое состояние *h* (для предсказания следующего значения), где *z* и *h* представляют собой числовые векторы [9]. На выходе контроллера формируется сигнал a, определяющий некую меру защиты как конкатенацию функций *z* и *h*.

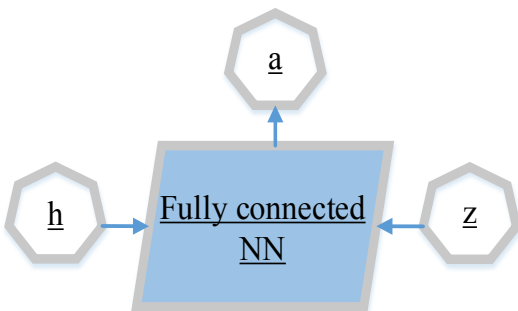


Рис. 3. Модель контроллера на основе полносвязной нейронной сети

На рис. 4 представлена общая модель обеспечения информационной безопасности АСУ ТП на основе метода предиктивной защиты. Система по косвенным признакам определяет состояние АСУ ТП (аномальное поведение системы), прогнозирует время, при наступлении которого возможны негативные последствия. Далее выполняется расчет уровня прогнозируемых последствий, на основе которого контроллер выбирает оптимальный вариант защиты из некоторого множества [7].

Модель реализована в облачной среде разработке Google Collab. На рис. 5 показан фрагмент потока данных процесса вычисления последствий (damage) для каждой итерации (iteration), основной задачей при этом является минимизация значения уровня последствий. Общий уровень последствий для каждой эпохи определялся как арифметическое среднее значений последствий на 7 итерациях.

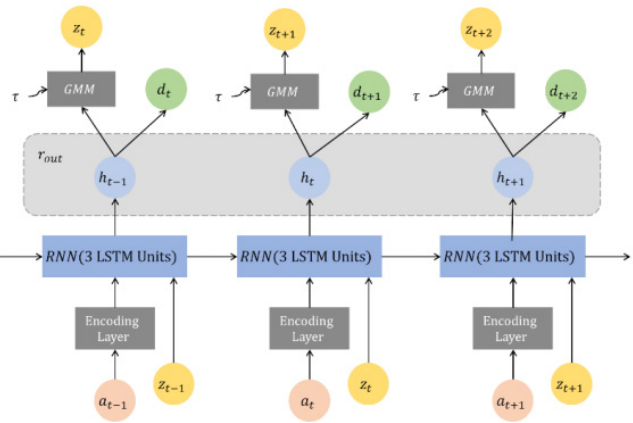


Рис. 2. Структура бокса LSTM RNN-MDN

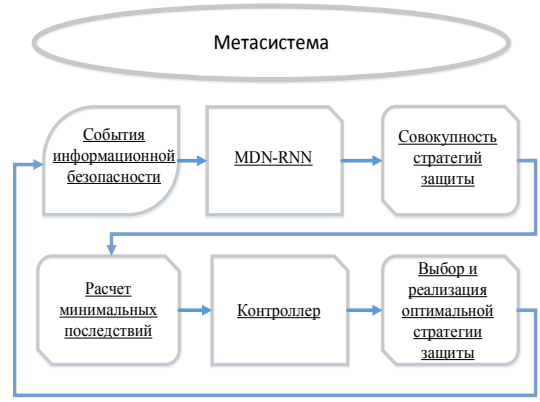


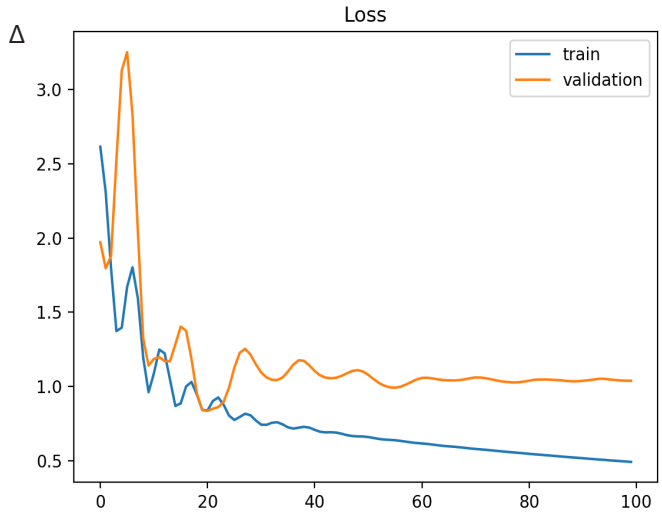
Рис. 4. Общая модель обеспечения информационной безопасности АСУ ТП на основе метода предиктивной защиты

3. Результаты экспериментов

На рис. 6 представлен график зависимости значения уровня последствий от количества итераций. Чем выше это значение, тем более значительными являются негативные последствия для метасистемы. Из рисунка видно, что при увеличении количества итераций уровень последствий уменьшается. Синей (темной) линией (train) показано изменение уровня последствий на обучающей выборке, а оранжевой (светлой) линией (validation) – на валидационной выборке, т.е. на новых данных, которые модель еще не обрабатывала.

```
Iteration #50 damage: 0.8528947830200195
Iteration #100 damage: 0.8866778016090393
Iteration #150 damage: 0.8778553009033203
Iteration #200 damage: 0.6406872272491455
Iteration #250 damage: 0.673102080821991
Iteration #300 damage: 0.6530210971832275
Epoch #0 damage: 0.7833202557753672
Iteration #350 damage: 0.6791139841079712
Iteration #400 damage: 0.7526218891143799
Iteration #450 damage: 0.8202939629554749
Iteration #500 damage: 0.5508345365524292
Iteration #550 damage: 0.6866168975830078
Iteration #600 damage: 0.5532808899879456
Iteration #650 damage: 0.784627377986908
Epoch #1 damage: 0.7561166847349972
Iteration #700 damage: 0.7903854846954346
Iteration #750 damage: 0.7944695949554443
Iteration #800 damage: 0.8289942741394043
Iteration #850 damage: 0.5659400224685669
```

Рис. 5. Фрагмент потока данных процесса расчета уровня последствий



N – номер итерации;
Δ - значение уровня последствий

Рис. 6. Значение уровня последствий в зависимости от количества итераций на обучающей (train) и тестовой (validation) выборке

4. Заключение

Таким образом, в статье представлена общая модель обеспечения информационной безопасности АСУ ТП на основе метода предиктивной защиты, которая использует две ИНС:

• рекуррентную нейронную сеть с сетью смеси распределений на выходе (MDN-RNN), которая оценивает временные и числовые характеристики прогнозируемого инцидента информационной безопасности;

• полносвязную нейронную сеть, которая реализует контроллер, позволяющий осуществлять выбор стратегии обеспечения информационной безопасности из числа возможных.

В результате работы модели формируется перечень действий при обнаружении новых видов угроз, связанных с деструктивными воздействиями на объект, исходя из приемлемости прогнозируемых последствий работы АСУ ТП.

Литература

1. Гарбук С.В., Правиков Д.И., Полянский А.В., Самарин И.В. Обеспечение информационной безопасности АСУ ТП с использованием метода предиктивной защиты // Вопросы кибербезопасности, 2019. №3(31). С. 30-36.

2. Боровков А.И. «Умные» цифровые двойники – основа новой парадигмы цифрового проектирования и моделирования глобально конкурентоспособной продукции нового поколения. Трамплин к успеху// Журнал АО «ОДК». 2018. № 13. С. 12-18.

3. Правиков Д.И. Об одном подходе к обеспечению информационной безопасности автоматизированных систем // Вопросы защиты информации. 2007. № 3. С. 17-19.

4. Гарбук С.В., Бурцев А.Г. Методические основы исследования уязвимостей компонентов АСУ ТП // Защита информации. Inside. 2012. № 3. С. 34-38.

5. Гарбук С.В. Перспективы применения интеллектуальных технологий для решения задач безопасности // Национальная безопасность / 2016. № 4. С. 451-457.

6. Башлыков А.А., Еремеев А.П. Методы и программные средства конструирования интеллектуальных систем поддержки принятия решений для объектов энергетики // Вестник МЭИ. 2018. № 1. С. 72—85.

7. Гарбук С.В. Интеллектуальные автоматизированные средства тематической обработки информации в системах безопасности // Искусственный интеллект и принятие решений. 2017. № 1. С. 95-104.

8. Гарбук С.В., Бакеев Р.Н. Конкурентная оценка качества технологий интеллектуальной обработки данных // Проблемы управления. 2017, № 6. С. 50-62.

9. Гарбук С.В., Правиков Д.И., Полянский А.В., Самарин И.В. Обеспечение информационной безопасности АСУ ТП с использованием метода предиктивной защиты // Вопросы кибербезопасности 2019 №3 (31). С. 30-36.

References

1. Garbuk S.V., Pravikov D.I., Polyanskiy A.V., Samarin I.V. Obespechenie informatsionnoy bezopasnosti ASU TP s ispol'zovaniem metoda prediktivnoy zashchity // Voprosy kiberbezopasnosti, 2019. No. 3(31). pp. 30-36.

2. Borovkov A.I. «Umnye» tsifrovye dvoĭniki – osnova novoĭ paradigmy tsifrovogo proektirovaniya i modelirovaniya global'no konkurentosposobnoĭ produktsii novogo pokoleniya. Tramplin k uspekhu// Zhurnal AO «ODK». 2018. No. 13. pp. 12-18.

3. Pravikov D.I. Ob odnom podkhode k obespecheniyu informatsionnoĭ bezopasnosti avtomatizirovannykh sistem // Voprosy zashchity informatsii. 2007. No. 3. pp. 17-19.

4. Garbuk S.V., Burtsev A.G. Metodicheskie osnovy issledovaniya uyazvimosteĭ komponentov ASU TP // Zashchita informatsii. Inside. 2012. No. 3. pp. 34-38.

5. Garbuk S.V. Perspektivy primeneniya intellektual'nykh tekhnologiĭ dlya resheniya zadach bezopasnosti // Natsional'naya bezopasnost' / 2016. No. 4. pp. 451-457.

6. Bashlykov A.A., Eremeev A.P. Metody i programmnye sredstva konstruirovaniya intellektual'nykh sistem podderzhki prinyatiya reshenĭ dlya ob"ektov energetiki // Vestnik MEI. 2018. No. 1. pp. 72—85.

7. Garbuk S.V. Intellektual'nye avtomatizirovannye sredstva tematicheskoĭ obrabotki informatsii v sistemakh bezopasnosti // Iskusstvennyĭ intellekt i prinyatie reshenĭ. 2017. No. 1. pp. 95-104.

8. Garbuk S.V., Bakeev R.N. Konkurentnaya otsenka kachestva tekhnologiĭ intellektual'noĭ obrabotki dannykh // Problemy upravleniya. 2017, No. 6. pp. 50-62.

9. Garbuk S.V., Pravikov D.I., Polyanskiy A.V., Samarin I.V. Obespechenie informatsionnoy bezopasnosti ASU TP s ispol'zovaniem metoda prediktivnoy zashchity // Voprosy kiberbezopasnosti 2019 No. 3 (31). pp. 30-36.

АСЯЕВ Григорий Дмитриевич, аспирант кафедры защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: asiaevgd@susu.ru

СОКОЛОВ Александр Николаевич, кандидат технических наук, доцент, заведующий кафедрой защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: sokolovan@susu.ru

ASYAEV Grigorii Dmitrievich, postgraduate student of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: asiaevgd@susu.ru

SOKOLOV Alexander Nikolaevich, Ph.D., Associate professor, Head of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: sokolovan@susu.ru

Материалы к публикации отправлять по адресу E-mail: urvest@mail.ru
в редакцию журнала «Вестник УрФО. Безопасность в информационной сфере».

Или по почте по адресу: Россия, 454080, г. Челябинск, пр. им. Ленина, д. 76,
ЮУрГУ, Издательский центр.

ВЕСТНИК УрФО
Безопасность в информационной сфере № 1(39) / 2021
Подписано в печать 31.03.2021.
Дата выхода в свет 05.04.2021. Формат 70×108 1/16. Печать цифровая.
Усл.-печ. л. 6,3. Тираж 100 экз. Заказ 453/3.
Цена свободная.

Отпечатано в типографии Издательского центра ЮУрГУ.
454080, г. Челябинск, пр. им. В. И. Ленина, 76.

Bulletin of the Ural Federal District
Security in the Sphere of Information No. 1(39) / 2021
Signed to print March 31, 2021.
Date of publication of the 05.04.2021. Format 70×108 1/16. Screen printing.
Conventional printed sheet 6,3. Circulation – 100 issues. Order 453/3. Open price.

Printed in the printing house of the Publishing Center of SUSU.
76, Lenina Str., Chelyabinsk, 454080