ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ

№5 2024 (63)

Спецвыпуск, посвящённый 70-летию Института интеллектуальных кибернетических систем Национального исследовательского ядерного университета «МИФИ»

DOI: 10.21681/2311-3456

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЯДЕРНЫЙ УНИВЕРСИТЕТ «МИФИ»

70 лет

ИНСТИТУТУ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ

НАУЧНЫЙ РЕЦЕНЗИРУЕМЫЙ ЖУРНАЛ

№5 (63) 2024 г.

Выходит 6 раз в год

Журнал выходит с 2013 г. (Свидетельство о регистрации ПИ № ФС77-75239). Перерегистрировано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций 07.03.2019.

Журнал входит в рейтинг научных изданий ВАК в категории К1, индексируется в RSCI, публикует статьи по специальностям 1.2.4 и 2.3.6 – физ-мат. науки; 2.2.15, 2.3.1, 2.3.5, 2.3.6 – техн.науки

Учредитель и издатель

АО «Научно-производственное объединение «Эшелон»

Над номером работали:

Г. И. Макаренко – *шеф-редактор*, И. Ю. Шахалов – *отв. секретарь*, С. С. Игнатов – *верстка*, Н. С. Рождественская – *маркетинг и подписка*

Подписано к печати 18.10.2024 г.
Общий тираж 120 экз. Цена свободная

Адрес: 107023, Москва, ул. Электрозаводская, д. 24, стр. 1.
E-mail: editor@cyberrus.info, тел.: +7 (985) 939-75-01.
Требования, предъявляемые к рукописям, размещены на сайте: **https://cyberrus.info/**

СОДЕРЖАНИЕ

Подписка на журнал осуществляется в почтовых отделениях по каталогу «Пресса России». Подписной индекс 40707

70 ЛЕТ НА СТРАЖЕ КИБЕРНЕТИКИ И КИБЕРБЕЗОПАСНОСТИ

Уважаемые преподаватели, сотрудники, аспиранты, студенты и выпускники Института интеллектуальных кибернетических систем! Дорогие друзья!

Примите самые искренние и сердечные поздравления со знаменательной датой – семидесятилетием Вашего факультета-института!

В этот праздничный день всех нас объединяет чувство гордости за славную историю ИИКС и его предшественников – факультетов КиБ, К, Б, В, ЭВУСА, ВМУ, их достижения и значимый вклад в развитие отечественной науки в сфере информационных технологий и информационной безопасности.

История ядерного университета неразрывно связана с историей нашей страны. Московский механический институт боеприпасов (первое название МИФИ), созданный в разгар Великой Отечественной войны с целью подготовки научных и инженерных кадров для оборонной промышленности, в 1945 году был перепрофилирован на работу по «Атомному проекту». Как особое учебное заведение для профессиональной подготовки специалистов-атомщиков для работ над техническими проблемами «Атомного проекта», университет прошел огромный новаторский путь и превратился в один из крупнейших вузов, авторитетный образовательный и научно-исследовательский центр с разветвленной структурой филиалов. Все исторические этапы развития университета отмечены блестящим профессорско-преподавательским составом: здесь читали лекции известные учёные, Нобелевские лауреаты, организовавшие свои научные школы и воспитавшие не одно поколение учеников.

Участие в «Атомном проекте» потребовало от вуза соответствующего программного и математического обеспечения, что привело к необходимости создания профильной кафедры. Сегодня трудно поверить, что всего 70 лет тому назад кафедра «Математические счетно-решающие приборы и устройства» (№12) стала тем маленьким зёрнышком, которое проросло, и на базе которого в 1954 г. образовался факультет «Вычислительные математические устройства» (ВМУ). В последующие годы несколько раз менялось название факультета, менялся состав кафедр, менялись направления подготовки. А в 2011 г. произошло знаковое событие – в целях координации действий университета по реализации стратегических направлений обеспечения национальной безопасности,

факультеты «Кибернетика» и «Информационная безопасность» были объединены в рамках одного факультета вместе с Институтом финансовой и экономической безопасности.

Сейчас Институт интеллектуальных кибернетических систем является одним из ведущих учебно-научных центров высшей школы по подготовке специалистов в области защищенных компьютерных технологий, криптографии, интеллектуального анализа, параллельной и распределенной обработки данных, математического моделирования, цифровой аппаратуры, робототехники, машинного обучения. За последние годы были существенно модернизированы существующие учебные программы, начата реализация новых «прорывных» программ, пользующихся повышенным интересом у абитуриентов, значительно омолодился педагогический состав института, чаще стали приглашать для проведения занятий специалистов из IT-компаний. Наши же выпускники идут работать в IT-компании со своими стартапами и идеями, получается взаимно эффективное взаимодействие.

И для меня, как выпускника нашего ядерного университета, нет большей радости, чем видеть, как меняется наша альма-матер. Я убежден, что благодаря слаженной командной работе, профессионализму и ответственности всех сотрудников ИИКС, удастся вписать новые славные страницы в историю нашего вуза, – историю интеллектуальных побед, амбициозных научных проектов и знаковых открытий.

Доброе имя и слава ИИКС НИЯУ МИФИ – в достижениях и практических делах его сотрудников и выпускников!

Желаю всем счастья, удачи, благополучия и новых свершений! Пусть этот юбилейный год всем нам запомнится яркими интересными событиями и высокими достижениями.

Ректор НИЯУ МИФИ,
д.ф.-м.н., профессор ***Шевченко Владимир Игоревич***

DOI: 10.21681/2311-3456-2024-5-2-3

НОРМАЛИЗАЦИЯ ТРАФИКА ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО СКРЫТЫМ КАНАЛАМ

Епишкина А. В.[1], Когос К. Г.[2]

DOI: 10.21681/2311-3456-2024-5-4-17

Возможность построения скрытых каналов в информационной системе влечет за собой потенциальную утечку защищаемой информации. Существует множество методов противодействия скрытым каналам, однако не все они применимы на практике. Целью исследования является разработка методов противодействия утечке информации по скрытым каналам по памяти и по времени путем нормализации трафика.

В работе исследованы скрытые каналы по памяти и по времени, предложены алгоритмы полной и частичной нормализации трафика для противодействия указанных скрытым каналам. С использованием методов теории информации, теории вероятности, дифференциального и интегрального исчисления и данных о распределении длин межпакетных интервалов пакетов сетевого трафика выведены формулы для оценки эффективной пропускной способности канала связи в условиях противодействия скрытым каналам и остаточной пропускной способности скрытого канала.

При полной нормализации трафика по памяти скрытый канал по памяти, основанный на изменении длин передаваемых пакетов, полностью уничтожается в связи с тем, что все пакеты становятся одинаковой длины. При частичной нормализации трафика скрытый канал по памяти, основанный на изменении длин передаваемых пакетов, уничтожается не полностью, следовательно, остается бинарный скрытый канал по памяти, оценки пропускной способности которого показывают нецелесообразность применения частичной нормализации скрытого канала по времени и указывают на необходимость его полной нормализации.

В случае, если была проведена полная нормализация длин пакетов, а остаточная пропускная способность скрытого канала все еще велика, можно дополнительно нормализовать трафик по времени. В работе предложен способ противодействия, при котором скрытый канал по времени полностью уничтожается.

Рассчитаны количественные значения эффективной пропускной способности канала связи и остаточной пропускной способности скрытого канала при использовании протоколов IPv4 и IPv6, которые могут быть полезны при применении методов нормализации трафика на практике.

Ключевые слова: *информационная безопасность, утечка информации, метод противодействия, сетевой скрытый канал, скрытый канал по памяти, скрытый канал по времени, нормализация трафика, частичная нормализация, пропускная способность.*

Введение

В современном мире бесспорно актуальной является задача обеспечения информационной безопасности, от качества решения которой во многом зависит функционирование государственных и коммерческих организаций.

В настоящее время и на прогнозируемую перспективу сохранится тенденция широкого использования сетей пакетной передачи данных. Применение этих технологий привносит, а повсеместное внедрение делает весьма значимой угрозу негласного использования особенностей протокола IP для скрытой передачи информации ограниченного доступа по каналам связи, выходящим за пределы объектов информатизации, на которых она обрабатывается.

Необходимость создания и постоянного совершенствования способов противодействия утечке информации по так называемым скрытым каналам обусловлена и тем, что такие каналы могут быть построены в условиях применения традиционных способов сетевой защиты, заключающихся в межсетевом экранировании, туннелировании трафика и др. Исследования показывают, что данная угроза сохраняется даже при передаче информации в зашифрованном виде, более того, существуют так называемые необнаруживаемые скрытые каналы [1].

Впервые термин «скрытый канал» был введен в 1973 году Лэмпсоном (Lampson), который под скрытым каналом понимал канал связи, который не разрабатывался и не предполагался для передачи информации.

Скрытые каналы по механизму передачи информации подразделяют на:

- скрытые каналы по памяти [2–5];
- скрытые каналы по времени [6–10];
- статистические скрытые каналы [11].

Скрытые каналы по памяти основаны на наличии памяти, в которую передающий субъект записывает

1 Епишкина Анна Васильевна, кандидат технических наук, доцент, доцент кафедры криптологии и кибербезопасности НИЯУ МИФИ; доцент Инженерной академии РУДН, Москва, Россия. E-mail: avepishkina@mephi.ru

2 Когос Константин Григорьевич, кандидат технических наук, доцент, доцент кафедры криптологии и кибербезопасности НИЯУ МИФИ. Москва, Россия. E-mail: kgkogos@mephi.ru

информацию, а принимающий считывает ее. Скрытность каналов по памяти определяется тем, что сторонний наблюдатель не знает того участка памяти, где записана скрываемая информация, а поскольку способ использования памяти зачастую не учитывается разработчиками систем защиты, скрытые каналы указанного типа могут не выявляться используемыми средствами защиты.

Скрытый канал является каналом по памяти при выполнении следующих условий:

- отправитель и получатель должны иметь доступ к элементу общего ресурса;
- отправитель имеет возможность изменить этот элемент разделяемого ресурса;
- получатель должен иметь возможность распознать такое изменение;
- должен существовать механизм синхронизации для отправителя и получателя для упорядочивания отправляемых данных;
- если не выбран специальный метод кодирования во избежание последовательности одинаковых символов, отправитель и получатель должны иметь возможность предварительно договориться о временном интервале, в течение которого получатель будет наблюдать за изменениями в канале.

Скрытые каналы по памяти подразделяют на следующие виды:

- скрытые каналы, основанные на сокрытии информации в структурированных данных (встраивание данных в информационные объекты с формально описанной структурой и формально описанными правилами обработки);
- скрытые каналы, основанные на сокрытии информации в неструктурированных данных (встраивание данных в информационные объекты в информационные объекты без учета формально описанной структуры).

Скрытые каналы по времени предполагают, что передающий информацию субъект моделирует с помощью передаваемой информации некий изменяющийся во времени процесс, а субъект, принимающий информацию, может демодулировать передаваемый сигнал, наблюдая несущий информацию процесс во времени.

Скрытый канал является каналом по времени при выполнении следующих условий:

- отправитель и получатель должны иметь доступ к элементу общего ресурса;
- отправитель и получатель должны иметь возможность синхронизировать свои действия;
- отправитель должен иметь возможность изменять время ответного сигнала получателя для выявления изменения в данном элементе разделяемого ресурса;
- должен быть механизм инициирования процесса передачи данных по скрытому каналу и упорядочивания отправляемых данных.

Скрытые статистические каналы используют для передачи информации изменение параметров распределений вероятностей любых характеристик системы, которые могут рассматриваться как случайные и описываться вероятностно-статистическими моделями. Скрытность таких каналов основана на том, что получатель информации имеет меньшую неопределенность в определении параметров распределений наблюдаемых характеристик системы, чем наблюдатель, не знающий структуру скрытого канала.

Скрытые каналы также можно разделить на каналы с шумом и каналы без шума [12]. Скрытые каналы с шумом — каналы, в которых вероятность верного распознавания переданных символов отлична от единицы. В частности, скрытый канал с шумом — канал, в котором наблюдаются как разрешенные, так и запрещенные политикой безопасности информационные потоки. В скрытом канале без шума общий ресурс используется исключительно скрытыми сторонами. Наличие шума важно учитывать при оценке пропускной способности скрытого канала. В частности, введение шума в скрытые каналы может применяться для ограничения пропускной способности скрытого канала.

По пропускной способности скрытые каналы подразделяют на следующие типы:

- каналы с низкой пропускной способностью (пропускной способности достаточно для передачи ценных информационных объектов минимального объема или команд за промежуток времени, на протяжении которого данная передача является актуальной);
- каналы с высокой пропускной способностью (пропускной способности достаточно для передачи информационных объектов среднего и большого размера за промежуток времени, на протяжении которого данные информационные объекты являются ценными).

Угрозы безопасности, которые могут быть реализованы с помощью скрытых каналов, включают в себя:

- внедрение вредоносных программ и данных;
- передачу злоумышленником команд агентам для выполнения;
- утечку криптографических ключей и паролей;
- утечку отдельных информационных объектов.

Приведем взаимосвязь угроз, реализуемых с помощью скрытых каналов, с типами скрытых каналов в зависимости от их пропускной способности (табл. 1),

Таблица 1.

Взаимосвязь угроз, реализуемых с помощью скрытых каналов, с типами скрытых каналов в зависимости от их пропускной способности

Угроза	Тип скрытых каналов	
	Скрытые каналы с низкой пропускной способностью	Скрытые каналы с высокой пропускной способностью
Внедрение вредоносных программ и данных	+	+
Подача злоумышленником команд агенту для выполнения	+	+
Утечка криптографических ключей или паролей	+	+
Утечка отдельных информационных объектов	–	+

Таблица 2.

Классификация скрытых каналов по механизму организации

Тип канала	Механизм организации канала
Параметрический пространственный	Отправитель изменяет значения наблюдаемых объектов. Получатель извлекает информацию на основании наблюдаемых значений.
Событийный пространственный	Отправитель определяет, какие из наблюдаемых объектов будут изменены. Получатель извлекает информацию путем определения наличия или отсутствия факта модификации.
Параметрический временной	Отправитель знает будущее значение наблюдаемого объекта и может управлять моментами наблюдения данного объекта получателем. С появлением необходимого значения отправитель дает возможность получателю осуществить наблюдение. Получатель извлекает информацию на основании наблюдаемых значений.
Событийный временной	Отправитель может управлять порядком изменения объектов, относительно наблюдений, осуществляемых получателем. Получатель извлекает информацию из порядка следования этих событий.

в таблице знак «+» означает, что угроза может быть реализована при наличии скрытого канала соответствующего типа; знак «–» означает, что наличие скрытого канала данного типа не может привести к реализации угрозы.

По механизму организации скрытые каналы подразделяются на четыре типа (табл.2).

Заметим, что важным является разделение на сетевые и несетевые скрытые каналы в связи с тем, что с развитием высокоскоростных сетевых технологий и возможностью негласного использования особенностей протоколов сетевого и других уровней взаимосвязи открытых систем значительно расширились возможности построения сетевых скрытых каналов и увеличились их пропускная способность. Под сетевым скрытым каналом понимается канал, в котором общий ресурс является компонентом сетевой среды.

В настоящей работе будут рассмотрены сетевые скрытые каналы, как по памяти, так и по времени. Поскольку существуют различные способы противодействия скрытым каналам путем генерации фиктивного трафика [13], увеличения длин пакетов [14], введения дополнительных случайных задержек [15], переупорядочивания пакетов [16], основное внимание будет уделено методами нормализации скрытых каналов.

1. Полная нормализация трафика как метод противодействия скрытым каналам по памяти

Пусть длины пакетов принимают значения на множестве $N_{l_{фикс}+n-1} \setminus N_{l_{фикс}-1}$, $l_{фикс}$, $n \in N$, где N_x — множество натуральных чисел, не превосходящих x. Предложен следующий способ выравнивания длин передаваемых пакетов: каждый пакет дополняется фиктивными битами до длины $l_{вып}$, если исходная длина пакета, который отправитель должен послать для передачи символа «i» не превосходит $l_{вып}$:

$$l(i) \le l_{вып}. \qquad (1)$$

В противном случае пакет дополняется фиктивными битами и разбивается на минимально возможное число пакетов длины $l_{вып}$. Здесь $l_{вып}$ — параметр метода противодействия (рис. 1).

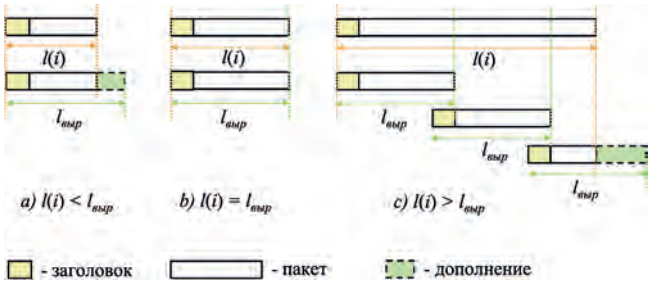


Рис. 1. Выравнивание длин передаваемых пакетов до $l_{выр}$

Рассмотрим подробнее алгоритм полной нормализации трафика. Пусть имеется исходный пакет длины $l(i) = l_{фикс} + i - 1$. Тогда:

- если $l(i) \le l_{выр}$, пакет дополняется фиктивными битами до длины $l_{выр}$;
- если $l(i) > l_{выр}$, находится минимальное число пакетов k, на которое следует разбить рассматриваемый пакет.

Выбор значения $l_{выр}$ продиктован минимизацией дополнительной нагрузки на канал связи и ограничением на максимально допустимую долю дополнительных пакетов α, где α задается владельцем канала связи.

Представим

$$l_{выр} = l_{фикс} + H, \tag{2}$$

где $l_{фикс}$ — минимально возможная длина пакета, являющаяся параметром канала связи, $H \in N_{n-1}$. Таким образом, имея распределение длин пакетов в канале связи и максимально допустимую долю дополнительных пакетов α, можно найти оптимальное значение параметра H.

Найдем дополнительную нагрузку на канал связи, заключающуюся в отправке пакетов большей длины:

$$\sum_{i=1}^{n}\left(l_{новая} - l(i)\right)p(i) = \sum_{i=1}^{n} l_{новая}\,p(i) - E(L), \tag{3}$$

где $l_{новая}$ — новая длина пакета, $p(i)$ — вероятность передачи символа «i», $E(L)$ — средняя длина пакета в трафике.

Поскольку величина $E(L)$ — константа, будем минимизировать среднюю длину новых пакетов:

$$\sum_{i=1}^{n} l_{новая}\,p(i) = \sum_{i=1}^{H+1} l_{выр}\,p(i) + \\ + \sum_{i=H+2}^{2H+1} l_{выр}\,p(i) + \ldots + \sum_{i=(k-1)H+2}^{n} kl_{выр}\,p(i). \tag{4}$$

Отсюда получаем:

$$\sum_{i=1}^{n} l_{новая}\,p(i) = (l_{вых} + H) \\ \left(\sum_{i=1}^{H+1} p(i) + \sum_{i=H+2}^{2H+1} 2p(i) + \ldots + \sum_{i=(k-1)H+2}^{n} kp(i)\right). \tag{5}$$

Выразим ограничение, что доля дополнительных пакетов при введении противодействия не должна превышать α:

$$\frac{\sum_{i=1}^{H+1} p(i) + \sum_{i=H+2}^{2H+1} 2p(i) + \ldots + \sum_{i=(k-1)H+2}^{n} kp(i)}{\sum_{i=1}^{n} p(i)} \le \alpha. \tag{6}$$

Отсюда получаем условие:

$$\sum_{i=1}^{H+1} p(i) + \sum_{i=H+2}^{2H+1} 2p(i) + \ldots + \sum_{i=(k-1)H+2}^{n} kp(i) \le \alpha. \tag{7}$$

Таким образом, решаемая задача минимизации ставится следующим образом:

$$\begin{cases} (l_{вых}+H)\left(\sum_{i=1}^{H+1} p(i)+\sum_{i=H+2}^{2H+1} 2p(i)+\ldots+\sum_{i=(k-1)H+2}^{n} kp(i)\right) \to \min\limits_{H}; \\ \sum_{i=1}^{H+1} p(i) + \sum_{i=H+2}^{2H+1} 2p(i) + \ldots + \sum_{i=(k-1)H+2}^{n} kp(i) \le \alpha. \end{cases} \tag{8}$$

Наглядно представим алгоритм нахождения оптимального значения $l_{выр}$ (рис. 2), где наилучшая длина пакета равна $l_{выр} = \min\_H + l_{фикс}$ байт, $\min\_nums$ – доля дополнительных пакетов.

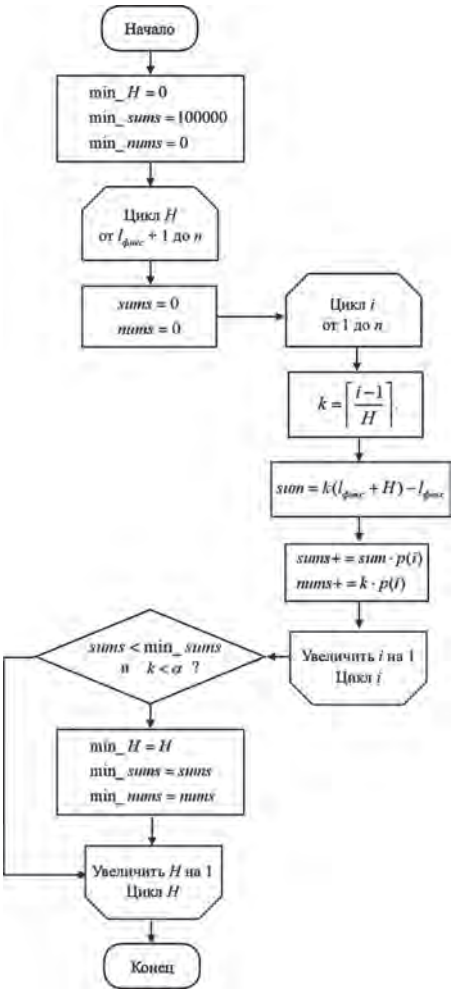


Рис. 2. Блок-схема алгоритма нахождения оптимального значения $l_{выр}$

С другой стороны, эффективная пропускная способность канала связи при введении данного метода противодействия равна

$$\frac{\beta E(L)}{(l_{вых}+H)\left(\sum_{i=1}^{H+1} p(i)+\sum_{i=H+2}^{2H+1} 2p(i)+...+\sum_{i=(k-1)H+2}^{n} kp(i)\right)}, \quad (9)$$

где β — пропускная способность канала связи.

2. Частичная нормализация трафика как метод противодействия скрытым каналам по памяти

Поскольку при полной нормализации трафика по памяти эффективная пропускная способность канала связи значительно снижается, рассмотрим частичную нормализацию трафика. При таком подходе каждый пакет дополняется фиктивными битами либо до длины $l_{вып\_1}$, либо до длины $l_{вып\_2}$, где $l_{вып\_1} = l_{фикс} + H_1$, $l_{вып\_2} = l_{фикс} + H_2$, $H_1, H_2 \in N_{n-1}$. Здесь $l_{вып\_1}$ и $l_{вып\_2}$ — параметры метода противодействия. Если длина пакета превышает $l_{вып\_2}$, то пакет дополняется фиктивными битами и разбивается на несколько пакетов с длинами $l_{вып\_1}$ и $l_{вып\_2}$.

Рассмотрим подробнее алгоритм частичной нормализации трафика (рис. 3).

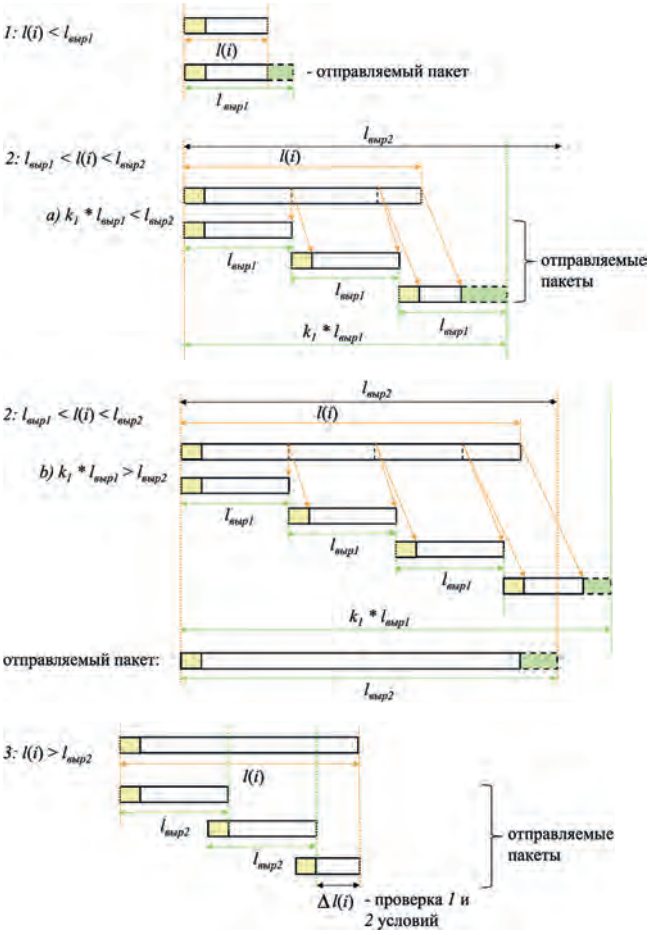


Рис. 3. Частичная нормализация трафика

Пусть имеется исходный пакет длины $l(i) = l_{фикс} + i - 1$. Тогда:

- если $l(i) \le l_{вып\_1}$, то пакет дополняется фиктивными битами до длины $l_{вып\_1}$;
- если $l_{вып\_1} < l(i) \le l_{вып\_2}$, вычисляем количество пакетов длины $l_{вып\_1}$, необходимых для отправки пакета:

$$k_1 = \left[\frac{i-1}{H_1}\right]; \quad (10)$$

- если $l_{вып\_2} \le k_1\ l_{вып\_1}$, то отправляется один пакет длины $l_{вып\_2}$;
- иначе отправляется k_1 пакетов длины $l_{вып\_1}$;
- если $l(i) > l_{вып\_2}$, то отправляется

$$k_2 = \left[\frac{i-1}{H_2}\right], \quad (11)$$

и остается нераспределенная часть пакета длиной не более $l_{вып\_2}$, поэтому повтор первых двух шагов алгоритма позволит найти искомое разбиение пакета.

Выбор параметров противодействия $l_{вып\_1}$ и $l_{вып\_2}$ производится на основе минимизации дополнительной нагрузки на канал связи и ограничением на максимально допустимую долю дополнительных пакетов α, где α задается владельцем канала связи.

Аналогично случаю полной нормализации по памяти вместо дополнительной нагрузки на канал связи найдем среднюю длину новых пакетов:

$$\sum_{i=1}^{n} l_{новая}\, p(i) = \sum_{i=1}^{n} \left\{ \left[\frac{i-1}{H_2}\right] l_{вых\_2} + \right.$$

$$\left. + \min \left\{ \frac{i-1-\left[\frac{i-1}{H_2}\right] l_{вых\_2}}{H_1}\ l_{вых\_1},\ l_{вых\_2} \right\} \right\} p(i). \quad (12)$$

Выразим ограничение, что доля дополнительных пакетов при введении противодействия не должна превышать α:

$$\sum_{i=1}^{n} \left\{ \left[\frac{i-1}{H_2}\right] \frac{i-1-\left[\frac{i-1}{H_2}\right] l_{вых\_2}}{H_1} \ если \right.$$

$$\left. \frac{i-1-\left[\frac{i-1}{H_2}\right] l_{вых\_2}}{H_1}\ l_{вых\_1} < l_{вых\_2}\ иначе\ 1 \right\} p(i) \le \alpha. \quad (13)$$

Наглядно представим алгоритм нахождения оптимальных значений

$$l_{вып\_1} = min\_H_1 + l_{фикс},\ l_{вып\_2}) = min\_H_2 + l_{фикс} \quad (14)$$

и доли дополнительных пакетов $\min\_nums$ (рис. 4).

Эффективная пропускная способность канала связи при введении данного метода противодействия равна

$$\frac{\beta E(L)}{\sum_{i=1}^{n}\left\{\left[\frac{i-1}{H_2}\right] l_{вых\_2}+\min\left\{\frac{i-1-\left[\frac{i-1}{H_2}\right] l_{вых\_2}}{H_1} l_{вых\_1},\ l_{вых\_2}\right\}\right\} p(i)} \quad (14)$$

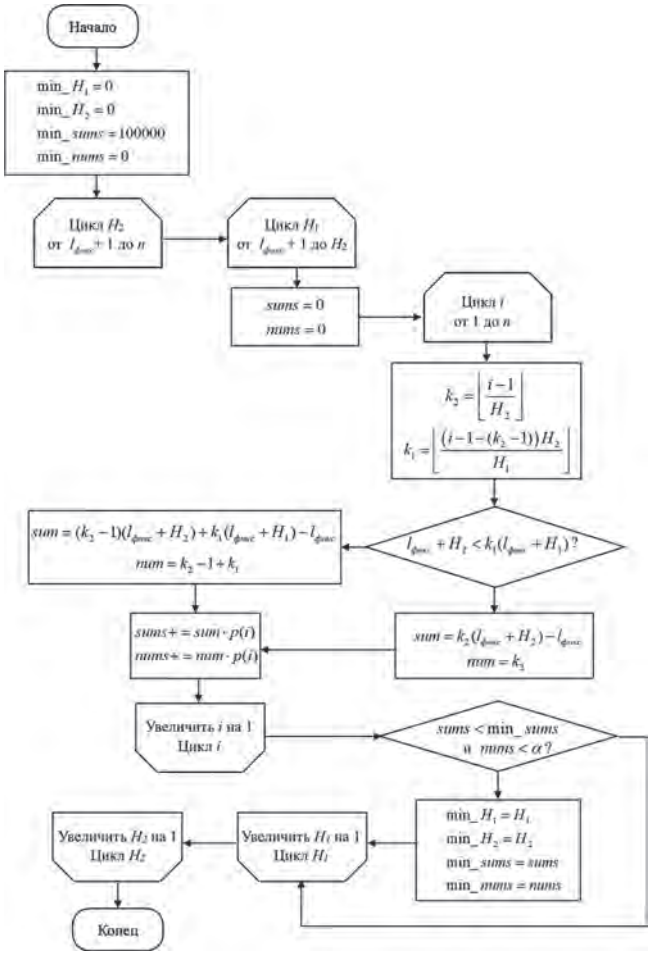


Рис. 4. Блок-схема алгоритма нахождения оптимальных значений $l_{выр\_1}$, $l_{выр\_2}$

3. Оценка остаточной пропускной способности скрытого канала по памяти при полной нормализации трафика

Для экспериментов использовались существующие данные о распределении длин пакетов протоколов IPv4 и IPv6 в трафике[3]. Были определены оптимальные значения параметра противодействия H для протоколов IPv4 и IPv6, параметр α был взят равным 2, то есть в среднем исходный пакет не должен разбиваться более чем на 2 части (табл. 3).

При полной нормализации трафика по памяти скрытый канал по памяти, основанный на изменении длин передаваемых пакетов, полностью уничтожается в связи с тем, что все пакеты становятся одинаковой длины. Однако если учесть, что нарушитель может построить скрытый канал по времени на основе изменения длин межпакетных интервалов, то остаточная пропускная способность скрытого канала будет приблизительно равна пропускной способности скрытого канала только по времени.

Приведем результаты оценки параметров скрытого канала по времени без ошибок (табл. 4) и с ошибками декодирования (табл. 5), в таблицах m — количество разных межпакетных интервалов, p — вероятность, с которой выбирается один из двух межпакетных интервалов в распределении Бернулли, v — пропускная способность. При исследовании параметры были выбраны следующим образом: среднее время, требуемое для передачи одного символа $\tau = 0{,}000895$ секунд, $\beta = 100$ Мбит/с.

4. Оценка остаточной пропускной способности скрытого канала при частичной нормализации трафика

При частичной нормализации трафика скрытый канал по памяти, основанный на изменении длин передаваемых пакетов, уничтожается не полностью, следовательно, остается бинарный скрытый канал по памяти. Нарушителю наиболее целесообразно построить бинарный скрытый канал на основе пакетов длины $l_{фикс} + H_1$ и $l_{фикс} + H_2$. Найдем остаточную

3 Al Falasi H., Zhang L. Modeling and justification of the store and forward protocol: covert channel analysis // Proceedings of the 6th International Conference on Information Warfare and Security, 2011, p. 8.

Таблица 3.

Результаты оценки параметров метода противодействия на основе нормализации канала по памяти

	Полная нормализация			Частичная нормализация			
	$l_{выр}$, бит	Доля дополнительных пакетов	Эффективная пропускная способность /β	$l_{выр\_1}$, бит	$l_{выр\_2}$, бит	Доля дополнительных пакетов	Эффективная пропускная способность /β
IPv4	6240	1,57807	0,76619	800	12000	1,97688	0,95644
IPv6	1656	2,00000	0,75897	1152	12000	1,28330	0,94644

Таблица 4.

Пропускная способность скрытых каналов по времени без ошибок при различных распределениях

Вид распределения	Протокол сетевого уровня					
	IPv4 ($l_{вып}$ = 780 байт)			IPv6 ($l_{вып}$ = 207 байт)		
	m	p	v(бит/с)	m	p	v(бит/с)
Равномерное	4	—	440,78	4	-	445,28
Параболическое	5	—	491,97	4	—	497,82
Линейное	5	—	507,01	4	—	513,39
Гиперболическое	5	—	518,28	5	—	524,32
Показательное	>10	—	549,09	>10	—	556,09
Пуассона (усечённое)	>7	—	510,24	>7	—	518,45
Схема Бернулли	2	0,615237	378,31	2	0,617278	385,27

Таблица 5.

Пропускная способность скрытых каналов по времени с ошибками декодирования при различных распределениях

Вид распределения	Протокол сетевого уровня					
	IPv4 ($l_{вып}$ = 780 байт)			IPv6 ($l_{вып}$ = 207 байт)		
	m	p	v(бит/с)	m	p	v(бит/с)
Равномерное	4	—	784,35	4	—	800,30
Параболическое	5	—	868,51	4	—	887,94
Линейное	5	—	901,90	5	—	921,54
Гиперболическое	5	—	925,01	5	—	946,46
Показательное	>10	—	973,43	>10	—	998,13
Пуассона (усечённое)	>7	—	872,95	>7	—	900,89
Схема Бернулли	2	0,5972	638,43	2	0,6007	661,47

пропускную способность полученного скрытого канала по памяти:

$$v = \max_p \frac{-\beta\,(p\log_2 p + (1-p)\log_2(1-p))}{(l_{фикс}+H_1)\,p + (l_{фикс}+H_2)\,(1-p) + \beta T} =$$

$$= \max_p \frac{-\beta\,(p\log_2 p + (1-p)\log_2(1-p))}{l_{фикс}+H_1+(H_2-H_1)\,(1-p)+\beta T}, \quad (15)$$

где T — длина межпакетного интервала.

Расчетным путем были найдены значение p и остаточная пропускная способность для протоколов IPv4 и IPv6 для канала без ошибок в скрытом канале только по памяти. Для протокола IPv4 пропускная способность равна 1042.24 бит/с, p = 0,520217; для протокола IPv6 пропускная способность равна 1038.53 бит/с, p = 0,519512.

Однако далее следует определить остаточную пропускную способность гибридного скрытого канала. Сначала рассмотрим скрытый канал без ошибок, то есть $T = 2\tau$. Формула пропускной способности для канала без ошибок:

$$v = \max_p \frac{-\beta\,(p\log_2 p + (1-p)\log_2(1-p)) + H(T)}{(l_{фикс}+H_1)\,p + (l_{фикс}+H_2)\,(1-p) + \beta E(T)} =$$

$$= \max_p \frac{-\beta\,(p\log_2 p + (1-p)\log_2(1-p) + H(T))}{l_{фикс}+H_1+(H_2-H_1)\,(1-p)+\beta E(T)}. \quad (16)$$

Приведем зависимость остаточной пропускной способности гибридного скрытого канала от параметра p для различных распределений в скрытом канале по времени без ошибок, причем для каждого распределения уже выбрано оптимальное значение параметра m (рис. 5) и оценки пропускной способности (табл. 6).

Приведем зависимости остаточной пропускной способности скрытого канала от параметра p для разных значений m для шести различных распределений в гибридном скрытом канале (рис. 6).

Таблица 6.

Значения остаточной пропускной способности гибридного скрытого канала без ошибок

Вид распределения	Протокол сетевого уровня					
	IPv4			IPv6		
	m	p	v(бит/с)	m	p	v(бит/с)
Равномерное	2	0,5141	727,32	2	0,5136	726,42
Параболическое	3	0,5152	781,92	3	0,5147	781,09
Линейное	3	0,5156	806,79	3	0,5151	805,89
Гиперболическое	3	0,5158	813,47	3	0,5153	812,54
Показательное	>10	0,5160	824,00	>10	0,5155	823,22
Пуассона (усечённое)	>7	0,5166	855,10	>7	0,5160	854,09
Схема Бернулли	2	0,5972	638,43	2	0,6007	661,47

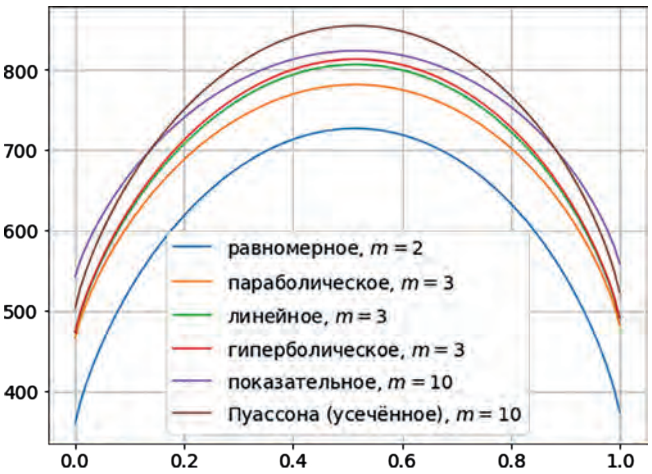


Рис. 5. График зависимости остаточной пропускной способности гибридного скрытого канала от параметра p для различных распределений в скрытом канале по времени без ошибок

Аналогично остаточная пропускная способность рассчитана для скрытого канала с ошибками декодирования. Приведем зависимость остаточной пропускной способности гибридного скрытого канала от параметра p для различных распределений в скрытом канале по времени с ошибками декодирования, отметим, что для каждого распределения выбрано оптимальное значение параметра m (рис. 7), а также результаты оценки пропускной способности для гибридного скрытого канала с ошибками декодирования для различных распределений и значений параметров m и p. (табл. 7).

Проведенные расчеты показывают, что частично нормализовать скрытые каналы по памяти не целесообразно, для такого типа скрытых каналов необходима полная нормализация.

Таблица 7.

Значения остаточной пропускной способности гибридного скрытого канала с ошибками декодирования

Вид распределения	Протокол сетевого уровня					
	IPv4			IPv6		
	m	p	v(бит/с)	m	p	v(бит/с)
Равномерное	2	0,5257	1328,77	2	0,5249	1325,51
Параболическое	3	0,5276	1425,84	3	0,5267	1422,85
Линейное	3	0,5284	1468,37	3	0,5275	1465,11
Гиперболическое	3	0,5287	1484,03	3	0,5278	1480,67
Показательное	>10	0,5293	1513,21	>10	0,5283	1510,38
Пуассона (усечённое)	>7	0,5300	1547,83	>7	0,5290	1544,21
Схема Бернулли	2	0,5972	638,43	2	0,6007	661,47

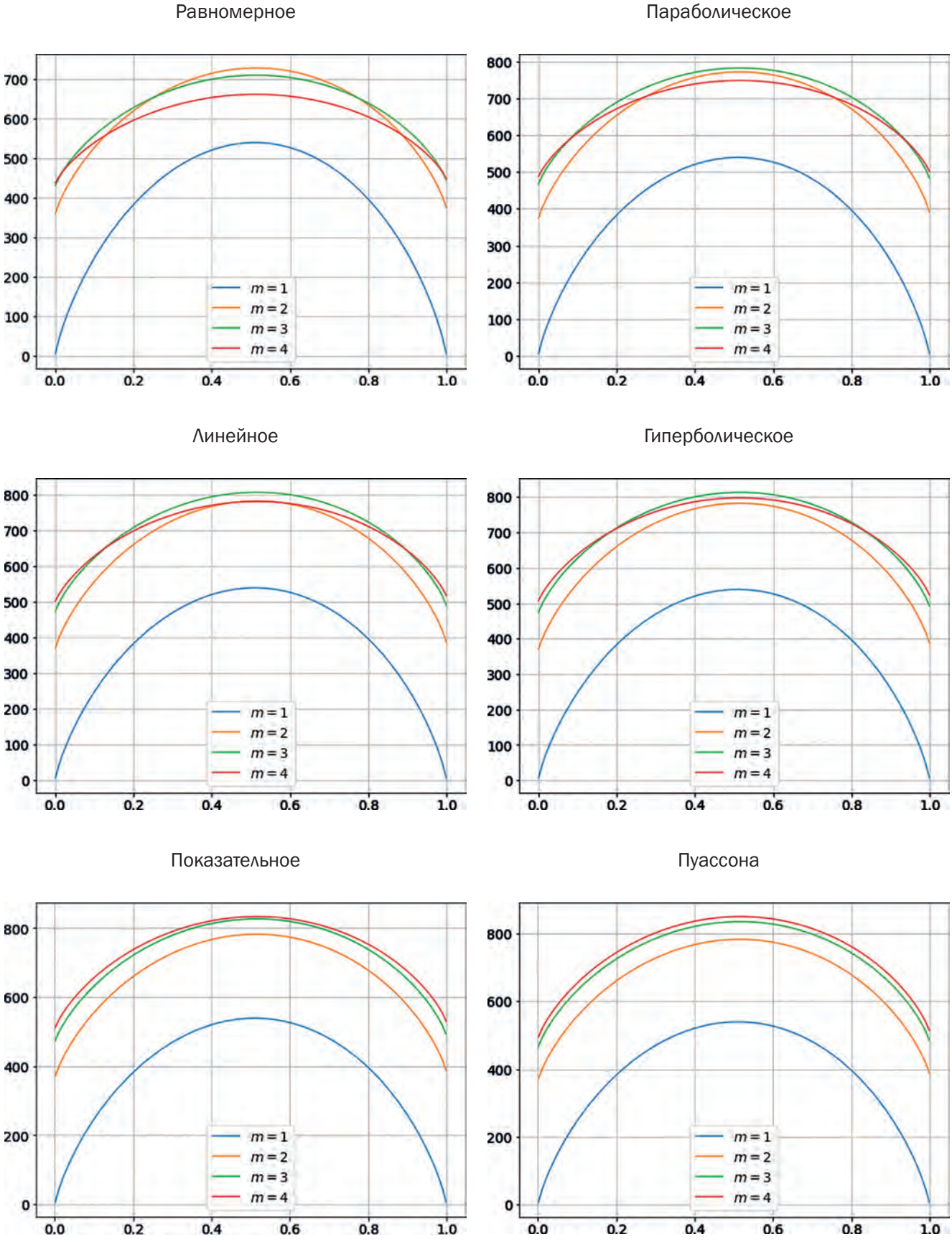


Рис. 6. Графики зависимости остаточной пропускной способности скрытого канала от параметра p для разных значений m для шести различных распределений в гибридном скрытом канале

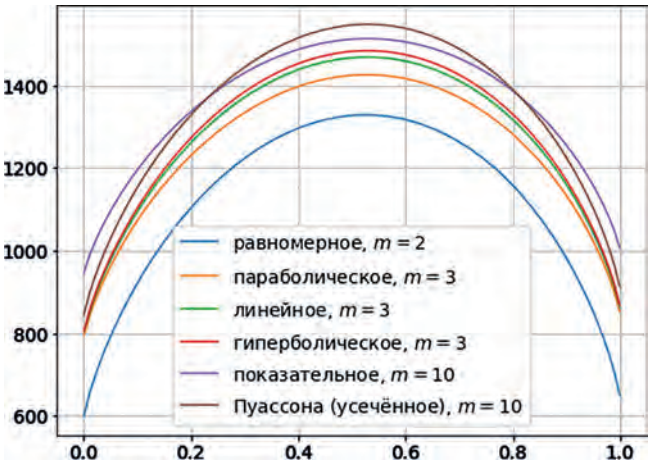


Рис. 7. График зависимости остаточной пропускной способности гибридного скрытого канала от параметра p для различных распределений в скрытом канале по времени с ошибками декодирования

5. Полная нормализация скрытого канала по времени

В случае, если была проведена полная нормализация длин пакетов, а остаточная пропускная способность скрытого канала все еще велика, можно дополнительно нормализовать трафик по времени. Так как в предыдущем разделе было показано, что скрытый канал по памяти необходимо полностью нормализовать, то остаточный скрытый канал может быть только скрытым каналом по времени. Соответственно, необходимо оценить возможность его нормализации.

Нормализация скрытого канала по времени осуществляется за счет введения задержек пакетов и генерации фиктивного трафика таким образом, чтобы в момент отправки между всеми пакетами были равные межпакетные интервалы $t_{выр}$. Если следующий после только что отправленного пакета пакет пришел через время $t(i) <= t_{выр}$, то этот пакет задерживается на $t_{выр} - t(i)$, и только потом отправляется. Если же пакет пришел через $t(i) > t_{выр}$, то генерируется и последовательно отравляется $[t(i) / t_{выр}] - 1$ пакетов, после чего отправляется пришедший пакет с необходимой задержкой.

При выборе параметра метода противодействия необходимо соблюдать баланс между средней задержкой пакета и объемом фиктивного трафика. Имея распределение вероятностей длин межпакетных интервалов в трафике, найдем среднюю задержку пакета d:

$$d = \sum_{i=1}^{m} \left(\left[\frac{t(i)}{t_{выр}} \right] t_{выр} \; t(i) \right) p(i). \qquad (17)$$

Доля фиктивных пакетов выражается как

$$\sum_{i=1}^{m} \left(\left[\frac{t(i)}{t_{выр}} \right] - 1 \right) p(i) \qquad (18)$$

Пусть задан параметр γ — максимально допустимая средняя задержка пакета. Тогда для нахождения оптимального значения параметра $t_{выр}$ необходимо решить следующую задачу минимизации:

$$\begin{cases} \sum_{i=1}^{m} \left(\left[\frac{t(i)}{t_{выр}} \right] - 1 \right) p(i) \longrightarrow \min\limits_{t_{выр}}; \\ d = \sum_{i=1}^{m} \left(\left[\frac{t(i)}{t_{выр}} \right] t_{выр} \; t(i) \right) p(i) \le \gamma. \end{cases} \qquad (19)$$

Найдем эффективную пропускную способность канала связи в условиях противодействия:

$$\beta' = \frac{E(T)}{E(T) + d} \beta = \frac{\sum_{i=1}^{m} t(i) \; p(i)}{\sum_{i=1}^{m} \left[\frac{t(i)}{t_{выр}} \right] t_{выр} \; p(i)} \beta, \qquad (20)$$

где $E(T)$ – средний межпакетный интервал в трафике.

При таком способе противодействия скрытый канал по времени полностью уничтожается. Если учесть, что длины пакетов были также выровнены, то можно прийти к выводу, что остаточная пропускная способность рассматриваемого гибридного скрытого канала стремится к нулю.

Для численной оценки параметров противодействия были проведены эксперименты с использованием данных о распределении длин межпакетных интервалов IPv4- и IPv6-пакетов, полученных из трафика[4]. При различных заданных параметрах γ расчетным путем было найдено оптимальное значение параметра $t_{выр}$, а также доля фиктивных пакетов в трафике. Также была оценена эффективная пропускная способность канала связи при значении пропускной способности канала связи $\beta = 100$ Мбит/с и при использовании значения $l_{выр}$, полученного в предыдущем подразделе (табл. 8).

Полученные результаты свидетельствуют о значительном уменьшении эффективной пропускной способности канала связи, что не позволяет применять данный метод противодействия на практике.

6. Частичная нормализация трафика как метод противодействия скрытым каналам по времени

Поскольку при полной нормализации трафика по времени эффективная пропускная способность канала связи значительно снижается, рассмотрим менее радикальный метод противодействия — частичную нормализацию трафика. При таком подходе для выравнивания используются два межпакетных интервала с длинами $t_{выр\_1}$ и $t_{выр\_2}$.

Пусть имеется исходный межпакетный интервал длиной $t(i)$. Тогда:

- если $t(i) \le t_{выр\_1}$, то пакет задерживается на $t_{выр\_1} - t(i)$ секунд;

4 https://www.caida.org/

Таблица 8.

Результаты оценки параметров метода противодействия на основе полной нормализации скрытого канала по времени

Протокол	γ, с	Средняя задержка d, с	$t_{выр}$, с	Доля фиктивных пакетов	Эффективная пропускная способность метода $/\beta$	Итоговая эффективная пропускная способность метода $/\beta$
IPv4	10^{-4}	$0{,}316 \cdot 10^{-4}$	$4{,}0055 \cdot 10^{-5}$	0	0,0499	0,0477
	10^{-5}	10^{-5}	$1{,}3829 \cdot 10^{-5}$	0,001	0,1443	0,1380
	10^{-6}	10^{-6}	$0{,}2504 \cdot 10^{-5}$	0,227	0,6269	0,5996
	10^{-7}	10^{-7}	$0{,}0338 \cdot 10^{-5}$	4,370	0,9451	0,9039
IPv6	10^{-4}	$0{,}143 \cdot 10^{-4}$	$2{,}0028 \cdot 10^{-5}$	0	0,1031	0,0976
	10^{-5}	10^{-5}	$1{,}4067 \cdot 10^{-5}$	0,001	0,1467	0,1388
	10^{-6}	10^{-6}	$0{,}2504 \cdot 10^{-5}$	0,241	0,6337	0,5997
	10^{-7}	10^{-7}	$0{,}0339 \cdot 10^{-5}$	4,355	0,9440	0,8934

- если $t_{выр\_1} < t(i) \le t_{выр\_2}$, вычисляем количество пакетов с межпакетными интервалами $t_{выр\_1}$, необходимых для того, чтобы отправить пакет через интервал $t(i)$ только с помощью длины $t_{выр\_1}$, необходимых для отправки пакета:

$$k_1 = \left[\frac{t(i)}{t_{выр\_1}} \right]; \tag{21}$$

  - если $t_{выр\_2} \le k_1 t_{выр\_1}$, то пришедший пакет задерживается на $t_{выр\_2} - t(i)$ секунд;
  - иначе отправляется $k_1 - 1$ фиктивный пакет и за ними пришедший пакет с межпакетными интервалами $t_{выр\_1}$;
- если $t(i) > t_{выр\_2}$, то отправляется

$$k_1 = \left[\frac{t(i)}{t_{выр\_2}} \right] - 1 \tag{22}$$

фиктивный пакет с межпакетными интервалами $t_{выр\_2}$, а оставшаяся комбинация пакетов с интервалами $t_{выр\_1}$ и $t_{выр\_2}$ находится аналогично.

Выбор параметров противодействия $t_{выр\_1}$ и $t_{выр\_2}$ производится на основе минимизации доли фиктивных пакетов в трафике и ограничением на максимально допустимую среднюю задержку пакетов γ, где γ задается владельцем канала связи.

При выборе параметра метода противодействия необходимо соблюсти баланс между средней задержкой пакета и объемом фиктивного трафика. Имея распределение вероятностей длин межпакетных интервалов в трафике, найдем среднюю задержку пакета:

$$d = \sum_{i=1}^{m} \left(\left(\left[\frac{t(i)}{t_{выр\_2}} \right] - 1 \right) t_{выр\_2} + \right.$$

$$\left. + \min \left\{ \left[\frac{t(i) - \left(\left[\frac{t(i)}{t_{выр\_2}} \right] - 1 \right) t_{выр\_2}}{t_{вых\_1}} \right] t_{вых\_1}, t_{вых\_2} \right\} - t(i) \right) p(i). \tag{23}$$

Пусть задан параметр γ — максимально допустимая средняя задержка пакета. Тогда для нахождения оптимального значения параметров $t_{выр\_1}$ и $t_{выр\_2}$ необходимо решить следующую задачу минимизации: минимизируем долю фиктивных пакетов при условии, что средняя задержка пакета не превышает γ.

Также найдем эффективную пропускную способность канала связи в условиях противодействия:

$$\beta' = \frac{E(T)}{E(T) + d} \beta . \tag{24}$$

Для численной оценки параметров противодействия были проведены эксперименты с использованием данных о распределении длин межпакетных интервалов IPv4- и IPv6-пакетов, полученных из трафика[5]. При различных заданных параметрах γ расчетным путем было найдено оптимальное значение параметров $t_{выр\_1}$ и $t_{выр\_2}$, а также доля фиктивных пакетов в трафике. Также была оценена эффективная пропускная способность канала связи при значении пропускной способности канала связи β = 100 Мбит/с и при использовании значения $l_{выр}$, полученного в предыдущем разделе (табл. 9).

7. Оценка остаточной пропускной способности скрытого канала при частичной нормализации канала по времени

После полной нормализации трафика по памяти и частичной нормализации трафика по времени у злоумышленника остается возможность построить только бинарный скрытый канал по времени на основе

5 https://www.caida.org/

Таблица 9.

Значения параметров метода противодействия на основе частичной нормализации канала по времени

	γ, с	Средняя задержка d, с	$t_{вып\_1}$, с	$t_{вып\_2}$, с	Доля фиктивных пакетов	Эффективная пропускная способность метода β' / β	Итоговая эффективная пропускная способность β' / β
IPv4	10^{-5}	$0{,}640 \cdot 10^{-5}$	$1{,}0014 \cdot 10^{-5}$	$2{,}0027 \cdot 10^{-5}$	0	0,2050	0,1937
	10^{-6}	10^{-6}	$0{,}2670 \cdot 10^{-5}$	$0{,}5027 \cdot 10^{-5}$	0,048	0,6312	0,6037
	10^{-7}	10^{-7}	$0{,}0436 \cdot 10^{-5}$	$0{,}1003 \cdot 10^{-5}$	1,106	0,9483	0,9070
IPv6	10^{-5}	10^{-5}	$1{,}4108 \cdot 10^{-5}$	$2{,}7204 \cdot 10^{-5}$	0	0,1467	0,1388
	10^{-6}	10^{-6}	$0{,}2558 \cdot 10^{-5}$	$0{,}4904 \cdot 10^{-5}$	0,068	0,6251	0,5916
	10^{-7}	10^{-7}	$0{,}0465 \cdot 10^{-5}$	$0{,}1004 \cdot 10^{-5}$	1,084	0,9473	0,8965

межпакетных интервалов $t_{вып\_1}$ и $t_{вып\_2}$. Найдем остаточную пропускную способность указанного скрытого канала по времени:

$$\nu = \max_{p} \frac{-\beta\,(p \log_2 p + (1-p) \log_2 (1-p))}{l_0 + H + (t_{вып\_1}\, p + t_{вып\_2}\, (1-p)\, \beta}. \quad (25)$$

Расчетным путем были найдены значение p и остаточная пропускная способность для протоколов IPv4 и IPv6 для канала без ошибок в скрытом канале только по памяти. Для протокола IPv4 пропускная способность равна 15843.1 бит/с, $p = 0{,}501557$; для протокола IPv6 пропускная способность равна 57826.7 бит/с, $p = 0{,}505401$. Таким образом, предложенные методы позволяют оценить целесообразность применения полной и частичной нормализации трафика для противодействия скрытым каналам по памяти и по времени.

Выводы

В работе исследованы скрытые каналы по памяти и по времени, предложены алгоритмы полной и частичной нормализации трафика для противодействия указанных скрытым каналам. Выведены формулы для оценки эффективной пропускной способности канала связи в условиях противодействия скрытым каналам и остаточной пропускной способности скрытого канала.

При полной нормализации трафика по памяти скрытый канал по памяти, основанный на изменении длин передаваемых пакетов, полностью уничтожается в связи с тем, что все пакеты становятся одинаковой длины. Однако если учесть, что нарушитель может построить скрытый канал по времени на основе изменения длин межпакетных интервалов, то остаточная пропускная способность скрытого канала будет приблизительно равна пропускной способности скрытого канала только по времени. При частичной нормализации трафика скрытый канал по памяти, основанный на изменении длин передаваемых пакетов, уничтожается не полностью, следовательно, остается бинарный скрытый канал по памяти, оценки пропускной способности которого показывают нецелесообразность применения частичной нормализации скрытого канала по времени и указывают на необходимость его полной нормализации.

В случае, если была проведена полная нормализация длин пакетов, а остаточная пропускная способность скрытого канала все еще велика, можно дополнительно нормализовать трафик по времени. Нормализация скрытого канала по времени осуществляется за счет введения задержек пакетов и генерации фиктивного трафика таким образом, чтобы в момент отправки между всеми пакетами были равные межпакетные интервалы. В работе предложен способ противодействия, при котором скрытый канал по времени полностью уничтожается.

Рассчитаны количественные значения эффективной пропускной способности канала связи и остаточной пропускной способности скрытого канала при использовании протоколов IPv4 и IPv6, которые могут быть полезны при применении методов нормализации трафика на практике.

Литература

1. *Zhang, X., Pang, L., Guo, L., Li, Y. Building Undetectable Covert Channels Over Mobile Networks with Machine Learning // Machine Learning for Cyber Security. ML4CS 2020. Lecture Notes in Computer Science, vol 12486, 2020, pp. pp 331–339. https://doi.org/10.1007/978-3-030-62223-7_28.*
2. *Dakhane, D. M., Narawade, V. E. Reference Model Storage Covert Channel for Secure Communications // Advanced Computing Technologies and Applications. Algorithms for Intelligent Systems, 2020, pp. 489–496. https://doi.org/10.1007/978-981-15-3242-9_46.*

3. Sattolo T. A. V., Jaskolka J. Evaluation Of Statistical Tests For Detecting Storage-Based Covert Channels // IFIP Advances in Information and Communication Technology, vol. 580, 2020, pp. 17–31.
4. Dua A., Jindal V., Bedi P. Detecting And Locating Storage-Based Covert Channels In Internet Protocol Version 6 // IEEE Access, vol. 10, 2022, pp. 110661-110675.
5. Когос К. Г., Финошин М. А., Айрапетян С. В. Метод идентификации скрытых каналов по памяти в сетях пакетной передачи данных // Безопасность информационных технологий, т. 28, № 3, 2021, с. 56–64.
6. Wang, C., Chen, RL. & Gu, L. Improving Performance of Virtual Machine Covert Timing Channel Through Optimized Run-Length Encoding // Journal of Computer Science and Technology, vol. 38, 2023, pp. 793–806. https://doi.org/10.1007/s11390-021-1189-z.
7. Nasseralfoghara, M., Hamidi, H. R. Covert timing channels: analyzing WEB traffic // Journal of Computer Virology and Hacking Techniques, vol. 18, pp. 117–126. https://doi.org/10.1007/s11416-021-00396-w.
8. Nasseralfoghara, M., Hamidi, H.R. Covert timing channels: analyzing WEB traffic // Journal of Computer Virology and Hacking Techniques, vol. 18, 2022, pp. 117–126. https://doi.org/10.1007/s11416-021-00396-w.
9. Massimi, F., Benedetto, F. Performance Improvements of Covert Timing Channel Detection in the Era of Artificial Intelligence // Advances in Distributed Computing and Machine Learning. Lecture Notes in Networks and Systems, vol. 955, 2024, pp. pp 399–410. https://doi.org/10.1007/978-981-97-1841-2_30.
10. Zhang, Z., Zhang, X., Xue, Y., Li, Y. Building a Covert Timing Channel over VoIP via Packet Length // Data Mining and Big Data. DMBD 2021. Communications in Computer and Information Science, vol. 1453, 2021, pp. pp 81–88. https://doi.org/10.1007/978-981-16-7476-1_8.
11. Zhang, X., Guo, L., Xue, Y., Jiang, H., Liu, L., Zhang, Q. A Hybrid Covert Channel with Feedback over Mobile Networks // Security and Privacy in Social Networks and Big Data. Communications in Computer and Information Science, vol. 1095, 2019, pp. 87–94. https://doi.org/10.1007/978-981-15-0758-8_7.
12. Belozubova A., Kogos K., Epishkina A. On/Off Covert Channel Capacity Limitation by Adding Extra Delays // Proceedings of the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus, 2021, pp. 2318–2322.
13. Epishkina, A., Karapetyants, N., Kogos, K. et al. Covert channel limitation via special dummy traffic generating // Journal of Computer Virology and Hacking Techniques, vol. 19, 2023, pp. 341–349. https://doi.org/10.1007/s11416-022-00428-z.
14. Epishkina, A., Frolova, D., Kogos, K. A technique to limit hybrid covert channel capacity via random increasing of packets' lengths // Procedia Computer Science, vol. 190, 2020, pp. 231–240. https://doi.org/10.1016/j.procs.2021.06.029.
15. Анна И. Белозубова, Константин Г. Когос, Филипп В. Лебедев. Ограничение пропускной способности сетевых скрытых каналов по времени путем введения дополнительных случайных задержек перед отправкой пакета // Безопасность информационных технологий, том 28, № 4, 2021, с. 74–89.
16. Gorokhov D. E., Ryabokon V. V., Kuzkin A. A., Sherbakov V. S., Kutsakin M. A. // Packet Fragmentation As Data Protection Method In Automated Systems // IOP Conference Series: Materials Science and Engineering, 2020, с. 52027.

TRAFFIC NORMALIZATION FOR INFORMATION LEAKAGE PROTECTION VIA COVERT CHANNELS

Epishkina A. V.[6], Kogos K. G.[7]

The possibility of building covert channels in an information system entails a potential leak of secured information. There are many methods of countering covert channels, but not all of them are applicable in practice. The purpose of the investigation is to develop counteraction tools to prevent information leakage via storage and timing covert channels by traffic normalization.

The authors investigate storage and timing covert channels and suggest algorithms for full and partial traffic normalization to counteract these covert channels. Using the methods of information theory, probability theory, differential and integral calculus, and data on the distribution of the lengths of inter-packet intervals of network traffic packets, formulas are derived to estimate the effective capacity of a communication channel in conditions of countering covert channels and the residual capacity of a covert channel.

When the traffic is fully normalized in memory, storage covert channel based on changing the length of transmitted packets is completely destroyed due to the fact that all packets become the same length. With partial normalization of traffic, storage covert channel, based on changing the lengths of transmitted packets, is not completely destroyed, therefore, a binary storage covert channel remains, estimates of the capacity of which show the inexpediency of using partial normalization of timing covert channel and indicate the need for its full normalization.

If full normalization of packet lengths has been carried out, and the residual capacity of the covert channel is still large, it is possible to additionally normalize traffic in time. The paper proposes a method of counteraction in which timing covert channel is completely destroyed.

Quantitative values of the effective capacity of the communication channel and the residual capacity of the covert channel when using IPv4 and IPv6 protocols are calculated, which can be useful when applying traffic normalization methods in practice.

Keywords: *information security, information leakage, counteraction tool, network covert channel, storage covert channel, timing covert channel, traffic normalization, partial normalization нормализация, channel capacity.*

6 Anna V. Epishkina, Ph.D., Associate Professor, Cryptology and Cybersecurity Department, NRNU MEPhI, Moscow, Russia. E-mail: avepishkina@mephi.ru
7 Konstantin G. Kogos, Ph.D., Associate Professor, Cryptology and Cybersecurity Department, NRNU MEPhI, Moscow, Russia. E-mail: kgkogos@mephi.ru

References

1. *Zhang, X., Pang, L., Guo, L., Li, Y. Building Undetectable Covert Channels Over Mobile Networks with Machine Learning // Machine Learning for Cyber Security. ML4CS 2020. Lecture Notes in Computer Science, vol 12486, 2020, pp. pp 331–339. https://doi.org/10.1007/978-3-030-62223-7_28.*
2. *Dakhane, D. M., Narawade, V. E. Reference Model Storage Covert Channel for Secure Communications // Advanced Computing Technologies and Applications. Algorithms for Intelligent Systems, 2020, pp. 489–496. https://doi.org/10.1007/978-981-15-3242-9_46.*
3. *Sattolo T. A. V., Jaskolka J. Evaluation Of Statistical Tests For Detecting Storage-Based Covert Channels // IFIP Advances in Information and Communication Technology, vol. 580, 2020, pp. 17–31.*
4. *Dua A., Jindal V., Bedi P. Detecting And Locating Storage-Based Covert Channels In Internet Protocol Version 6 // IEEE Access, vol. 10, 2022, pp. 110661–110675.*
5. *Kogos K. G., Finoshin M. A., Ajrapetjan S. V. Metod identifikacii skrytyh kanalov po pamjati v setjah paketnoj peredachi dannyh // Bezopasnost' informacionnyh tehnologij, t. 28, № 3, 2021, s. 56–64.*
6. *Wang, C., Chen, RL. & Gu, L. Improving Performance of Virtual Machine Covert Timing Channel Through Optimized Run-Length Encoding // Journal of Computer Science and Technology, vol. 38, 2023, pp. 793–806. https://doi.org/10.1007/s11390-021-1189-z.*
7. *Nasseralfoghara, M., Hamidi, H. R. Covert timing channels: analyzing WEB traffic // Journal of Computer Virology and Hacking Techniques, vol. 18, pp. 117–126. https://doi.org/10.1007/s11416-021-00396-w.*
8. *Nasseralfoghara, M., Hamidi, H. R. Covert timing channels: analyzing WEB traffic // Journal of Computer Virology and Hacking Techniques, vol. 18, 2022, pp. 117–126. https://doi.org/10.1007/s11416-021-00396-w.*
9. *Massimi, F., Benedetto, F. Performance Improvements of Covert Timing Channel Detection in the Era of Artificial Intelligence // Advances in Distributed Computing and Machine Learning. Lecture Notes in Networks and Systems, vol. 955, 2024, pp. pp 399–410. https://doi.org/10.1007/978-981-97-1841-2_30.*
10. *Zhang, Z., Zhang, X., Xue, Y., Li, Y. Building a Covert Timing Channel over VoIP via Packet Length // Data Mining and Big Data. DMBD 2021. Communications in Computer and Information Science, vol. 1453, 2021, pp. pp 81–88. https://doi.org/10.1007/978-981-16-7476-1_8.*
11. *Zhang, X., Guo, L., Xue, Y., Jiang, H., Liu, L., Zhang, Q. A Hybrid Covert Channel with Feedback over Mobile Networks // Security and Privacy in Social Networks and Big Data. Communications in Computer and Information Science, vol. 1095, 2019, pp. 87–94. https://doi.org/10.1007/978-981-15-0758-8_7.*
12. *Belozubova A., Kogos K., Epishkina A. On/Off Covert Channel Capacity Limitation by Adding Extra Delays // Proceedings of the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus, 2021, pp. 2318–2322.*
13. *Epishkina, A., Karapetyants, N., Kogos, K. et al. Covert channel limitation via special dummy traffic generating // Journal of Computer Virology and Hacking Techniques, vol. 19, 2023, pp. 341–349. https://doi.org/10.1007/s11416-022-00428-z.*
14. *Epishkina, A., Frolova, D., Kogos, K. A technique to limit hybrid covert channel capacity via random increasing of packets' lengths // Procedia Computer Science, vol. 190, 2020, pp. 231–240. https://doi.org/10.1016/j.procs.2021.06.029.*
15. *Anna I. Belozubova, Konstantin G. Kogos, Filipp V. Lebedev. Ogranichenie propusknoj sposobnosti setevyh skrytyh kanalov po vremeni putem vvedenija dopolnitel'nyh sluchajnyh zaderzhek pered otpravkoj paketa // Bezopasnost' informacionnyh tehnologij, tom 28, № 4, 2021, s. 74–89.*
16. *Gorokhov D. E., Ryabokon V. V., Kuzkin A. A., Sherbakov V. S., Kutsakin M. A. // Packet Fragmentation As Data Protection Method In Automated Systems // IOP Conference Series: Materials Science and Engineering, 2020, c. 52027.*

ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ПРИМЕНЕНИЯ ПРЕДВАРИТЕЛЬНО ОБУЧЕННЫХ ГРАФОВЫХ НЕЙРОННЫХ СЕТЕЙ С МЕХАНИЗМОМ ВНИМАНИЯ

Шевченко В. А.[1], Запечников С. В.[2]

DOI: 10.21681/2311-3456-2024-5-18-27

Аннотация. *В статье предлагается комплекс криптографических протоколов для реализации системы конфиденциального машинного обучения на основе графовых нейронных сетей с механизмом внимания (далее – системы «КонфГраф»). Приведена классификация искусственных нейронных сетей, лежащих в основе глубокого обучения. Выделены основные задачи обеспечения конфиденциальности, возникающие при обучении и применении моделей машинного обучения на основе искусственных нейронных сетей. Приведено описание основных криптографических примитивов, необходимых для реализации протоколов безопасных многосторонних вычислений, а именно схем разделения секрета и протокола передачи с забыванием. В статье приводится краткая характеристика методологии доказательства безопасности криптографических протоколов, в том числе протоколов безопасных многосторонних вычислений, называемой универсальной компонуемостью (UC-security). Описываются и анализируются основные и вспомогательные протоколы, лежащие в основе системы «КонфГраф»: «коррелированный» протокол передачи с забыванием, а также протоколы конфиденциального умножения матриц, вычисления значений функций активации ReLU и LeakyReLU, приводятся доказательства их безопасности. Остальные протоколы, применяющиеся в «КонфГраф», перечислены в статье с кратким описанием их входных и выходных данных. Безопасность предлагаемых протоколов системы «КонфГраф» доказывается на основе методологии универсальной компонуемости.*

Ключевые слова: *криптография, информационная безопасность, конфиденциальное машинное обучение, безопасные многосторонние вычисления, графовые нейронные сети с механизмом внимания, схемы разделения секрета, протокол передачи с забыванием.*

Введение

Одной из ключевых технологических тенденций XXI века, несомненно, является искусственный интеллект (ИИ). Его внедрение в различные области может оказать существенное влияние как на бизнес, так и на повседневную жизнь человека. По оценкам Министерства экономического развития РФ Россия входит в первую десятку стран по объему совокупных вычислительных мощностей, используемых для реализации функций ИИ.

Реализация технологий ИИ стала возможной благодаря бурному развитию машинного обучения (МО). В настоящий момент существуют десятки видов моделей МО, решающих различные задачи от прогнозирования численных значений до создания изображений или иных типов данных. Особенно высоких результатов в той или иной сфере применения ИИ можно достигнуть посредством глубокого обучения, которое, по сути, представляет собой МО с применением искусственных нейронных сетей (НС).

Выделяют следующие основные классы НС: полносвязные, рекуррентные, сверточные и графовые. В современных глубоких НС используются преимущественно три последние типа архитектур [1]. Рекуррентные НС представляют собой совокупность слоёв нейронов, накапливающих предыдущее состояние НС и циклически обрабатывающих вновь поступающие данные, что делает их инструментом обработки линейно упорядоченных данных. В основе сверточных НС, как понятно из названия, лежит математическая операция кросс-корреляции (свёртки), что обуславливает их высокую эффективность при обработке многомерных регулярных массивов данных, в том числе, при решении задач распознавания образов. Граф является мощным инструментом представления и обработки сложноструктурированных данных, благодаря чему графовые НС (ГНС) преимущественно используются для решения задачи анализа данных, не имеющих регулярной структуры [2].

1. Графовые нейронные сети

Простейшим, но и наиболее востребованным в прикладных задачах видом ГНС являются сверточные ГНС. Пусть задан некоторый граф $G = (V,E)$,

1 Шевченко Вячеслав Андреевич, соискатель, Национальный исследовательский ядерный университет «МИФИ», Москва, Россия. E-mail sheff-slava@mail.ru
2 Запечников Сергей Владимирович, доктор технических наук, доцент, профессор Национального исследовательского ядерного университета «МИФИ», Москва. Россия. E-mail: svzapechnikov@mephi.ru

где V – множество вершин, E – множество рёбер. Пусть каждой вершине v_i сопоставлен вектор атрибутов x_i. Совокупность векторов атрибутов вершин графа образует матрицу X. ГНС позволяет решать задачи классификации на множестве вершин графа, подграфах графа и графе в целом. Идея свёрточной ГНС основана на том, что в такой сети эмбеддинги (векторные представления в признаковом пространстве) каждой из вершин графа вычисляются на основе атрибутов как самой вершины, так и соседних с ней вершин. Глубина распространения влияния атрибутов на соседние вершины графа определяется количеством слоёв ГНС.

Пусть x_i – атрибут вершины графа v_i, X – матрица атрибутов вершин, W – матрица весов модели МО, тогда состояние вершины графа v_i в сверточной ГНС будет обновляться в соответствии с выражением [3]:

$$h_i = \sum_{j \in N(v_i)} x_j W^T, \quad (1)$$

что в матричной форме можно представить так

$$H = \tilde{A}^T X W^T, \quad (2)$$

где A – матрица смежности графа, $\tilde{A} = A + I$, I – единичная матрица.

Дальнейшее развитие ГНС привело к появлению ГНС с механизмом внимания (attention mechanism), отличительной чертой которых является наличие весов внимания, которые, в буквальном смысле, увеличивают влияние весов одних вершин, а других – уменьшают. В таких НС состояние вершины графа v_i будет обновляться в соответствии с выражениями в линейной форме

$$h_i = \sum_{j \in N(v_i)} a_{i,j} W x_j, \quad (3)$$

и в матричной форме

$$H = \tilde{A}^T W_\alpha X W^T, \quad (4)$$

где $a_{i,j}$ – коэффициент внимания вершины v_i по отношению к вершине v_j, W_α – матрица коэффициентов (весов) внимания.

2. Конфиденциальное машинное обучение

Однако при создании, развертывании и применении моделей МО, в том числе ГНС с механизмом внимания, не всегда уделяется должное внимание конфиденциальности. Риски нарушения конфиденциальности информации возникают как при обучении, так и при применении моделей МО, развернутых в недоверенной среде, например, в облаке. Требования к конфиденциальности особенно актуальны при обработке персональных данных, а также информации, содержащей охраняемые законом виды тайны: коммерческую, банковскую, врачебную и др. Кроме того, сама модель МО может являться интеллектуальной собственностью её владельца, поэтому даже при известной архитектуре НС её параметры тоже требуют защиты.

Перечисленные факторы привели к появлению новой области исследований на стыке МО и криптографии – конфиденциального машинного обучения (КМО). Предметом КМО является разработка методов и алгоритмов, позволяющих обучать и применять модели МО в условиях взаимного недоверия между владельцем модели МО, провайдером вычислительных ресурсов и клиентом, желающим направить некоторый запрос к модели (или даже обучить модель) [4]. КМО стало возможно благодаря развитию таких методов криптографии, как гомоморфное шифрование и безопасные многосторонние вычисления (БМВ).

Основная цель протоколов БМВ состоит в вычислении несколькими участниками общей функции без раскрытия друг другу своих исходных данных, которые являются конфиденциальными. Это достигается посредством применения ряда криптографических примитивов [5].

1. Схемы разделения секрета. В БМВ используются два основных вида СРС: пороговые и арифметические. (t,n)-пороговой схемой разделения секрета называют схему, позволяющую разделить секрет x на n долей, причем обладание любыми $t-1$ долями не позволяет получить никакой информации об x, тогда как обладание t долями позволяет однозначно восстановить x. Более строго схемы разделения секрета можно описать следующим образом. Пусть X – множество секретов, X_1 – множество долей секретов, $Shr: X \longrightarrow X_1^n$ – алгоритм разделения секрета, $Rec: X_1^n \longrightarrow X$ – алгоритм восстановления секрета. Тогда (t,n)-пороговой схемой разделения секрета называется пара алгоритмов (Shr,Rec), обладающих двумя свойствами [6]:

1) корректностью: если $Shr(x) = (x_1,x_2,...,x_n)$, то $Pr[\forall k \geq t, Rec(x_{i_1},x_{i_2},...,x_{i_k}) = x] = 1$;
2) совершенной секретностью: если a, b – секреты, а $v = v_1,v_2,...,v_k$ – вектор любых возможных долей секрета, причем $k < t$, то $Pr[Shr(a)|_k = v] = Pr[Shr(b)|_k = v]$, где $|_k$ – проекция на множество из k элементов.

В настоящей работе нашла применение арифметическая схема разделения секрета (АСРС). Основные операции АСРС можно описать так:

- Shr: S_i случайно выбирает $r \in_{\mathbb{R}} \mathbb{Z}_q$, где q – большое простое число, известное обоим участникам, отправляет его S_{1-i}, вычисляет $\langle x \rangle_i^A = x - r \bmod q$, S_{1-i} принимает, что $\langle x \rangle_{1-i}^A = x$;
- Rec: S_{1-i} отправляет S_i имеющееся у него значение $\langle x \rangle_{1-i}^A$, S_i рассчитывает $x = \langle x \rangle_i^A + \langle x \rangle_{1-i}^A \bmod q$.

2. Протокол передачи с забыванием (oblivious transfer). Пусть взаимодействуют два участника: отправитель, хранящий секреты x_0 и x_1, и получатель, выбирающий один из только один из двух секретов путем генерации бита выбора $b \in \{0,1\}$. Протокол передачи с забыванием позволяет получателю узнать выбранный секрет x_b, при этом не получая никакой информации о значении другого секрета x_{1-b}. В то же время, отправитель не получает информации о выборе, сделанном получателем [7].

3. Протоколы системы конфиденциального машинного обучения на основе ГНС

Предлагаемая система КМО на основе ГНС с механизмом внимания, названная нами «КонфГраф», поддерживает конфиденциальное применение предварительно обученной модели МО и подразумевает наличие следующих участников протокола:

1) клиента, обладающего матрицей атрибутов вершин X некоторого графа G и желающего сохранить ее в тайне;
2) владельца обученной ГНС с механизмом внимания, обладающей следующими параметрами: матрицей смежности графа A, матрицей весов W и матрицей весов линейного преобразования для вычисления коэффициентов внимания W_{att} – желающего сохранить перечисленные параметры модели в тайне;
3) двух независимых серверов S_i, $i \in \{0,1\}$ (например, принадлежащих разным облачным провайдерам).

Клиенту требуется получить ответ от модели МО на его данных, представленных в форме матрицы X. Владелец модели МО обладает предварительно обученной моделью на основе ГНС с механизмом внимания, способной дать желаемый клиентом результат, но не имеет достаточных вычислительных ресурсов для этого, поэтому вынужден прибегать к помощи двух независимых облачных провайдеров. Однако ни клиент, ни владелец модели не доверяют ни друг другу, ни облачным провайдерам, поэтому для сохранения конфиденциальности информации клиента и владельца модели требуется применение механизмов КМО.

В первом приближении принцип работы предлагаемой системы «КонфГраф» можно описать следующим образом.

1. Все участники протокола согласуют ряд значений общедоступных величин:
   1) большого простого числа q;
   2) длины чисел ℓ в битах;
   3) параметра безопасности κ;
   4) длины дробной части чисел f, измеряющейся в битах (предполагается использование чисел с фиксированной точкой).
2. Клиент и владелец модели подготавливают исходные данные.
3. Сервер S_i вычисляет разделенную по АСРС матрицу коэффициентов внимания $\langle W_\alpha \rangle_i^A$ с применением протоколов БМВ следующим образом:
   3.1. Транспонирование $\left(\langle W \rangle_i^A\right)^T$.
   3.2. Конфиденциальное вычисление произведения матриц $\langle X \rangle_i^A \cdot \left(\langle W \rangle_i^A\right)^T$.
   3.3. Составление матрицы
   $$\left(\langle X \rangle_i^A \cdot \left(\langle W \rangle_i^A\right)^T\right)[\langle X \rangle_i^A[0]],$$
   для чего при помощи протокола конфиденциального доступа к элементам массива выбираются те строки матрицы $\langle X \rangle_i^A \cdot \left(\langle W \rangle_i^A\right)^T$, номера которых соответствуют нулевой строке матрицы C.
   3.4. Составление матрицы
   $$\left(\langle X \rangle_i^A \cdot \left(\langle W \rangle_i^A\right)^T\right)[\langle X \rangle_i^A[1]],$$
   по аналогии с п. 3.3.
   3.5. Построчная конкатенация матриц
   $$\left(\langle X \rangle_i^A \cdot \left(\langle W \rangle_i^A\right)^T\right)\left[\langle X \rangle_i^A[0]\right] \text{ и } \left(\langle X \rangle_i^A \cdot \left(\langle W \rangle_i^A\right)^T\right)\left[\langle X \rangle_i^A[1]\right]$$
   (т.е. запись указанных матриц «друг рядом с другом»).
   3.6. Транспонирование результата п. 3.5:
   $$\left(\left(\langle X \rangle_i^A \cdot \left(\langle W \rangle_i^A\right)^T\right)\left[\langle X \rangle_i^A[0]\right] \parallel \left(\langle X \rangle_i^A \cdot \left(\langle W \rangle_i^A\right)^T\right)\left[\langle X \rangle_i^A[1]\right]\right)^T. \quad (5)$$
   3.7. Конфиденциальное вычисление произведения $\langle W_{att} \rangle_i^A$ и матрицы, полученной в п. 3.6, т.е.
   $$\langle W_{att} \rangle_i^A \left(\left(\langle X \rangle_i^A \cdot \left(\langle W \rangle_i^A\right)^T\right)\left[\langle X \rangle_i^A[0]\right] \parallel \parallel \left(\langle X \rangle_i^A \cdot \left(\langle W \rangle_i^A\right)^T\right)\left[\langle X \rangle_i^A[1]\right]\right)^T. \quad (6)$$
   3.8. Поэлементное конфиденциальное вычисление значения функции LeakyReLU от матрицы, полученной в п. 3.7, т.е.
   $$\text{LeakyReLu}\left(\left(\langle W_{att} \rangle_i^A \left(\left(\langle X \rangle_i^A \cdot \left(\langle W \rangle_i^A\right)^T\right)\left[\langle C \rangle_i^A[0]\right] \parallel \parallel \left(\langle X \rangle_i^A \cdot \left(\langle W \rangle_i^A\right)^T\right)\left[\langle C \rangle_i^A[1]\right]\right)^T\right)_j\right), \; i \in \{0,1\}, \; j \in \{0, R-1\} \quad (7)$$
   3.9. Создание матрицы $\langle E \rangle_i^A$, размерность которой совпадает с размерностью $\langle A \rangle_i^A$, и заполнение $\langle E \rangle_i^A$ нулями.
   3.10. Заполнение матрицы $\langle E \rangle_i^A$ посредством протокола конфиденциальной записи элемента массива (т.е. элементы матрицы, полученной в п. 3.8, будут записаны в E в соответствии с координатами, указанными в матрице C, а результат будет получен в виде $\langle E \rangle_i^A$).
   3.11. Конфиденциальное вычисление значения функции Softmax от каждой строки матрицы $\langle E \rangle_i^A$:
   $$\langle W_\alpha \rangle_i^A = \text{softmax}\left(\left(\langle E \rangle_i^A\right)_j\right), \; j \in \{0, V-1\}. \quad (8)$$

4. Сервер S_i вычисляет разделенную по АСРС матрицу вложений $\langle H\rangle_i^A$ с применением протокола конфиденциального умножения матриц:

$$\langle H\rangle_i^A = (\langle \tilde{A}\rangle_i^A)^T \cdot \langle W_\alpha\rangle_i^A \cdot \langle X\rangle_i^A \cdot (\langle W\rangle_i^A)^T. \quad (9)$$

5. Если в рассматриваемой ГНС с механизмом внимания применяется механизм многомерного внимания (multi-head attention), то серверы выполняют перечисленные операции необходимое количество раз с разными матрицами W и W_{att}, а затем локально усредняют полученные результаты.

4. Модель нарушителя и методология доказательства безопасности

Система КМО «КонфГраф» допускает присутствие пассивного нарушителя, который следует протоколу, но может собирать данные для их анализа с целью нарушения конфиденциальности информации (такого нарушителя нередко называют получестным). Кроме того, предполагается, что каждый из облачных провайдеров заинтересован в сохранении своей репутации и не будет вступать в сговор с другим с целью нарушения конфиденциальности обрабатываемых им данных. К защищаемой информации относятся матрицы X, A, C, W и W_{att}. Допускается, что нарушителю могут стать известны размерности указанных матриц, что не приведет к нарушению конфиденциальности информации. Между всеми участниками протокола существуют защищенные каналы связи с гарантированной криптографической стойкостью механизмов шифрования и аутентификации, ключи для которых распределены заранее и неизвестны нарушителю.

Для доказательства безопасности протоколов БМВ, как правило, прибегают к методологии универсальной компонуемости (UC – universal composability), в соответствии с которой сравниваются два режима работы криптографического протокола: выполнение его в реальном мире и в идеальном. Под реальным миром понимают такие условия, при которых выполнение протокола БМВ происходит привычным способом: существуют несколько участников, взаимодействующих друг с другом, а также нарушитель и некоторое окружение, предоставляющее участникам исходные данные и получающее от них результат (рис. 1). В идеальном мире все вычисления выполняет третья сторона, пользующаяся неограниченным доверием других участников (в реальности такого быть не может), а действия нарушителя моделирует специальный алгоритм – симулятор. Основная идея сравнения реального и идеального миров состоит в том, что в случае безопасного протокола БМВ нарушитель в реальном мире может добыть информации не более, чем симулятор в идеальном мире. Верно и обратное: если существует такой симулятор, который может смоделировать действия нарушителя так, что результат протокола и все промежуточные вычисления для окружения будут статистически неразличимы от соответствующих в реальном мире, то такой протокол БМВ является безопасным. Иными словами, окружение не сможет «отличить» реальный мир от идеального.

Рис. 1. Схематичное представление реального (а) и идеального (б) миров

Таким образом, применительно к предлагаемому в настоящей работе комплекту протоколов системы КМО «КонфГраф» требуется доказать следующую теорему:

Теорема 1. Система «КонфГраф» безопасно реализует применение ГНС с механизмом внимания посредством протоколов БМВ в предположении о наличии пассивного нарушителя, одновременно компрометирующего не более одного участника протокола. Доказательство проведем ниже, в п. 6, путем демонстрации существования симулятора, отвечающего условиям безопасности протокола БМВ в парадигме реального / идеального миров.

5. Протоколы системы «КонфГраф»

Приведём описания протоколов системы КМО «КонфГраф».

Протокол подготовки данных. Перед началом вычислений владельцу модели требуется преобразовать матрицу смежности графа A в форму списка координат, например:

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix} \quad (10)$$

$$C = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 4 & 4 & 5 & 5 \\ 1 & 2 & 3 & 0 & 2 & 0 & 1 & 4 & 5 & 0 & 2 & 5 & 2 & 4 \end{pmatrix}$$

Затем клиент и владелец модели применяют АСРС для представления защищаемых матриц в виде двух частей секрета:

$$X = (\langle X\rangle_0^A + \langle X\rangle_1^A) \bmod q,$$
$$A = (\langle A\rangle_0^A + \langle A\rangle_1^A) \bmod q,$$
$$C = (\langle C\rangle_0^A + \langle C\rangle_1^A) \bmod q,$$
$$W = (\langle W\rangle_0^A + \langle W\rangle_1^A) \bmod q,$$
$$W_{att} = (\langle W_{att}\rangle_0^A + \langle W_{att}\rangle_1^A) \bmod q. \quad (11)$$

После подготовки исходных данных для работы «КонфГраф» клиент и владелец модели передают серверам S_i, $i \in \{0,1\}$ $\langle X\rangle_i^A$ и $\langle A\rangle_i^A$, $\langle C\rangle_i^A$, $\langle W\rangle_i^A$ и $\langle W_{att}\rangle_i^A$ соответственно.

Коррелированный протокол передачи с забыванием [8] – специальный вариант протокола передачи с забыванием, в котором участники на выходе получают доли произведения секретов, которые они передают на вход протокола.

Входные данные: отправитель S хранит ℓ-битное число a, получатель R хранит ℓ-битное число b, g – образующий элемент циклической группы $\mathbb{Z}_q$, q – большое простое число, κ – параметр безопасности.

Результат: S вычисляет значение $\langle c\rangle_S^A$, не получая при этом никакой информации о значении b, а R вычисляет значение $\langle c\rangle_R^A$, не получая при этом никакой информации о значении b, причем $\left(\langle c\rangle_S^A + \langle c\rangle_R^A\right) \bmod 2^\ell = a \cdot b$.

Протокол:

1. S случайно выбирает κ бит $s = [s_0,\ldots,s_{\kappa-1}]$.
2. R случайно выбирает κ пар κ-битных чисел (k_i^0, k_i^1), $i \in \{0,\kappa-1\}$.
3. Посредством выполнения κ протоколов передачи с забыванием, в которых при $i \in \{0,\kappa-1\}$ S играет роль получателя с битом выбора s_i, а R играет роль отправителя с парой сообщений (k_i^0, k_i^1), S выбирает κ чисел $k_i^{s_i}$.
4. R вычисляет $t_i = G(k_i^0)$ и $u_i = t_i \oplus G(k_i^1) \oplus b$, где $G(x)$ – любой генератор псевдослучайных последовательностей (ГПСП), расширяющий входную κ-битную последовательность в ℓ-битную, t_i – i-й столбец матрицы T размерности $\ell \times \kappa$, и отправляет S все полученные u_i, $i \in \{0,\kappa-1\}$.
5. S рассчитывает $q^i = (s_i \cdot u^i) \oplus G(k_i^{s_i})$, где q^i – i-й столбец матрицы Q размерности $\ell \times \kappa$.
6. S для $j \in \{0,\ell-1\}$ рассчитывает $y_j = f_j(H(q_j)) \oplus H(q_j \oplus s)$, где $f_j(x) = (a \cdot 2^j + x) \bmod 2^\ell$ – функция корреляции, $H(x)$ – корреляционно стойкая криптографическая хэш-функция (в данной работе применяется хэш-функция SHA-3), q_j – j-я строка матрицы Q, и отправляет полученные значения R.
7. R определяет результат, как $\langle c\rangle_R^A = \sum_{j=0}^{\ell-1}(y_j \cdot \sigma_j) \oplus H(t_j)$, а S – $\langle c\rangle_S^A = \sum_{j=0}^{\ell-1} - H(q_j)$.

Конфиденциальное умножение матриц – протокол, позволяющий двум участникам получить доли элементов матрицы, равной произведению двух матриц, доли которых они передают на вход протокола.

Входные данные: разделенные по АСРС матрицы $\langle X\rangle_i^A$, $\langle Y\rangle_i^A$ размерностей $(r_0;r_1)$ и $(r_1;r_2)$ соответственно, ℓ – размерность чисел в битах, q – большое простое число, κ – статистический параметр безопасности.

Результат: матрица $\langle Z\rangle_i^A$ такая, что $Z = \sum_i \langle Z\rangle_i^A$ и $Z = X \cdot Y$.

Фаза предварительных вычислений:

1. S_i случайно выбирают 2 матрицы $\langle A\rangle_i^A$ и $\langle B\rangle_i^A$, состоящие из целых чисел в интервале $[0;2^\ell-1]$. Размерности указанных матриц совпадают с размерностями $\langle X\rangle_i^A$ и $\langle Y\rangle_i^A$ соответственно.
2. S_0 и S_1 выполняют коррелированный протокол «забывчивой передачи», в котором S_0 – отправитель, а S_1 – получатель, а в результате серверы получают разделенную по АСРС матрицу $\langle U\rangle_i^A$. Элемент матрицы $(\langle U\rangle_i^A)_{j,k}$, $j \in \{0,r_0-1\}$, $k \in \{0,r_2-1\}$ рассчитывается следующим образом:

$$(\langle U\rangle_i^A)_{j,k} = \sum_{l=0}^{r1-1} \text{C–OT}_\ell^\ell\left((\langle U\rangle_0^A)_{j,l}, (\langle B\rangle_1^A)_{l,k}, q, \kappa\right) = \sum_{l=0}^{r1-1}\sum_{i=0}^{l-1} s_i \bmod 2^\ell,\ s_i \in_R \mathbb{Z}_{2\ell},$$

$$(\langle U\rangle_1^A)_{j,k} = \sum_{l=0}^{r1-1} \text{C–OT}_\ell^\ell\left((\langle U\rangle_0^A)_{j,l}, (\langle B\rangle_1^A)_{l,k}, q, \kappa\right) = \sum_{l=0}^{r1-1}\sum_{i=0}^{l-1}\left((\langle B\rangle_1^A)_{l,k}[i] \cdot (\langle A\rangle_0^A)_{j,l} \cdot 2^i - s_i\right) \bmod 2^\ell. \quad (12)$$

3. S_0 и S_1 выполняют коррелированный протокол «забывчивой передачи», в котором S_1 – отправитель, а S_0 – получатель, а в результате серверы получают разделенную по АСРС матрицу $\langle V\rangle_i^A$. Элемент матрицы $(\langle V\rangle_i^A)_{j,k}$, $j \in \{0,r_0-1\}$, $k \in \{0,r_2-1\}$ рассчитывается следующим образом:

$$(\langle V\rangle_0^A)_{j,k} = \sum_{l=0}^{r1-1} \text{C–OT}_\ell^\ell\left((\langle A\rangle_1^A)_{j,l}, (\langle B\rangle_0^A)_{l,k}, q, \kappa\right) = \sum_{l=0}^{r1-1}\sum_{i=0}^{l-1}\left((\langle B\rangle_0^A)_{l,k}[i] \cdot (\langle A\rangle_1^A)_{j,l} \cdot 2^i - s_i\right) \bmod 2^\ell,$$

$$(\langle V\rangle_0^A)_{j,k} = \sum_{l=0}^{r1-1} \text{C–OT}_\ell^\ell\left((\langle A\rangle_1^A)_{j,l}, (\langle B\rangle_0^A)_{l,k}, q, \kappa\right) = \sum_{l=0}^{r1-1}\sum_{i=0}^{l-1} s_i \bmod 2^\ell,\ s_i \in_R \mathbb{Z}_{2\ell}. \quad (13)$$

4. Расчет матрицы $\langle C\rangle_i^A$ производится серверами следующим образом:

$$\langle C\rangle_i^A = \langle A\rangle_i^A \cdot \langle B\rangle_i^A + \langle U\rangle_i^A + \langle V\rangle_i^A. \quad (14)$$

Протокол:

1. S_i вычисляет разности $\langle X\rangle_i^A - \langle A\rangle_i^A$, $\langle Y\rangle_i^A - \langle B\rangle_i^A$ и отправляет результат серверу S_{1-i}.
2. S_i восстанавливает значения разностей:

$$X - A = (\langle X\rangle_i^A - \langle A\rangle_i^A) + (\langle X\rangle_{1-i}^A - \langle A\rangle_{1-i}^A),$$
$$Y - B = (\langle Y\rangle_i^A - \langle B\rangle_i^A) + (\langle Y\rangle_{1-i}^A - \langle B\rangle_{1-i}^A). \quad (15)$$

3. S_i вычисляет результат:

$$\langle Z\rangle_i^A = -i\cdot(X-A)(Y-B) + \langle A\rangle_i^A \cdot \cdot (Y-B) + \langle B\rangle_i^A \cdot (X-A) + \langle C\rangle_i^A. \quad (16)$$

Покажем безопасность этого протокола. Для этого приведем описание симулятора $S_{\text{MatrixMult}}$:

1. Симулятор $S_{\text{MatrixMult}}$ случайно выбирает $\langle A\rangle_t^A$, $\langle A\rangle_{1-t}^A$ и $\langle B\rangle_t^A$, $\langle B\rangle_{1-t}^A$, где n – индекс скомпрометированного участника.
2. Дважды используя симулятор $S_{\text{C-OT}}$ «коррелированного» протокола передачи с забыванием, $S_{\text{MatrixMult}}$ получает ансамбль величин, статистически неразличимых от получаемых в результате шага 2 и 3 фазы предварительных вычислений протокола.
3. Симулятор $S_{\text{MatrixMult}}$ рассчитывает $\langle C\rangle_t^A$ и $\langle C\rangle_{1-t}^A$ в соответствии с выражением (14).
4. Симулятор $S_{\text{MatrixMult}}$ рассчитывает $\langle X\rangle_t^A - \langle A\rangle_t^A$, $\langle Y\rangle_t^A - \langle B\rangle_t^A$ и $\langle X\rangle_{1-t}^A - \langle A\rangle_{1-t}^A$, $\langle Y\rangle_{1-t}^A - \langle B\rangle_{1-t}^A$ и восстанавливает указанные разности.
5. Симулятор $S_{\text{MatrixMult}}$ вычисляет результат в соответствии с выражение (16).

Конфиденциальное вычисление значения функции ReLU – протокол, позволяющий двум участникам получить доли значения функции ReLU, широко используемой в качестве функции активации нейронов в ГНС, подав на вход доли некоторого значения аргумента этой функции.

Входные данные: $\langle a\rangle_i^A$ – входное число, разделенное по АСРС, q – большое простое число, ℓ – размерность чисел в битах.

Результат: серверы S_i рассчитывают разделенное по АСРС число $\langle s\rangle_i^A$, где

$$s = \begin{cases} x, x \geq 0, \\ 0, x < 0. \end{cases}.$$

Протокол:

1. Серверы S_i применяют протокол конфиденциальной проверки числа на положительность:

$$\langle s'\rangle_i^A = \text{GTZ}\left(\langle a\rangle_i^A\right). \quad (17)$$

2. Серверы S_i вычисляют результат при помощи протокола конфиденциального умножения чисел:

$$\langle s\rangle_i^A = \langle a\rangle_i^A \cdot \langle s'\rangle_i^A. \quad (18)$$

Покажем безопасность этого протокола. Для этого приведем описание симулятора S_{ReLU}:

1. Для моделирования п. 1 протокола S_{ReLU} применяет S_{GTZ}, который описан в [9].
2. Затем S_{ReLU} применяет S_{Mult}, который описан в [10], для моделирования п. 2 протокола.

Конфиденциальное вычисление значения функции активации LeakyReLU – протокол, функция которого полностью аналогичная предыдущему, за исключением того, что вычисляется значение функции LeakyReLU.

Входные данные: $\langle a\rangle_i^A$ – входное число, разделенное по АСРС, α – отрицательный уклон (англ. negative slope), q – большое простое число, ℓ – размерность чисел в битах.

Результат: серверы S_i рассчитывают разделенное по АСРС число $\langle s\rangle_i^A$, где

$$s = \begin{cases} x, x \geq 0, \\ \alpha x, x < 0. \end{cases}.$$

Протокол:

1. Серверы S_i конфиденциально вычисляют значение функции ReLU:

$$\langle s\rangle_i^A = \text{ReLU}\left(\langle a\rangle_i^A\right). \quad (19)$$

2. Серверы S_i локально преобразуют α к виду числа с фиксированной точкой и длиной дробной части f, представленному в поле $\mathbb{Z}_q$:

$$\alpha' = [2^f \cdot \alpha] \bmod q. \quad (20)$$

3. Серверы S_i вычисляют результат посредством протокола конфиденциального усечения числа:

$$\langle s'\rangle_i^A = \text{Trunc}\left(\langle s\rangle_i^A \cdot (2^f - \alpha') + \alpha' \cdot \langle s\rangle_i^A, \ell, f\right). \quad (21)$$

Покажем безопасность этого протокола. Для этого приведем описание симулятора $S_{\text{LeakyReLU}}$:

1. $S_{\text{LeakyReLU}}$ применяет описанный выше S_{ReLU} для моделирования 1 шага протокола.
2. Симулятор $S_{\text{LeakyReLU}}$ преобразует α к α' в соответствии с выражением, указанным в п. 2 протокола.
3. Последним $S_{\text{LeakyReLU}}$ применяет S_{Trunc}, который описан в [9], для моделирования п. 3 протокола.

Другие протоколы. Кроме перечисленных выше, в системе «КонфГраф» используются в качестве примитивов следующие готовые протоколы БМВ:

1. Конфиденциальное согласование случайного бита [9]: входные данные: q – большое простое число, результат: серверы S_i, $i \in \{0,1\}$ согласуют случайный бит $\langle d\rangle_i^A$, разделенный по АСРС, т.е. $(\langle d\rangle_0^A + \langle d\rangle_1^A) \bmod q \in \{0,1\}$.
2. Конфиденциальное согласование случайных величин [9]: входные данные: q – большое простое число, κ – статистический параметр безопасности, α – количество выходных случайных бит, k – разрядность выходного числа, результат: серверы S_i, $i \in \{0,1\}$ согласуют α случайных бит $\langle r_0\rangle_i^A,\ldots,\langle r_{\alpha-1}\rangle_i^A$, разделенных по АСРС, а также α-битное число $\langle r\rangle_i^A = \sum_{j=0}^{\alpha-1} 2^j \cdot \langle r_j\rangle_i^A$ и $(k+\kappa-\alpha)$-битное $\langle r'\rangle_i^A$.
3. Конфиденциальное префиксное умножение чисел [9]: входные данные: $(\langle a\rangle_i^A)_0,\ldots,(\langle a\rangle_i^A)_{l-1}$ – массив входных ненулевых чисел, разделенных по АСРС, q – большое простое число, ℓ – размерность чисел в битах, результат: серверы S_i, $i \in \{0,1\}$ рассчитывают разделенный по АСРС массив значений $(\langle p\rangle_i^A)_j = \prod_{k=0}^{j} (\langle a\rangle_i^A)_k$, $j \in \{0,\ell-1\}$.

4. Конфиденциальное вычисление остатка от деления на 2 [9]: входные данные: $\langle a\rangle_i^A$ – входное число, разделенное по АСРС, q – большое простое число, ℓ – размерность чисел в битах, результат: серверы S_i, $i \in \{0,1\}$ рассчитывают разделенное по АСРС число $\langle a_0\rangle_i^A = \langle a \bmod 2\rangle_i^A$.
5. Протокол конфиденциального сравнения с известным значением [11]: входные данные: a – число, известное обоим серверам, $(\langle b\rangle_i^A)_0,\ldots,(\langle b\rangle_i^A)_{l-1}$ – входное число, представленное в форме l-битной последовательности, каждый бит которой разделён с использованием АСРС, q – большое простое число, ℓ – размерность чисел в битах, результат: серверы S_i, $i \in \{0,1\}$ вычисляют разделенный по АСРС бит $\langle u\rangle_i^A$, где $u = (a<b)?1:0$.
6. Конфиденциальное вычисление остатка от деления на 2^m [11]: входные данные: $\langle a\rangle_i^A$ – входное число, разделенное по АСРС, m – общеизвестное целое число, $m \in \{1,\ell-1\}$, q – большое простое число, ℓ – размерность чисел в битах, результат: серверы S_i, $i \in \{0,1\}$ вычисляют разделенное по АСРС число $\langle a'\rangle_i^A = \langle a \bmod 2^m\rangle_i^A$.
7. Конфиденциальное усечение числа [9]: входные данные: $\langle a\rangle_i^A$ – входное число, разделенное по АСРС, m – общеизвестное целое число, $m \in \{1,\ell-1\}$, q – большое простое число, ℓ – размерность чисел в битах, результат: серверы S_i, $i \in \{0,1\}$ вычисляют разделенное по АСРС число $\langle d\rangle_i^A = \langle[\frac{a}{2^m}]\rangle_i^A$.
8. Конфиденциальное вероятностное усечение числа [9]: входные данные: $\langle a\rangle_i^A$ – входное число, разделенное по АСРС, m – общеизвестное целое число, $m \in \{1,\ell-1\}$, q – большое простое число, ℓ – размерность чисел в битах, результат: серверы S_i, $i \in \{0,1\}$ вычисляют разделенное по АСРС число $\langle d\rangle_i^A = \langle[\frac{a}{2^m}] + u\rangle_i^A$, где $u \in \{0,1\}$.
9. Протокол передачи с забыванием (oblivious transfer) [12]: входные данные: отправитель S хранит 2 сообщения (m_0,m_1), получатель R – бит выбора $\sigma \in \{0,1\}$, g – генератор циклической группы $\mathbb{Z}_q$, q – большое простое число, результат: R определяет значение m_σ, причем R не получает никакой информации о значении $m_{1-\sigma}$, а S – о значении бита выбора σ.
10. Конфиденциальное умножение чисел [10]: входные данные: разделенные по АСРС числа $\langle x\rangle_i^A$, $\langle y\rangle_i^A$, $i \in \{0,1\}$, ℓ – размерность чисел в битах, q – большое простое число, κ – статистический параметр безопасности, результат: число $\langle z\rangle_i^A$, $i \in \{0,1\}$, причем $z = \sum_i \langle z\rangle_i^A$ и $z = x \cdot y$.
11. Конфиденциальное умножение чисел с фиксированной точкой [13]: входные данные: разделенные по АСРС числа $\langle x\rangle_i^A,\langle y\rangle_i^A$, $i \in \{0,1\}$, f – длина дробной части в битах, ℓ – полная длина чисел в битах, q – большое простое число, κ – статистический параметр безопасности, результат: число $\langle z\rangle_i^A$, $i \in \{0,1\}$, причем $z = \sum_i \langle z\rangle_i^A$ и $z = x \cdot y$.
12. $\mathrm{AllOr}\left((\langle d\rangle_i^A)_{k-1},\ldots,(\langle d\rangle_i^A)_0\right)$ [14]: входные данные: серверы S_i, $i \in \{0,1\}$ хранят массив $(\langle d\rangle_i^A)_0,\ldots,(\langle d\rangle_i^A)_{k-1}$ длиной k, разделенный по АСРС, причем $\left((\langle d\rangle_0^A)_j + (\langle d\rangle_1^A)_j\right) \bmod q \in \{0,1\}$, q – большое простое число, результат: S_i, $i \in \{0,1\}$ согласуют разделенный по АСРС массив $(\langle b\rangle_i^A)_0,\ldots,(\langle b\rangle_i^A)_{2^k-1}$ длиной 2^k и состоящий из результата логического «ИЛИ» от всех возможных комбинаций входных бит, разделенных по АСРС.
13. Конфиденциальный доступ к элементам массива [14]: входные данные: массив a, состоящий из m элементов и разделенный по АСРС между S_i, $i \in \{0,1\}$, т.е. $\left[(\langle a\rangle_i^A)_0,(\langle a\rangle_i^A)_1,\ldots,(\langle a\rangle_i^A)_{m-1}\right]$, индекс j, также разделенный по АСРС, – $\langle j\rangle_i^A$, q – большое простое число, результат: элемент b, разделенный по АСРС между S_i, $i \in \{0,1\}$, причем $b = a_j$.
14. Конфиденциальная запись элемента массива [14]: входные данные: массив a, состоящий из m элементов и разделенный по АСРС между S_i, $i \in \{0,1\}$, т.е. $\left[(\langle a\rangle_i^A)_0,(\langle a\rangle_i^A)_1,\ldots,(\langle a\rangle_i^A)_{m-1}\right]$, $i \in \{0,1\}$, индекс j, также разделенный по АСРС, – $\langle j\rangle_i^A$, $\langle w\rangle_i^A$ – записываемое значение, q – большое простое число, результат: массив d, состоящий из m элементов и разделенный по АСРС между S_i, $i \in \{0,1\}$, причем
$$d_k = \begin{cases} a_k, k \neq j, \\ w, k = j. \end{cases}$$
15. Конфиденциальная проверка числа на отрицательность [9]: входные данные: $\langle a\rangle_i^A$ – входное число, разделенное по АСРС, q – большое простое число, ℓ – размерность чисел в битах, результат: серверы S_i, $i \in \{0,1\}$ рассчитывают разделенное по АСРС число $\langle s'\rangle_i^A$, где $s' = a < 0? 1:0$.
16. Конфиденциальная проверка числа на положительность [9]: входные данные: $\langle a\rangle_i^A$ – входное число, разделенное по АСРС, q – большое простое число, ℓ – размерность чисел в битах, результат: серверы S_i, $i \in \{0,1\}$ рассчитывают разделенное по АСРС число $\langle s'\rangle_i^A$, где $s' = a > 0? 1:0$.
17. Конфиденциальное вычисление значения функции Softmax [15]: входные данные: массив x, состоящий из m элементов и разделенный по АСРС между участниками протокола $\left[(\langle x\rangle_i^A)_0,(\langle x\rangle_i^A)_1,\ldots,(\langle x\rangle_i^A)_{m-1}\right]$, $i \in \{0,1\}$, $r = 2^{l-f}$ – количество итераций протокола, f – длина дробной части в битах, ℓ – размерность чисел в битах, результат: массив g, состоящий из m элементов и разделенный по АСРС между участниками протокола $\left[(\langle g\rangle_i^A)_0,(\langle g\rangle_i^A)_1,\ldots,(\langle g\rangle_i^A)_{m-1}\right]$, где
$$g_j \approx \frac{e^{x_j}}{\sum_{k=0}^{m-1} e^{x_k}}, j \in \{0,m-1\}.$$

Безопасность перечисленных протоколов в рассматриваемой модели нарушителя доказана в соответствующих источниках, поэтому далее они используются в качестве готовых структурных элементов с доказанными свойствами безопасности.

6. Анализ безопасности протоколов системы «КонфГраф»

Для доказательства безопасности протоколов системы КМО «КонфГраф» в целом воспользуемся методологией универсальной компонуемости: окружение не отличит реальный мир от идеального, если протокол безопасен. При условии безопасности протоколов, лежащих в основе системы, доказательство ее безопасности оказывается достаточно простым. Для демонстрации безопасности протоколов системы «КонфГраф» опишем алгоритм работы симулятора в модели получестного противника. Пусть $n \in \{0,1\}$ – номер скомпрометированного нарушителем сервера. Тогда:

1. Симулятор $S_{\text{КонфГраф}}$ локально вычисляет $\left(\langle W\rangle_n^A\right)^T$.
2. Симулятор $S_{\text{КонфГраф}}$ пользуется симулятором $S_{\text{MatrixMult}}$ для моделирования протокола конфиденциального умножения матриц $\langle X\rangle_n^A \cdot \left(\langle W\rangle_n^A\right)^T$.
3. Симулятор $S_{\text{КонфГраф}}$ использует $S_{\text{ArrayAccess}}$ для моделирования протокола конфиденциального доступа к элементам массива для составления матриц

$$\left(\langle X\rangle_n^A \cdot \left(\langle W\rangle_n^A\right)^T\right)\left[\langle C\rangle_n^A[0]\right]$$
$$\text{и } \left(\langle X\rangle_n^A \cdot \left(\langle W\rangle_n^A\right)^T\right)\left[\langle C\rangle_n^A[1]\right].$$

4. Симулятор $S_{\text{КонфГраф}}$ производит построчную конкатенацию матриц $\left(\langle X\rangle_n^A \cdot \left(\langle W\rangle_n^A\right)^T\right)\left[\langle C\rangle_n^A[0]\right]$ и $\left(\langle X\rangle_n^A \cdot \left(\langle W\rangle_n^A\right)^T\right)\left[\langle C\rangle_n^A[1]\right]$, а затем транспонирование результата

$$\left(\left(\langle X\rangle_n^A \cdot \left(\langle W\rangle_n^A\right)^T\right)\left[\langle C\rangle_n^A[0]\right] \parallel \right.$$
$$\left. \parallel \left(\langle X\rangle_n^A \cdot \left(\langle W\rangle_n^A\right)^T\right)\left[\langle C\rangle_n^A[1]\right]\right)^T.$$

5. Симулятор $S_{\text{КонфГраф}}$ использует $S_{\text{MatrixMult}}$ для моделирования протокола конфиденциального умножения матриц для вычисления:

$$\langle W_{att}\rangle_n^A \cdot \left(\left(\langle X\rangle_n^A \cdot \left(\langle W\rangle_n^A\right)^T\right)\left[\langle C\rangle_n^A[0]\right] \parallel \right.$$
$$\left. \parallel \left(\langle X\rangle_n^A \cdot \left(\langle W\rangle_n^A\right)^T\right)\left[\langle C\rangle_n^A[1]\right]\right)^T. \quad (22)$$

6. Симулятор $S_{\text{КонфГраф}}$ использует $S_{\text{LeakyReLU}}$ для моделирования протокола конфиденциального вычисления значения функции LeakyReLU:

$$\text{LeakyReLU}\left(\left(\langle W_{att}\rangle_n^A \cdot \left(\left(\langle X\rangle_n^A \cdot \left(\langle W\rangle_n^A\right)^T\right)\left[\langle C\rangle_n^A[0]\right] \parallel \right.\right.\right.$$
$$\left.\left.\left. \parallel \left(\langle X\rangle_n^A \cdot \left(\langle W\rangle_n^A\right)^T\right)\left[\langle C\rangle_n^A[1]\right]\right)^T\right)_j\right), j \in \{0,R-1\}. \quad (23)$$

7. Симулятор $S_{\text{КонфГраф}}$ создает нулевую матрицу $\langle E\rangle_n^A$ размерностью, совпадающей с $\langle A\rangle_n^A$.
8. Симулятор $S_{\text{КонфГраф}}$ использует $S_{\text{ArrayWrite}}$ для моделирования протокола конфиденциальной записи элементов массива для заполнения матрицы $\langle E\rangle_n^A$ значениями, полученными от симулятора $S_{\text{LeakyReLU}}$ (см. п. 6), в соответствии с координатами в матрице C.
9. Симулятор $S_{\text{КонфГраф}}$ использует S_{softmax} для моделирования протокола конфиденциального вычисления значения функции Softmax:

$$\langle W_\alpha\rangle_n^A = \text{softmax}\left(\left(\langle E\rangle_n^A\right)_j\right), j \in \{0,V-1\}. \quad (24)$$

10. Симулятор $S_{\text{КонфГраф}}$ трижды пользуется симулятором $S_{\text{MatrixMult}}$ для моделирования протокола конфиденциального умножения матриц

$$\langle H\rangle_n^A = \left(\langle A\rangle_n^A\right)^T \cdot \langle W_\alpha\rangle_n^A \cdot \langle X\rangle_n^A \cdot \left(\langle W\rangle_n^A\right)^T. \quad (25)$$

В итоге, результатом каждого из шагов работы симулятора $S_{\text{КонфГраф}}$ будет ансамбль случайных величин, которые статистически неразличимы от величин, получаемых в реальном мире, что говорит о том, что окружение не сможет «отличить» реальный мир от идеального, следовательно, систему КМО «КонфГраф» можно считать безопасной в рассматриваемой модели угроз.

7. Заключение

В работе предложен комплекс криптографических протоколов для реализации системы конфиденциального машинного обучения на основе графовых нейронных сетей с механизмом внимания, названной нами «КонфГраф», и доказана безопасность как отдельных протоколов, так и системы в целом.

Система «КонфГраф» позволяет осуществлять конфиденциальное применение графовых нейронных сетей с механизмом внимания при компрометации одного из двух провайдеров облачных вычислений. Система основана на использовании арифметической схемы разделения секрета, однако в ее составе нашли применение и другие базовые для БМВ криптографические примитивы, например, протокол передачи с забыванием. Благодаря использованию таких примитивов стала возможна разработка протоколов для конфиденциального вычисления более сложных математических функций, например, LeakuReLU и Softmax, являющихся базой современных моделей искусственных нейронных сетей. Собрав все протоколы в единую систему и согласовав их работу, удалось создать систему для конфиденциального вычисления функции, задаваемой уравнением (4), и доказать ее безопасность в рассматриваемой модели угроз.

Литература

1. *Younes L. Introduction to Machine Learning. arXiv, 2024. – 649 p. DOI: https://doi.org/10.48550/arXiv.2409.02668.*
2. *Brody S., Alon U., Yahav E. How Attentive are Graph Attention Networks? arXiv, 2022. – 26 p. DOI: https://doi.org/10.48550/arXiv.2105.14491.*
3. *Liao Y. Zhang X. Ferrie C. Graph Neural Networks on Quantum Computers. arXiv, 2024. – 50 p. DOI: https://doi.org/10.48550/arXiv.2405.17060.*
4. *Xu R., Baracaldo N., Joshi J. Privacy-Preserving Machine Learning: Methods, Challenges and Directions. aXiv, 2021. – 40 p. DOI: http://dx.doi.org/10.48550/arXiv.2108.04417*
5. *Запечников С. В. Модели и алгоритмы конфиденциального машинного обучения // Безопасность информационных технологий. Т. 27. № 1. 2020. С. 51–67. DOI: https://doi.org/10.26583/bit.2020.1.05.*
6. *Запечников С. В. Конфиденциальное машинное обучение на основе четырехсторонних протоколов безопасных вычислений // Безопасность информационных технологий. Т. 29. № 2. 2022. С. 46–56. DOI: http://dx.doi.org/10.26583/bit.2022.2.04.*
7. *Mishra P., Lehmkuhl R., Srinivasan A., Zheng W., Popa R. A. Delphi: A cryptographic inference service for neural networks. Proc. of USENIX Security 2020 (USENIX Security Symposium). URL: https://eprint.iacr.org/2020/050.pdf.*
8. *Liu X., Wu B., Yuan X., Yi X. Leia: A Lightweight Cryptographic Neural Network Inference System at the Edge. IEEE Transactions on Information Forensics and Security, vol. 17, 2022, pp. 237–252. DOI: https://doi.org/10.1109/TIFS.2021.3138611.*
9. *Catrina O., de Hoogh S. Improved Primitives for Secure Multiparty Integer Computation. Security and Cryptography for Networks. Lecture Notes in Computer Science, vol 6280, Springer, 2010, pp 182–199. DOI: https://doi.org/10.1007/978-3-642-15317-4_13.*
10. *Patra A., Schneider T., Suresh A., Yalame H. ABY2.0: Improved Mixed-Protocol Secure Two-Party Computation. Cryptology ePrint Archive, 2020. – 29 p. DOI: https://eprint.iacr.org/2020/1225.*
11. *Catrina O. Round-Efficient Protocols for Secure Multiparty Fixed-Point Arithmetic. Proc. of 12th IEEE International Conference on Communications, 2018, pp 431–436. DOI: https://doi.org/10.1109/ICComm.2018.8484794.*
12. *Yadav V., Andola N., Verma S, Venkatesan S. A Survey of Oblivious Transfer Protocol. ACM Comput. Surv., 2022. – 37 p. DOI: https://doi.org/10.1145/3503045.*
13. *Catrina O., Saxena A. Secure Computation With Fixed-Point Numbers. Lecture Notes in Computer Science, vol. 6052, Springer, 2010, pp 35–50. DOI: https://doi.org/10.1007/978-3-642-14577-3_6.*
14. *Blanton M., Kang A., Yuan C. Improved Building Blocks for Secure Multi-Party Computation based on Secret Sharing with Honest Majority. Cryptology ePrint Archive, 2019. – 26 p. URL: https://eprint.iacr.org/2019/718.*
15. *Zheng Y., Zhang Q., Chow S., Peng Y., Tan S., Li L., Yin S. Secure Softmax/Sigmoid for Machine-Learning Computation. Proc. of the 39th Annual Computer Security Applications Conference, 2023, pp 463–476. DOI: https://doi.org/10.1145/3627106.3627175.*

PRIVACY-PRESERVING INFERENCE OF PRE-TRAINED GRAPH NEURAL NETWORKS WITH AN ATTENTION MECHANISM

Shevchenko V. A.[3], Zapechnikov S. V.[4]

Abstract. *The article proposes a set of cryptographic protocols for privacy-preserving machine learning (PPML) system based on graph neural networks with an attention mechanism. The classification of artificial neural networks underlying deep learning is given. The main tasks of ensuring privacy that arise during the training and inference of machine learning models based on artificial neural networks are highlighted. The main cryptographic primitives underlying secure multi-party computations are described, namely secret sharing schemes, an oblivious transfer protocol. It is provided a brief description of the methodology for proving the security of cryptographic protocols, including protocols for secure multi-party computations, known as universal composability (UC-security). The main and auxiliary protocols underlying the PPML system are described and analyzed: the correlated oblivious transfer, as well as protocols for private matrix multiplication, private ReLU and LeakyReLU functions computation, and the proof of their security is provided. The rest of the protocols used in the PPML system are listed in the article with a brief description of their input and output data. The security of the PPML system as a whole is proved based on the universal composability paradigm.*

Keywords: *cryptography, information security, confidential machine learning, secure multi-party computing, graph neural networks with an attention mechanism, secret sharing schemes, transmission protocol with forgetting.*

3 Vyacheslav A. Shevchenko, Applicant, National Research Nuclear University MEPhI, Moscow, Russia. E-mail sheff-slava@mail.ru

4 Sergey V. Zapechnikov, Doctor of Technical Sciences, Associate Professor, Professor, National Research Nuclear University MEPhI, Moscow, Russia. E-mail: svzapechnikov@mephi.ru

References

1. *Younes L. Introduction to Machine Learning. arXiv, 2024. – 649 p. DOI: https://doi.org/10.48550/arXiv.2409.02668.*
2. *Brody S., Alon U., Yahav E. How Attentive are Graph Attention Networks? arXiv, 2022. – 26 p. DOI: https://doi.org/10.48550/arXiv.2105.14491.*
3. *Liao Y. Zhang X. Ferrie C. Graph Neural Networks on Quantum Computers. arXiv, 2024. – 50 p. DOI: https://doi.org/10.48550/arXiv.2405.17060.*
4. *Xu R., Baracaldo N., Joshi J. Privacy-Preserving Machine Learning: Methods, Challenges and Directions. aXiv, 2021. – 40 p. DOI: http://dx.doi.org/10.48550/arXiv.2108.04417*
5. *Zapechnikov S. V. Modeli i algoritmy konfidencial'nogo mashinnogo obuchenija // Bezopasnost' informacionnyh tehnologij. T. 27. № 1. 2020. S. 51–67. DOI: https://doi.org/10.26583/bit.2020.1.05.*
6. *Zapechnikov S. V. Konfidencial'noe mashinnoe obuchenie na osnove chetyrehstoronnih protokolov bezopasnyh vychislenij // Bezopasnost' informacionnyh tehnologij. T. 29. № 2. 2022. S. 46–56. DOI: http://dx.doi.org/10.26583/bit.2022.2.04.*
7. *Mishra P., Lehmkuhl R., Srinivasan A., Zheng W., Popa R. A. Delphi: A cryptographic inference service for neural networks. Proc. of USENIX Security 2020 (USENIX Security Symposium). URL: https://eprint.iacr.org/2020/050.pdf.*
8. *Liu X., Wu B., Yuan X., Yi X. Leia: A Lightweight Cryptographic Neural Network Inference System at the Edge. IEEE Transactions on Information Forensics and Security, vol. 17, 2022, pp. 237-252. DOI: https://doi.org/10.1109/TIFS.2021.3138611.*
9. *Catrina O., de Hoogh S. Improved Primitives for Secure Multiparty Integer Computation. Security and Cryptography for Networks. Lecture Notes in Computer Science, vol 6280, Springer, 2010, pp 182–199. DOI: https://doi.org/10.1007/978-3-642-15317-4_13.*
10. *Patra A., Schneider T., Suresh A., Yalame H. ABY2.0: Improved Mixed-Protocol Secure Two-Party Computation. Cryptology ePrint Archive, 2020. – 29 p. DOI: https://eprint.iacr.org/2020/1225.*
11. *Catrina O. Round-Efficient Protocols for Secure Multiparty Fixed-Point Arithmetic. Proc. of 12th IEEE International Conference on Communications, 2018, pp 431-436. DOI: https://doi.org/10.1109/ICComm.2018.8484794.*
12. *Yadav V., Andola N., Verma S, Venkatesan S. A Survey of Oblivious Transfer Protocol. ACM Comput. Surv., 2022. – 37 p. DOI: https://doi.org/10.1145/3503045.*
13. *Catrina O., Saxena A. Secure Computation With Fixed-Point Numbers. Lecture Notes in Computer Science, vol. 6052, Springer, 2010, pp 35–50. DOI: https://doi.org/10.1007/978-3-642-14577-3_6.*
14. *Blanton M., Kang A., Yuan C. Improved Building Blocks for Secure Multi-Party Computation based on Secret Sharing with Honest Majority. Cryptology ePrint Archive, 2019. – 26 p. URL: https://eprint.iacr.org/2019/718.*
15. *Zheng Y., Zhang Q., Chow S., Peng Y., Tan S., Li L., Yin S. Secure Softmax/Sigmoid for Machine-Learning Computation. Proc. of the 39th Annual Computer Security Applications Conference, 2023, pp 463-476. DOI: https://doi.org/10.1145/3627106.3627175.*

АЛГОРИТМ СТОХАСТИЧЕСКОГО ПРЕОБРАЗОВАНИЯ 3DGOST

Иванов М. А.[1], Комаров Т. И.[2], Кондахчан М. А.[3], Стариковский А. В.[4]

DOI: 10.21681/2311-3456-2024-5-28-33

Аннотация. *Перспективным направлением при решении задач защиты информации является использование стохастических методов, основным результатом применения которых является внесение непредсказуемости в работу компьютерной системы и средств ее защиты.*

Целью данной работы *является обоснование возможности эффективного использования 64-разрядных алгоритмов стохастического преобразования данных, хорошо зарекомендовавших себя в прошлом.*

Метод достижения цели *заключается в использовании архитектуры Куб.*

Полученные результаты: *представлен 3D алгоритм нелинейного преобразования данных, ориентированный на реализацию с использованием гетерогенных суперкомпьютерных технологий. Тестирование алгоритма в режиме генерации псевдослучайных чисел показало его статистическую безопасность.*

Ключевые слова: *генератор псевдослучайных чисел, стохастическое преобразование, непредсказуемость, стохастические методы защиты информации.*

Введение

Важнейшей характеристикой любой компьютерной системы (КС), независимо от ее сложности и назначения, является безопасность обрабатываемой в ней информации. Перспективным направлением при решении задач защиты информации (ЗИ) является использование стохастических методов, основанных на использовании генераторов псевдослучайных чисел (ГПСЧ). Главным результатом применения стохастических методов обработки данных является внесение непредсказуемости в работу КС и средств ее защиты [1, 2].

3D алгоритм стохастического преобразования

Тенденцией последних лет является массовое появление 2D и 3D алгоритмов стохастического преобразования, в частности криптоалгоритмов, ориентированных на реализацию с использованием суперкомпьютерных технологий [2–17]. В [17] предлагается новый 3D алгоритм стохастического преобразования, названный 3DGOST, который может использоваться при построении нелинейной функции ГПСЧ (функции выхода в случае использования режима CTR (Counter Mode) или функции обратной связи в случае использования режима OFB (Output Feedback)).

В данной работе предлагается Light-Weight версия алгоритма 3DGOST, при создании которой главной целью являлось построение нелинейного многораундового преобразования, имеющего повышенное быстродействие за счет упрощения процедуры формирования раундовых ключей и подключей.

В совокупности признаков предлагаемого алгоритма используются следующие термины:

Стохастическое преобразование (Stochastic Transformation) – непредсказуемое преобразование данных; примером стохастического преобразования может являться криптографическое преобразование;

Генератор псевдослучайных чисел (Pseudo-Random Number Generator) – генератор последовательности чисел, статистически не отличимой от последовательности случайных чисел с равномерным законом распределения; наиболее жесткие требования предъявляются к ГПСЧ, ориентированным на решение задач ЗИ;

Ключ (Key) – секретный параметр стохастического преобразования, представляет собой двоичную информацию, известную только законному пользователю;

Подключ (SubKey) – часть ключа;

Раунд (Round) – последовательность шагов, образующих одну итерацию итеративного (многораундового) преобразования;

Раундовый ключ (RoundKey) – ключевая информация, использующаяся при выполнении одного раунда преобразования, существует два способа формирования раундовых ключей: раундовый ключ может являться частью секретного ключа (пример –

1 Иванов Михаил Александрович, доктор технических наук, профессор, главный научный сотрудник ИИКС НИЯУ МИФИ, Москва, Россия. E-mail: maivanov@mephi.ru
2 Комаров Тимофей Ильич, доцент кафедры компьютерных систем и технологий (№12) НИЯУ МИФИ, Москва, Россия. E-mail: tikomarov@mephi.ru
3 Кондахчан Микаэл Арсенович, студент кафедры компьютерных систем и технологий (№12) НИЯУ МИФИ, Москва, Россия. E-mail: mikarkon@gmail.com
4 Стариковский Андрей Викторович, Руководитель проектов Государственного университета управления, Москва, Россия. E-mail: av_starikovskiy@guu.ru

ГОСТ 28147-89), последовательность раундовых ключей может получаться в результате работы процедуры разворачивания исходного ключа (KeyExpansion) (пример – американский стандарт AES);

Раундовый подключ (SubRoundKey) – часть раундового ключа;

Двоичный вектор – некоторая последовательность нулевых и единичных бит, например, (01101010); двоичный вектор разрядности n может быть интерпретирован как элемент конечного поля $GF(2^n)$;

Замена (Substitution) – операция, выполняемая над двоичным вектором $i \in GF(2^n)$, при этом результат операции равен содержимому ячейки с индексом i таблицы замен размерности $n \times 2^n$;

Перемешивание (Mix) – операция, выполняемая над двоичным вектором разрядности m, результат разрядности m которой зависит от всех входных бит и от их взаимного расположения.

Базовое стохастическое преобразование – n раундов произвольного блочного преобразования, работающего с 64-разрядными блоками данных (примеры таких преобразований – ГОСТ 26147-89, Магма (ГОСТ Р 34.12-2015)). Величина n выбирается таким образом, чтобы соответствующее число раундов преобразования обеспечивали полное рассеивание и перемешивание информации (например, для ГОСТ 26147-89 $n \geq 6$).

Суть предлагаемого алгоритма проиллюстрирована рис. 1–4. На рис. 1 показаны блок данных (состояние S или ключ K), принцип разделения блока данных на слои параллельно плоскостям $y0z$, $x0z$, $x0y$, отдельные слои L_{xi}, L_{yi}, L_{zi} блока данных; $i = 0, 1, ..., 7$. На рис. 2 приведена последовательность выполнения преобразования, показаны входной преобразуемый блок данных, выходной преобразованный блок данных; раундовые ключи $KL_{x0}, KL_{x1}, ..., KL_{x7}$ первого раунда; раундовые ключи $KL_{y0}, KL_{y1}, ..., KL_{y7}$ второго раунда; раундовые ключи $KL_{z0}, KL_{z1}, ..., KL_{z7}$ третьего раунда; слои блока данных, которые преобразуются в первом раунде; слои блока данных, которые преобразуются во втором раунде; слои блока данных, которые преобразуются в третьем раунде.

Основные идеи, лежащие в основе предлагаемого алгоритма:

- Представление 512-разрядного состояния S (State) алгоритма, т.е. входных и выходных блоков данных, всех промежуточных результатов преобразований в виде кубического массива бит 8 × 8 × 8 (рис. 1);
- Определение понятия слоя данных (L_{ji}, Layer) – квадратного массива битов 8 × 8, при этом $S = L_{x0} \| L_{x1} \| ... \| L_{x7} = L_{y0} \| L_{y1} \| ... \| L_{y7} = L_{z0} \| L_{z1} \| ... \| L_{z7}$; где $\|$ – операция конкатенации; L_{xi} – слои данных, параллельные плоскости $y0z$; L_{yi} – слои данных, параллельные плоскости $x0z$; L_{zi} – слои данных, параллельные плоскости $x0y$; $i = 0, 1, ..., 7$; $j \in \{x, y, z\}$;
- Представление 512-разрядного ключа K в виде трехмерного массива 8 × 8 × 8 бит (рис. 1);
- Определение понятия слоя ключа (KL_{ji}, KeyLayer), представляемого в виде двухмерного массива 8 × 8 бит, при этом $K = KL_{x0} \| KL_{x1} \| ... \| KL_{x7} = KL_{y0} \| KL_{y1} \| ... \| KL_{y7} = KL_{z0} \| KL_{z1} \| ... \| KL_{z7}$, где $\|$ – операция конкатенации, $j \in \{x, y, z\}$;
- Деление куба данных или ключа на слои параллельно плоскостям $y0z$, $x0z$, $x0y$;
- Двадцатичетырехкратное (по числу слоев) выполнение операции перемешивания слоя Mix с использованием шестираундового базового стохастического преобразования; операция Mix перемешивания слоя данных L_{ji} реализована в виде 6 итераций сети Фейстеля, обеспечивающих полное рассеивание и перемешивание информации. В каждой итерации используются таблицы замен размерностью 4 × 8 × 256 (в случае использования четырех 8-разрядных блоков замены) или 8 × 4 × 16 (в случае использования восьми 4-разрядных блоков замены);
- В качестве двадцати четырех 64-разрядных раундовых ключей преобразования слоев данных используются соответствующие 64-разрядные слои ключа; восемь слоев $KL_{x0}, KL_{x1}, ..., KL_{x7}$ используются в первом раунде преобразования состояния S в качестве раундовых ключей при преобразовании слоев данных соответственно $L_{x0}, L_{x1}, ..., L_{x7}$; восемь слоев $KL_{y0}, KL_{y1}, ..., KL_{y7}$ используются во втором раунде преобразования состояния S в качестве раундовых ключей при преобразовании слоев данных соответственно $L_{y0}, L_{y1}, ..., L_{y7}$; восемь слоев $KL_{z0}, KL_{z1}, ..., KL_{z7}$ используются в третьем раунде преобразования состояния S в качестве раундовых ключей при преобразовании слоев данных соответственно $L_{z0}, L_{z1}, ..., L_{z7}$;
- каждый 64-разрядный слой ключа KL_{ji} суть конкатенация 32-разрядных подключей k_1 и k_2, которые при выполнении шести раундов базового стохастического преобразования используются в следующей последовательности $k_1, k_2, k_2, k_1, k_1, k_2$ (шаг вперед, шаг назад и шаг вперед).

Последовательность преобразования (рис. 2):

1) По входному блоку данных M разрядностью 512 бит формируется блок данных S (состояние алгоритма) той же разрядности в соответствии с выражением $S := M$, после этого выполняются три раунда преобразования состояния S соответственно параллельно плоскостям $y0z$, $x0z$, $x0y$.

2) При выполнении преобразований первого раунда состояние S делится на восемь слоев данных $L_{x0}, L_{x1}, ..., L_{x7}$ параллельно плоскости $y0z$; каждый слой L_{xi} условно представляется в виде квадратного массива битов 8 × 8, после чего подвергается преобразованию Mix, затем преобразованные слои данных объединяются в преобразованный блок данных S.
3) При выполнении преобразований второго раунда состояние S делится на восемь слоев данных $L_{y0}, L_{y1}, ..., L_{y7}$ параллельно плоскости $x0z$; каждый слой L_{yi} условно представляется в виде квадратного массива битов 8 × 8, после чего подвергается преобразованию Mix, затем преобразованные слои данных объединяются в преобразованный блок данных S.
4) При выполнении преобразований третьего раунда состояние S делится на восемь слоев данных $L_{z0}, L_{z1}, ..., L_{z7}$ параллельно плоскости $x0y$, каждый слой L_{zi} условно представляется в виде квадратного массива битов 8 × 8, после чего подвергается преобразованию Mix, затем преобразованные слои данных объединяются в преобразованный блок данных S.

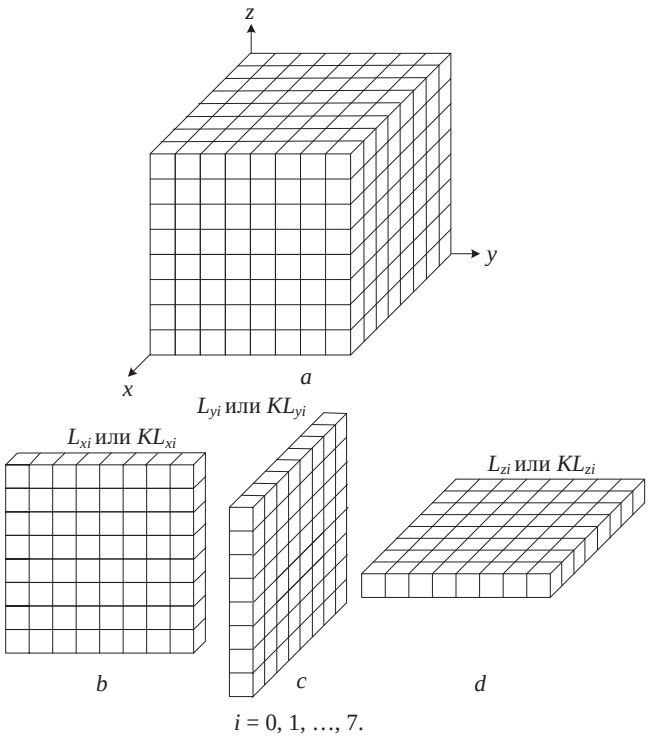


Рис. 1. Стохастическое преобразование 3DGOST: ***a*** *– блок данных (состояние S или ключ K);* ***b*** *– принцип разделения блока данных на слои параллельно плоскости $y0z$, слой L_{xi};* ***c*** *– принцип разделения блока данных на слои параллельно плоскости $x0z$, слой L_{yi};* ***d*** *– принцип разделения блока данных на слои параллельно плоскости $x0y$, слой L_{zi} блока данных; $i = 0, 1, ..., 7; j \in \{x, y, z\}$.*

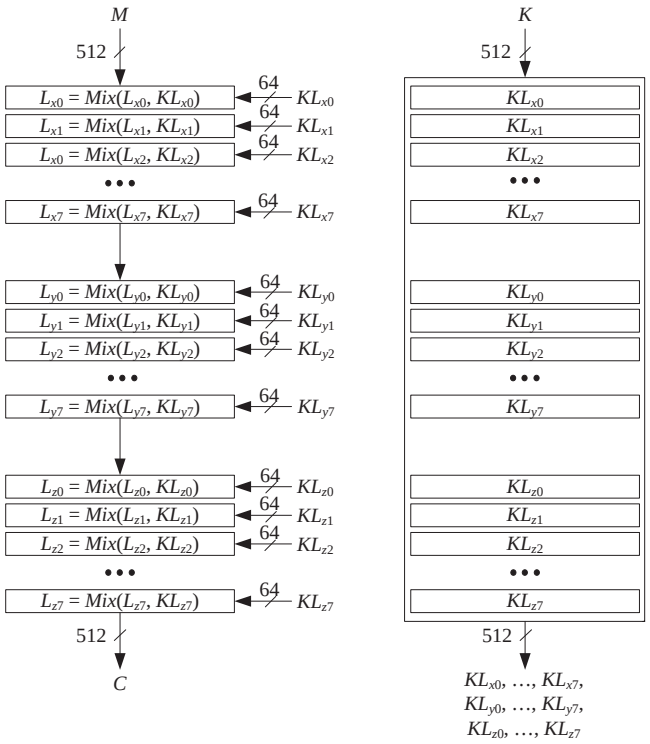


Рис. 2. Последовательность преобразования 3DGOST

Рис. 2 демонстрирует также принцип деления ключа на раундовые ключи. Показан ключ K; слои KL_{xi} ключа, которые являются раундовыми ключами первого раунда преобразования; слои KL_{yi} ключа, которые являются раундовыми ключами второго раунда преобразования; слои KL_{zi} ключа, которые являются раундовыми ключами третьего раунда преобразования.

На рис. 3 показан пример реализации базового стохастического преобразования (БСП) на основе шестираундовой сети Фейстеля.

Каждая из 6 итераций БСП (преобразования Mix) (рис. 3, а) может являться, например, раундом ГОСТ 28147-89, предполагающим деление входного 64-разрядного блока данных на левую L (Left) и правую R (Right) половины, последовательное выполнение операций $T = (R + SK) \bmod 2^{32}$, $T = S(T)$, $T = \mathrm{Rol}^{11}(T)$, $T = T$ XOR L, $L = R$, $R = T$, объединение новых значений L и R в преобразованный 64-разрядный блок данных, где T (Temporary) – временная переменная, SK (SubKey) – 32-разрядный подключ, $S()$ – 32-разрядная операция замены (Substitution), Rol^{11} (RotateLeft) – операция циклического сдвига на 11 разрядов влево 32-разрядного входного слова, XOR – 32-разрядная операция поразрядного сложения по модулю два (рис. 3, б).

На рис. 3 показаны RL_{ji} и LL_{ji} – соответственно младшая (Right) и старшая (Left) половины входного слоя данных L_{ji}; $RL_{ji}{}^*$ и $LL_{ji}{}^*$ – соответственно младшая и старшая половины преобразованного

слоя данных L_{ji}^*; F – раундовая функция, DI (DataIn) – входные 32-разрядные данные, k – 32-разрядный раундовый подключ (k_1 или k_2), DO (DataOut) – выходные 32-разрядные данные, Sub (Substitution) – 32-разрядный блок замены (S-блок).

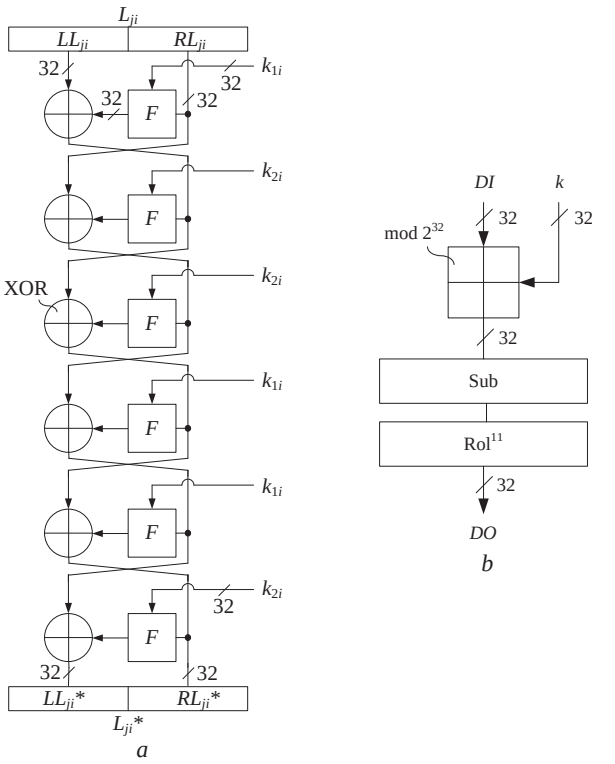


Рис. 3. Вариант реализации преобразования Mix слоев Lij:
***a** – схема базового стохастического преобразования на основе шестираундовой сети Фейстеля; **b** – вид функции F, которая была специфицирована в ГОСТ 28147-89.*

На рис. 4 показан принцип деления раундовых ключей KL_{xi}, KL_{yi} и KL_{zi} на подключи k_1 и k_2. RKL_{ji} и LKL_{ji} – соответственно младшая (Right) и старшая (Left) половины входного слоя ключа KL_{ji}.

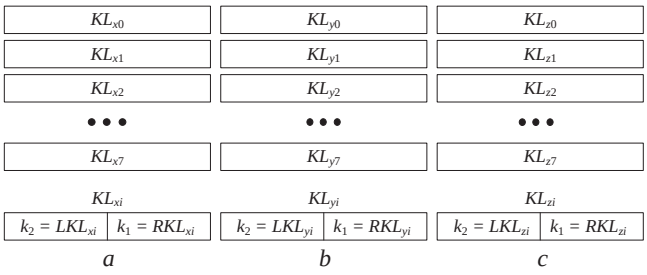


Рис. 4. Принцип деления раундовых ключей KL_{xi} (a), KL_{yi} (b) и KL_{zi} (c) на подключи k_1 и k_2.

Результаты статистического тестирования

Результаты статистического тестирования по методике НИСТ [18, 19] генератора псевдослучайных чисел, построенного по двухступенчатой схеме Counter Mode, где вторая ступень – это преобразование 3DGOST, показаны на рис. 5.

Файлов в запросе:	1000
Пропущено из-за размера:	0
Пропущено из-за периода:	0
Тестировалось:	1000
Из них прошло тесты:	
Проверка 0 и 1:	992
Проверка 0 и 1 в подпосл:	989
Проверка несц. серий:	976
Проверка сцеп. серий:	972
Проверка дырок:	990
Проверка дырок в подпосл.:	988
Проверка непер. шаблонов:	1000
Проверка пер. шаблонов:	986
Проверка частот:	987
Проверка интервалов:	960
Проверка перестановок:	912
Проверка на монотонность:	910
Универсальный тест Маурера:	985
Проверка рангов:	986
Проверка кум. сумм:	985
Проверка случ. отклон.:	927

a

Файлов в запросе:	1000
Пропущено из-за размера:	0
Пропущено из-за периода:	0
Тестировалось:	1000
Из них прошло тесты:	
Проверка 0 и 1:	990
Проверка 0 и 1 в подпосл:	992
Проверка несц. серий:	979
Проверка сцеп. серий:	977
Проверка дырок:	995
Проверка дырок в подпосл.:	988
Проверка непер. шаблонов:	1000
Проверка пер. шаблонов:	978
Проверка частот:	998
Проверка интервалов:	964
Проверка перестановок:	903
Проверка на монотонность:	907
Универсальный тест Маурера:	988
Проверка рангов:	993
Проверка кум. сумм:	985
Проверка случ. отклон.:	914

b

Рис. 5. Результаты тестирования ГПСЧ с функцией выхода на основе преобразования 3DGOST:
***a** – разрядность выходной последовательности 512 бит;*
***b** – разрядность выходной последовательности 8 бит.*

Заключение

Предложенное 3D стохастическое преобразование ориентировано на реализацию с использованием гетерогенных суперкомпьютерных технологий. Очевидно, что в пределах каждого раунда преобразования все восемь слоев состояния могут быть обработаны параллельно, поэтому применение, например, технологии CUDA [20, 21] позволит существенно упростить процесс разработки ПО. Предлагаемое решение позволит продлить жизнь многим качественным 64-разрядным криптоалгоритмам, не «дотягивающим» до требуемого сейчас 256-битного уровня безопасности для блочных шифров и 512-битного уровня безопасности для криптографических хеш-функций.

Нелинейное трехмерное многораундовое преобразование данных имеет повышенное быстродействие за счет максимального упрощения процедуры формирования раундовых ключей и подключей. Строго говоря, никакого формирования вообще нет. Раундовые ключи – это 24 слоя исходного ключа, имеющего кубическую структуру 8 × 8 × 8, показанную на рис. 1. Раундовые подключи каждого из 24-х шестираундовых преобразований Mix – это младшая и старшая половины раундовых ключей, которые используются по принципу «шаг вперед, шаг назад и шаг вперед». В результате нелинейное трехмерное многораундовое преобразование данных может использоваться в условиях ограниченных ресурсов, так как является Light-Weight алгоритмом, т.е. для решения задач защиты информации в RFID-системах и Интернете вещей.

Тестирование преобразование показало статистическую безопасность алгоритма.

Литература

1. Иванов М. А. Стохастические методы защиты информации. – Всероссийская научно-техническая конференция «Кибернетика и информационная безопасность» (КИБ 2023). Сборник научных трудов, Москва, 2023, с. 42-43.
2. Иванов М. А., Скитев А. А., Стариковский А. В. Классификация генераторов псевдослучайных чисел, ориентированных на использование в задачах защиты информации. (2016). [Электронный ресурс]. https://www.aha.ru/~msa/papers11.pdf (Дата обращения: 10.06.2024).
3. Joan Daemen, Lars Knudsen, Vincent Rijmen. The Block Cipher Square. (1998). [Электронный ресурс]. https://www.ime.usp.br/~rt/cranalysis/square.pdf (Дата обращения: 07.06.2016).
4. Joan Daemen, Vincent Rijmen. The Design of Rijndael. AES — The Advanced Encryption Standard. Springer-Verlag, Berlin, Heidelberg, NewYork, London, Paris, Tokyo, Hong Kong, Barcelona, Budapest, 2001, 253 p.
5. Jorge Nakahara Jr. 3D: A Three-Dimensional Block Cipher. In: Franklin M.K., Hui L.C.K., Wong D.S. (eds.) CANS 2008. LNCS, vol. 5339, pp. 252–267. Springer, Heidelberg, 2008.
6. P. Barreto, V. Rijmen. The WHIRLPOOL Hashing Function. (2003). [Электронный ресурс]. https://cryptospecs.googlecode.com/svn/trunk/hash/specs/whirlpool.pdf (дата обращения: 10.06.2024).
7. Keccak sponge function family. Main document. Guido Bertoni, Joan Daemen, Michael Peeters, Gilles Van Assche. (2008) [Электронный ресурс]. https://keccak.noekeon.org/Keccak-main-2.1.pdf (дата обращения: 10.06.2024).
8. G. Bertoni, J. Daemen, M. Peeters, G. Van Assche. Keccak specifications. (2009). [Электронный ресурс]. https://keccak.noekeon.org/Keccak-specifications-2.pdf (дата обращения: 10.06.2024).
9. R. Benadjila, O. Billet, H. Gilbert, G. Macario-Rat, T. Peyrin, M. Robshaw, Y. Seurin. SHA-3 proposal: ECHO. (2009). [Электронный ресурс]. https://crypto.rd.francetelecom.com/echo/doc/echo_description_1-5.pdf (Дата обращения: 10.06.2024).
10. P. Gauravaram, L. R. Knudsen, K. Matusiewicz, F. Mendel, C. Rechberger, M. Schlaffer and S. S. Thomsen. Grøstl – a SHA-3 candidate. (2011). [Электронный ресурс]. https://perso.uclouvain.be/fstandae/ source_codes/hash_atmel/specs/groestl.pdf (Дата обращения: 10.06.2024).
11. Eli Biham and Orr Dunkelman. The SHAvite-3 Hash Function. (2009). [Электронный ресурс]. https://ehash.iaik.tugraz.at/uploads/f/f5/Shavite.pdf (Дата обращения: 10.06.2024).
12. Информационная технология. Криптографическая защита информации. Функция хеширования. ГОСТ Р 34.11-2012. – Москва, Стандартинформ, 2012.
13. GOST 34.12-2018. Information Technology. Cryptographic Information Defense. Block Ciphers, 2018. Moscow: Standartinform.
14. Ivanov M. A., Vasilyev N. P., Chugunkov I. V. Three-dimensional data stochastic transformation algorithms for hybrid supercomputer implementation. (2012). [Электронный ресурс]. https://2012.nscf.ru/Tesis/Ivanov.pdf (Дата обращения: 10.06.2024).
15. Using Sequential and Parallel Composition for Stochastic Data Processing/ Ivanov M. A., Kozyrsky B. L., Komarov T. I., et.al. – Proceedings of The Radio-Electronic Devices and Systems for the Infocommunication Technologies (REDS-2013), Moscow, Russia, May 22-23, 2013, pp.144–148.
16. Three New Methods of Stochastic Data Transformaion/M. A. Ivanov, I. V. Matveychikov, A. A. Skitev, et. al. – Proceedings of The Radio-Electronic Devices and Systems for the Infocommunication Technologies (REDS-2016), Moscow, Russia, May 25-26, 2016, pp.351–355.
17. Иванов М. А., Стариковский А. В., Щустова Л. И. Новая жизнь старого ГОСТа: переход от одномерной версии к 3D. – REDS: Телекоммуникационные устройства и системы, 2017, Т. 7, № 4, с. 488–491.
18. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. A. Rukhin, J. Soto, J. Nechvatal, et.al. NIST Special Publication 800-22, Revision 1a. 2010.
19. Чугунков И. В. Методы и средства оценки качества генераторов псевдослучайных последовательностей, ориентированных на решение задач защиты информации. Учебное пособие. – М.: НИЯУ МИФИ, 2012.
20. Боресков А. В., Харламов А. А. Основы работы с технологией CUDA. М.: ДМК Пресс, 2011.
21. CUDA C++ Programming Guide. Release 12.5. NVIDIA, 2024.

3DGOST STOCHASTIC TRANSFORMATION ALGORITHM

Ivanov M. A.[5], Komarov T. I.[6], Kondakhchan M. A.[7], Starikovsky A. V.[8]

Abstract. *A promising direction in solving information security problems is the use of stochastic methods, the main result of which is the introduction of unpredictability into the operation of a computer system and network security tools.*

The purpose of this work *is to substantiate the possibility of effective use of 64-bit stochastic data transformation algorithms, which have proven themselves well in the past.*

The method to achieve *the goal is to use the Cube architecture.*

Results obtained: *a 3D algorithm for nonlinear data transformation is presented, oriented towards implementation using heterogeneous supercomputer technologies. Testing the algorithm in pseudorandom number generation mode showed its statistical safety.*

Keywords: *pseudorandom number generator, stochastic transformation, unpredictability, stochastic methods of information security.*

5 Mikhail A. Ivanov, Dr. Sc. (Eng), Professor, Chief Researcher, Institute of Computer Systems, National Research Nuclear University MEPhI, Moscow, Russia. E-mail: maivanov@mephi.ru

6 Timofey I. Komarov, Associate Professor, Department of Computer Systems and Technologies (No12), National Research Nuclear University MEPhI, Moscow, Russia. E-mail: tikomarov@mephi.ru

7 Mikael A. Kondakhchan, Student, Department of Computer Systems and Technologies (No12), National Research Nuclear University MEPhI, Moscow, Russia. E-mail: mikarkon@gmail.com

8 Andrey V. Starikovsky, Project Manager, State University of Management, Moscow, Russia. E-mail: av_starikovskiy@guu.ru

References

1. *Ivanov M. A. Stohasticheskie medody zashchity infomacii. – Vserossijskaj nauchno-technicheskaya Conferentsya «Kibernetica i informatcionnaya bezopasnost» (KIB 2023). Sbornik nauchnih trudov, Moskva, 2023, c. 42-43. (in Russian).*
2. *Ivanov M. A., Skitev A. A., Starikovskij A. V. Klassifikatciya generatorov psevdosluchainyh chisel orientirovannyh na ispolsovanie v zadachah zachity informatsii. (2016). [Electronic resource]. https://www.aha.ru/~msa/papers11.pdf (Date Views: 10.06.2024). (in Russian).*
3. *Joan Daemen, Daemen, Joan, Lars Knudsen, Vincent Rijmen. The Block Cipher Square. (1998). [Electronic resource]. https://www.ime.usp.br/~rt/cranalysis/square.pdf (Date Views: 07.06.2016).*
4. *Joan Daemen, Vincent Rijmen. The Design of Rijndael. AES – The Advanced Encryption Standard. Springer-Verlag, Berlin, Heidelberg, NewYork, London, Paris, Tokyo, Hong Kong, Barcelona, Budapest, 2001, 253 p.*
5. *Jorge Nakahara Jr. 3D: A Three-Dimensional Block Cipher. In: Franklin M. K., Hui L. C. K., Wong D. S. (eds.) CANS 2008. LNCS, vol. 5339, pp. 252–267. Springer, Heidelberg, 2008.*
6. *P. Barreto, V. Rijmen. The WHIRLPOOL Hashing Function. (2003). [Electronic resource]. https://cryptospecs.googlecode.com/svn/trunk/hash/specs/whirlpool.pdf (Date Views: 10.06.2024).*
7. *G. Bertoni, J. Daemen, M. Peeters, G. Van Assche. Keccak specifications. (2009). [Electronic resource]. https://keccak.noekeon.org/Keccak-specifications-2.pdf (Date Views: 10.06.2024).*
8. *Keccak sponge function family. Main document. Guido Bertoni, Joan Daemen, Michael Peeters, Gilles Van Assche. [Electronic resource]. http://keccak.noekeon.org/Keccak-main-2.1.pdf (Date Views 07.06.2016)*
9. *R. Benadjila, O. Billet, H. Gilbert, G. Macario-Rat, T. Peyrin, M. Robshaw, Y. Seurin. SHA-3 proposal: ECHO. (2009). [Electronic resource]. http://crypto.rd.francetelecom.com/echo/doc/echo_description_1-5.pdf (Date Views: 10.06.2024).*
10. *P. Gauravaram, L. R. Knudsen, K. Matusiewicz, F. Mendel, C. Rechberger, M. Schlaffer and S. S. Thomsen. Grøstl – a SHA-3 candidate. (2011). [Electronic resource]. https://perso.uclouvain.be/fstandae/ source_codes/hash_atmel/specs/groestl.pdf (Date Views: 10.06.2024).*
11. *Eli Biham and Orr Dunkelman. The SHAvite-3 Hash Function. (2009). [Electronic resource]. https://ehash.iaik.tugraz.at/uploads/f/f5/Shavite.pdf (Date Views: 10.06.2024).*
12. *GOST R 34.11-2012. Information Technology. Cryptographic Information Defense. Hash Finction.– Moscow, Standartinform, 2012. (in Russian).*
13. *GOST 34.12-2018. Information Technology. Cryptographic Information Defense. Block Ciphers. –Moscow, Standartinform, 2018. (in Russian).*
14. *Ivanov M. A., Vasilyev N. P., Chugunkov I. V. Three-dimensional data stochastic transformation algorithms for hybrid supercomputer implementation. (2012). [Electronic resource]. https://2012.nscf.ru/Tesis/Ivanov.pdf (Date Views: 10.06.2024).*
15. *Using Sequential and Parallel Composition for Stochastic Data Processing/ Ivanov M. A., Kozyrsky B. L., Komarov T. I., et.al. – Proceedings of The Radio-Electronic Devices and Systems for the Infocommunication Technologies (REDS-2013), Moscow, Russia, May 22-23, 2013, pp.144–148.*
16. *Three New Methods of Stochastic Data Transformaion/M. A. Ivanov, I. V. Matveychikov, A. A. Skitev, et. al. – Proceedings of The Radio-Electronic Devices and Systems for the Infocommunication Technologies (REDS-2016), Moscow, Russia, May 25-26, 2016, pp.351–355.*
17. *Ivanov M. A., Starikovskiy A. V., Shchustova L. I. Novaya zhizn' starogo GOSTa: perekhod ot odnomernoy versii k 3D. – REDS: Telekommunikatsionnyye ustroystva i sistemy, 2017, T. 7, № 4, s. 488–491. (in Russian).*
18. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. A. Rukhin, J. Soto, J. Nechvatal, et.al. NIST Special Publication 800-22, Revision 1a. 2010.*
19. *Chugunkov I. V. Metody i sredstva otsenki kachestva generatorov psevdosluchaynyh posledovatel'nostey. Uchebnoe posobie. – M.: NRNU MEPhI, 2012. (in Russian).*
20. *Boreskov A. V., Harlamov A. A. Osnovy raboty s tehnologiey CUDA. M.: DMK Press, 2011. (in Russian).*
21. *CUDA C++ Programming Guide. Release 12.5. NVIDIA, 2024.*

БЫСТРЫЙ СИНТЕЗ АУДИОСИГНАЛОВ ПО ИЗОБРАЖЕНИЯМ СПЕКТРОГРАММ В ЗАДАЧАХ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ

Дворянкин С. В.[1], Дворянкин Н. С.[2], Алюшин А. М.[3]

DOI: 10.21681/2311-3456-2024-5-34-46

Цель исследования: *разработка методов и алгоритмов инверсии спектрограмм: синтеза волновой формы сигнала по заранее известным данным его амплитудных спектральных разверток в отсутствии информации о фазе, – для генерации в реальном масштабе времени аудиосигналов с заданными частотно-временными свойствами с их последующем применением в системах защиты речевой информации.*

Методы исследования: *прикладного системного анализа, цифрового спектрально-временного анализа, цифровой обработки сигналов и изображений, образного анализа сонограмм.*

Результаты исследования: *предложены методы и алгоритмы синтеза звуковых и речевых сигналов по априори заданной спектрограмме, реализуемые в рамках концепции образного анализа-синтеза, работающие в реальном масштабе времени и обеспечивающие хорошие качественные оценки фазы пиковых значений спектральных срезов за один полностью детерминированный проход. Могут использоваться самостоятельно или для получения начальных оценок фазы для улучшения результатов итеративных алгоритмов типа Гриффина-Лима и др. Получаемые по обработанным изображениям спектрограмм оценки позиций и фазы спектральных пиков определяются точнее с помощью квадратичной интерполяции, а расчет приращения фазы по шагам времени ведется в специально введенном фазовом аккумуляторе, не требуя вычисления арктангенсов.*

Научная новизна: *предложен новый метод инверсии спектрограмм на основе рассечения-разнесения образа исходной спектрограммы для получения более точных спектральных описаний, синтезированного по ней аудиосигнала, лучше соответствующих оригиналу, чем у известных итерационных методов спектральной инверсии.*

Практическая значимость: *разработан эффективный, с точки зрения вычислений, алгоритм реального времени для однопроходной инверсии спектрограмм. Полученные результаты позволят расширить возможности существующих систем защиты речевой информации и проектировать более эффективные на основе изложенных подходов.*

Ключевые слова: *информационная безопасность, инверсия спектрограмм, образный анализ, защита от несанкционированного доступа, речеподобный сигнал, синусоидальная модель речи.*

Введение

Анализ существующих методов и средств обработки и защиты речевой информации (ЗРИ) от НСД показывает, что все они, так или иначе связаны с трансформацией, модификацией и-или заменой спектральных характеристик исходного речевого сигнала (РС), прежде всего с изменениями динамических разверток амплитудного спектра – спектрограмм[4] [1–8].

Сегодня амплитудные спектрограммы (для речи сонограммы) широко используются для представления, визуализации и выполнения операций над сигналами в частотной области. Приложения с их участием включают, но не ограничиваются следующими областями: перевод текста в речь, техническое маскирование (закрытие) речи, распознавание речи, генерация активных речеподобных помех для выделенных помещений, улучшение качества звука, акустическая стеганография, аудиокодеки и сжатие речи, изменение масштаба звучания по времени, изменение высоты тона, конвергенция и клонирование голоса, идентификация диктора, шумоподавление, реконструкция искаженных фонограмм и др [5,6,7]. [1–8].

Во многих приложениях, в том числе для ЗРИ, необходимы анализ и модификация изображений

1 Дворянкин Сергей Владимирович, доктор технических наук, профессор, профессор кафедры стратегических информационных исследований НИЯУ МИФИ, заведующий лабораторией защиты и обработки аудиовизуальной информации МГЛУ, г. Москва, Россия. E-mail: svdvoryankin@mephi.ru, https://orcid.org/0000-000-6908-0676

2 Дворянкин Никита Сергеевич, аспирант НИЯУ МИФИ, г. Москва, Россия. E-mail: nik.dvrn@gmail.com

3 Алюшин Александр Михайлович, старший преподаватель кафедры информатики и процессов управления НИЯУ МИФИ, научный сотрудник лаборатории защиты и обработки аудиовизуальной информации МГЛУ, г. Москва, Россия. E-mail:alyshin@list.ru

4 Барсуков В. С., Дворянкин С. В., Шеремет И. А. Безопасность связи в каналах телекоммуникаций / М.: НИФ «Электронные знания», 1992. 122 с.

5 Дворянкин С. В. Цифровая шумоочистка аудиоинформации. Под ред. А. В. Петракова. М.: ИП РадиоСофт, 2011. 208 с.

6 Дворянкин С. В., Макаров Ю. К., Хорев А. А. Обоснование критериев эффективности защиты речевой информации от утечки по техническим каналам // Защита информации. Инсайд. – № 2 (14). Март-апрель 2007. С. 18–25.

7 Петраков А. В., Лагутин В. С. Утечка и защита информации в телефонных каналах / М.: Энергоатомиздат, 1998. 317 с.

спектрограмм, полученных в результате кратковременного преобразования Фурье (КПФ) аудиосигналов, с последующим переходом к новому сигналу во временной области с так заданными свойствами. Совокупность указанных модулей и процедур, а именно: построение спектрограмм посредством КПФ, их обработка, трансформация или замена, в том числе методами искусственного интеллекта (ИИ), а также инверсия спектрограмм для получения нового речеподобного сигнала (РПС) с нужными характеристиками – составляют основу технологии «звук – изображение – звук» реализуемой в системе образного анализа – синтеза (ОАС), представленной на рис. 1, активно и успешно продвигаемой в решении ряда задач ЗРИ [1–8].

Рис. 1. Общая схема системы образного анализа-синтеза речи для технологии «звук-изображение-звук» при моделировании методов и средств ЗРИ в РМВ

Крайний модуль системы ОАС: «инверсия спектрограмм» или вокодер, – вычислительно ресурсоемкий, требует значительного времени на свою реализацию. Выходной сигнал РПС как правило имеет недостатки и по качеству звучания. В современных исследованиях функции вокодера перекладываются на нейросетевые решения и алгоритмы, что значительно суживает области применения ОАС в автономных системах ЗРИ, особенно работающих в режимах масштаба времени близких к реальному (РМВ).

В связи с этим разработка и исследование эффективного для РМВ алгоритма однопроходной инверсии спектрограмм в рамках концепции ОАС для решения задач защиты речевой информации остается весьма актуальной.

Образный анализ-синтез акустического речевого сигнала

Рассмотрим основные модули ОАС подробнее (рис.1).

Модуль построения спектрограмм

Спектрограмма сигнала представляет собой последовательность спектральных срезов, получаемых в ходе выполнения скачущего или скользящего кратковременного преобразования Фурье (КПФ). Уравнение КПФ известно как:

$$X(mS,\varpi) = \sum_{n=-\infty}^{\infty} x(n)w(n - mS)e^{-j\varpi n} \qquad (1)$$

Мгновенный амплитудный спектр как результат КПФ может быть представлен в виде модуля $|\ X(mS,\varpi)\ |$ этого преобразования, где w – окно анализа, S – шаг анализа (скачка) по оси времени, ϖ – круговая частота и m – индекс текущего кадра (фрейма) исходного сигнала, над которым делается КПФ.

На практике процедура вычисления КПФ состоит в том, чтобы разделить сигнал длительного времени на более короткие, перекрывающиеся сегменты равной длины, а затем вычислить через быстрое преобразование Фурье БПФ) амплитудный и фазовый спектры, на каждом выделенном коротком сегменте (фрейме).

Ансамбль последовательно получаемых неотрицательных амплитудных спектральных срезов позволяет рассматривать спектрограмму как некое изображение (графический образ), где в уровнях одного выбранного цвета (например, серого) на частотно-временной сетке отображаются мощностные характеристики звукового сигнала и «следы» (треки) элементарных гармоник его составляющих (рис. 2) [4, 6].

Модуль обработки изображений спектрограмм

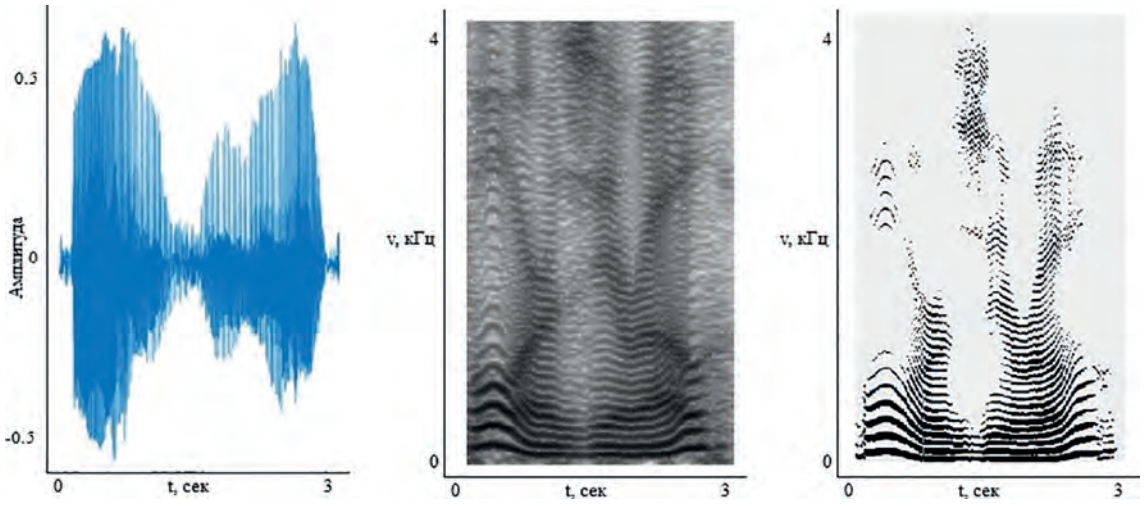
Современная обработка спектрограмм для различных приложений предполагает применение не только методов цифровой обработки изображений (ЦОИ) и сигналов, но и методов машинного обучения, распознавания образов, эффективных решений искусственного интеллекта (ИИ).

Отметим, что без потери информативности при переходе от временной к частотной области анализа возможны два типа представления спектрограммы: полутоновая и бинарная. Соответственно разные методы обработки изображений могут быть применены для решения той или иной задачи. Так хорошо проработанные давно известные методы обработки бинарных изображений показывают неплохие результаты в решении задач сжатия речи через сжатие её бинарных сонограмм [4, 6].

А реконструкция спектрограмм искаженных РС с помощью нейросетей и речевой базы данных целевого диктора позволяет решать задачи обработки и защиты речевой информации, ранее трудно решаемые или нерешаемые совсем. Например, речевая подпись, речевая реабилитация, адаптивная речеподобная помеха, стойкая к шумоочистке, и др.

Модуль инверсии спектрограммы (вокодер)

Как правило, амплитудные спектрограммы обрабатываются отдельно от фазовых составляющих частотных компонентов. Поэтому в некоторых приложениях, в частности в области ЗРИ, часто необходима инверсия спектрограммы, как процесс реконструкции волновой формы сигнала во временной области по его уже имеющейся заданной спектрограмме,



А) Б) В)

Рис. 2. Осциллограмма и спектрограммы РС: а) – волновая форма РС; б) – узкополосная полутоновая спектрограмма (гармоническая и формантная структура вместе); в) – бинарная спектрограмма с треками локальных максимумов узкополосных составляющих речи.

для которого требуется оценка фаз частотных составляющих спектра.

Если даже никаких изменений в исходных изображениях спектрограмм не проводилось, то волновая форма созданных по ним РПС может не совпадать с оригинальной и даже существенно от неё отличаться из-за различных начальных фаз в моделях РС, используемых в процедуре синтеза. А звучание оригинального и синтезированного по спектрограмме сигналов тем не менее будет идентичным, поскольку слух почти не восприимчив к фазам базовых гармоник.

В процессе аудио обработки, фазы либо теряются, либо становятся некорректными, либо их просто не существует для искусственно созданных спектрограмм. Таким образом, задача модуля состоит в том, чтобы использовать полученные посредством КПФ и модифицированные с помощью ИИ и ЦОИ амплитудные спектральные описания для генерации сигнала, спектр которого наилучшим образом будет соответствовать оригинальным спектрограммам.

Рассмотрим подробнее вопросы создания модуля однопроходной инверсии спектрограмм (вокодера) реального времени для решения задач ЗРИ. В качестве прототипов, подлежащих уточнению и совершенствованию, возьмем за основу и сориентируемся на алгоритмы инверсии спектрограмм и синтеза РПС с заданными спектральными характеристиками, приведенные в работах[8,9,10] [4, 6, 7].

Анализ существующих алгоритмов инверсии спектрограмм

В блоке вокодера (рис. 1) в основе преобразования (инверсии) изображения сгенерированной спектрограммы в новый звуковой или речевой сигнал от целевого диктора довольно часто используется итерационный алгоритм Гриффина-Лима (GLA) или ему подобные или производные [9–25], имеющие схожие недостатки по скорости и качеству синтеза нового РПС. Рассмотрим алгоритм Гриффина-Лима (GLA)[11].

Начиная с первоначальной оценки $X^0(n)$ исходного сигнала во временной области $x(n)$, каждая итерация алгоритма GLA итеративно обновляет оценку:

$$x^{i+1}(\mathrm{n}) = \frac{\sum_{m=-\infty}^{\infty} w(n - mS)\,\frac{1}{2\pi}\int_{\omega=-\pi}^{\pi} \hat{X}^i(mS,\omega)\, e^{-jwn}\, d\omega}{\sum_{m=-\infty}^{\infty} w^2(n - mS)}. \quad (2)$$

Здесь $\hat{X}^i(mS,\omega)$ есть результат КПФ от $x^i(n)$ со следующим ограничением на величину:

$$\hat{X}^i(mS,\omega) = X^i(mS,\omega)\frac{|\,X(mS,\omega)\,|}{|\,X^i(mS,\omega)\,|}, \quad (3)$$

где $|\,X(mS,\omega)\,|$ – модуль спектра в результате КПФ от исходного сигнала $x(n)$, $|\,X^i(mS,\omega)\,|$ – модуль КПФ i-й оценки $x^i(n)$, а S соответствует размеру шага анализа (сдвига) окна.

То есть, каждая новая итерация дает новый набор фаз, которые сочетаются с исходным спектром амплитуд для проведения следующей итерации.

Расстояние или мера близости часто рассчитывается как квадратичная ошибка между исходной

8 Beauregard, Gerald Harish, Mithila Wyse, Lonce Single Pass Spectrogram Inversion 2015/07/01, pp. 427–431. DOI – 10.1109/ICDSP.2015.7251907

9 R. Decorsiere, P. L. Sondergaard, E. N. MacDonald, and T. Dau, «Inversion of Auditory Spectrograms, Traditional Spectrograms, and Other Envelope Representations» Audio Speech Lang. Process. IEEEACM Trans. On, vol. 23, no. 1, pp. 46–56, 2015.

10 Дворянкин С. В. Речевая подпись. М.: РИО-МТУСИ. 2003. – 184 с.

11 D. Griffin and J. Lim, «Signal estimation from modified short-time fourier transform» Acoustics, Speech and Signal Processing, IEEE Transactions on, vol. 32, no. 2, pp. 236–243, 1984.

и реконструированной сигнальными спектрограммами с использованием показателя SER (Signal Error Ratio). Одним из достоинств алгоритма Гриффина-Лима[12] [15, 16] заключается в том, что он монотонно увеличивает SER с каждой новой итерацией. Для получения качественного синтезируемого сигнала на практике таких итераций должно быть около сотни, что требует существенного вычислительного ресурса.

Существенным недостатком является то, что оценка фазы для текущего кадра зависит от всех будущих и всех прошлых кадров исходного сигнала, а звучание нового синтезированного сигнала имеет металлизированные оттенки [8, 9] из-за размытости спектра на верхних частотах. Таким образом, этот метод уже по своей сути, изначально не является методом реального времени, что крайне востребовано в автономных системах ЗРИ.

Кроме того, отмечается, что для GLA важно выбрать подходящие начальные оценки фазовых компонент поскольку различающиеся начальные оценки дают разные результаты, и нет гарантии, что будет достигнуто оптимальное решение [13, 14, 15].

Нейросетевые алгоритмы восстановления фазы также ресурсоемкие и качество звучания синтезированного сигнала часто оставляет желать лучшего.

Поэтому для приложений РМВ в области ЗРИ предлагается разработать алгоритм однопроходной инверсии спектрограммы (ОИС), лишенный указанных недостатков алгоритма «GLA» и ему подобных, с использованием найденных зависимостей между амплитудным и фазовым спектрами РС[13], позволяющих восстанавливать фазовый спектр по амплитудному с точностью до начальной фазы и амплитудный спектр по фазовому с точностью до постоянного множителя.

Для этого сначала уточним используемую модель РС пофреймно рассматриваемого в виде суперпозиции узкополосных опорных синусоидальных сигналов[14] (синусоидальная модель [4–6]).

Синусоидальная модель РС и методы синтеза по локальным максимумам спектральных срезов

Во многих приложениях ЗРИ используются Гильбертовские модели, где РС рассматривается как произведение неотрицательной огибающей на косинус фазы. Согласно уточненной синусоидальной модели исходный РС при длительности анализируемого фрейма речи менее *40 мс* (оптимально 6–*8 мс*) [4–6] может быть представлен как:

$$x(n) = \sum_{k=1}^{K} A_k \, e^{-n^2/\sigma_{nk}} \cos(\omega_k n + \theta(n) + \varphi_{0k}), \qquad (4)$$

где n – номер временного отсчета; K – количество значимых синусоид для текущего фрейма; A_k – амплитуда k-й синусоиды; ω_k –круговая частота и φ_{0k} – начальная фаза k-й синусоиды, σ – эффективная ширина окна функции Гаусса, $\theta(n)$ – нелинейная часть фазы.

Достоверность данного описания может быть проверена путем сравнения фазовых значений элементарной гармоники из соотношения (4) на двух соседних спектральных срезах по фазограмме[15]:

$$\lim_{\Delta t \to 0} (\varphi_{i+1,k} - \varphi_{i,j} - \omega_i \Delta t) = 0 \qquad (5)$$

где $\varphi_{i,j}$ – значение фазы гармоники с частотой, соответствующей j-ому элементу ДПФ на i-ом спектральном срезе, $\varphi_{i+1,k}$ – значение фазы этой же гармоники, соответствующей k-ому элементу ДПФ на $(i+1)$-ом спектральном срезе, Δt – временной интервал между двумя соседними спектральными срезами.

Данное описание РС по формуле (4) обладает рядом преимуществ:

1. Здесь, с одной стороны, привнесённое окно Гаусса применяется для сглаживания краевых эффектов на границах фреймов, а с другой – позволяет рассматривать исходный речевой сигнал на каждом фрейме как суперпозицию узкополосных сигналов или вейвлетов Морле (синусоид взвешенных окном Гаусса).
2. Для синтеза речи по изображению спектрограммы достаточно учитывать только локальные максимумы спектрального среза, полученного в результате ДПФ.

   Действительно, в соответствии со следствиями преобразования Фурье перемножение функции окна на гармонический сигнал во временной области приводит к сдвигу образа окна на частоту этой синусоиды в частотной области. А образ окна Гаусса также является окном Гаусса. Следовательно локальные максимумы (ЛМ) или пиковые бины на столбцах (срезах) изображений спектрограмм с параметрами $\{A_i; \omega_i; \varphi_{0i}\}$ полностью определяют базовые узкополосные составляющие (4) анализируемого фрейма, по которым они могут быть восстановлены в составе нового синтезируемого по ним РС.
3. Появляется возможность описывать РС в виде (4) как на вокализованных, так и на невокализованных участках как суперпозицию элементарных базовых гармоник.
4. Для восстановления звукового сообщения только по изображению спектрограммы можно синтетически рассчитать фазу сигнала для ЛМ спектральных срезов, что может быть использовано при

12 D. Griffin and J. Lim, «Signal estimation from modified short-time fourier transform» Acoustics, Speech and Signal Processing, IEEE Transactions on, vol. 32, no. 2, pp. 236–243, 1984.

13 Дворянкин С. В. Речевая подпись. М.: РИО-МТУСИ. 2003. – 184 с.

14 R. McAulay and T. Quatieri, Speech analysis/Synthesis based on a sinusoidal representation, in IEEE Transactions on Acoustics, Speech, and Signal Processing. V. 34, no. 4. P. 744–754, August 1986.

15 Дворянкин С. В. Речевая подпись. М.: РИО-МТУСИ. 2003. – 184 с.

синтезе сигнала без использования оригинальных фазовых значений.

Исходя из этих преимуществ можно определить выражение (4) в качестве базового описания РС и предусмотреть возможность следующих видов синтеза РПС по ЛМ, найденным на исходной спектрограмме с оригинальной и искусственной фазой:

- ✓ синтез на основе обратного БПФ по трекам ЛМ синусоидальных составляющих на срезах, полученных с использованием КПФ;
- ✓ синтез по уточненным позициям ЛМ на спектральном срезе с использованием генераторов синусоидальных колебании;
- ✓ синтез по ЛМ базисных функций преобразования Фурье с рассечением-разнесением (прореживанием) спектрограммы.

Указанные методы синтеза будут подробно рассмотрены ниже.

Протяжка фазы для спектральных локальных максимумов

При отсутствии данных о фазе сигнала, например, для шумоочистки изображения его сонограммы и последующего синтеза по ней разборчивого РС, необходимо провести «протяжку» фазы, суть которой заключается в следующем:

а) в начальный момент времени полагаем фазу каждой гармоники равной нулю или случайному значению (на разборчивость речи это не влияет);

б) в каждый текущий момент времени фаза гармоники с номером i находится по формуле

$$\varphi_i(t + \Delta t) = \varphi_j(t) + \Delta t \frac{2\pi}{N} i, \text{ где } \arg\max_{j \in \{i-3,\ i+3\}} | X_j(t) | \qquad (6)$$

в) если на предыдущем временном срезе пределах створа наблюдения не найден ЛМ гармоники текущего среза, то фаза берется нулевой/случайной.

Таким образом становится возможным провести синтез речи только по изображению сонограммы, не имея в наличии оригинальной фазограммы сигнала.

Изменения в спектральных компонентах треков ЛМ узкополосных (синусоидальных) составляющих отслеживаются на обрабатываемой спектрограмме с использованием понятий «рождение», «жизнь» и «смерть», лежащих в основе принятого синусоидального представления (4) для РС[16].

Иллюстрация результатов процедур спектральных изменений в виде процессов «рождения», «смерти» и «жизни» (продолжения треков ЛМ) с учетом возможных положений пиковых бинов на последовательности спектральных срезов показана на рис. 3.

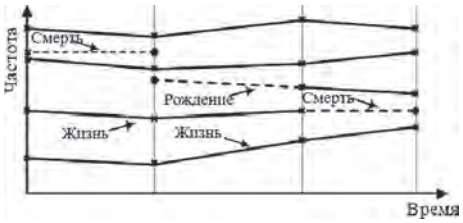


Рис. 3. Сопоставление на спектральных срезах треков локальных максимумов элементарных опорных гармоник и процедур «рождения-жизни-смерти»

На этапе синтеза, для каждого трека (следа) или контура базовой синусоиды, определенного на изображении спектрограммы (например, траектории линий гармоник основного тона на вокализованных фреймах), к заданным параметрам частоты и амплитуды трека будет присоединяться выбранная фазовая функция (оригинальная или искусственная в зависимости от задачи), необходимая для разворачивания и интерполяции фазы, построенная таким образом, чтобы фазовый след был максимально гладким [4–6].

Детализированная система образного анализа-синтеза речевого сигнала на основе синусоидальной узкополосной модели с учетом свойств слуха в составе модулей КПФ, обработки локальных максимумов треков базовых синусоид и инверсии спектрограмм показана на рис. 4.

В зависимости от решаемой задачи для каждого ЛМ на текущем спектральном срезе выбирается фазовая функция, либо как исходная, вычисленная по комплексному спектру исходного сигнала в ходе КПФ, либо искусственная, вычисленная на основе анализа треков ЛМ опорных синусоид на изображении амплитудного спектра, которая затем и применяется для синтеза нового речеподобного сигнала.

Как уже отмечалось, синтез нового РПС может проходить либо в блоке обратного БПФ с перекрываемым взвешиванием и суммированием, либо в гребенке синусоидальных генераторов (рис. 4), выход каждого звена которой модулируется амплитудой на уточненной частоте найденной опорной синусоиды и добавляется к другим найденным базовым синусоидальным волнам, чтобы сформировать окончательный вывод речи или звука, синтезированных по заданному изображению спектрограммы, которое в принципе может быть произвольного содержания.

Поскольку фазовая скорость пиков оценивается непосредственно по амплитудному спектру, а фазы непиковых бинов просчитываются через фазы пиков[17] или обнуляются, метод позволяет эффективно преобразовать спектрограмму, содержащую только величины амплитуд ЛМ, их частоту и фазу, в РПС

16 R. McAulay and T. Quatieri, Speech analysis/Synthesis based on a sinusoidal representation, in IEEE Transactions on Acoustics, Speech, and Signal Processing. V. 34, no. 4. P. 744–754, August 1986.

17 Beauregard, Gerald Harish, Mithila Wyse, Lonce Single Pass Spectrogram Inversion 2015/07/01, pp. 427–431. DOI - 10.1109/ICDSP.2015.7251907

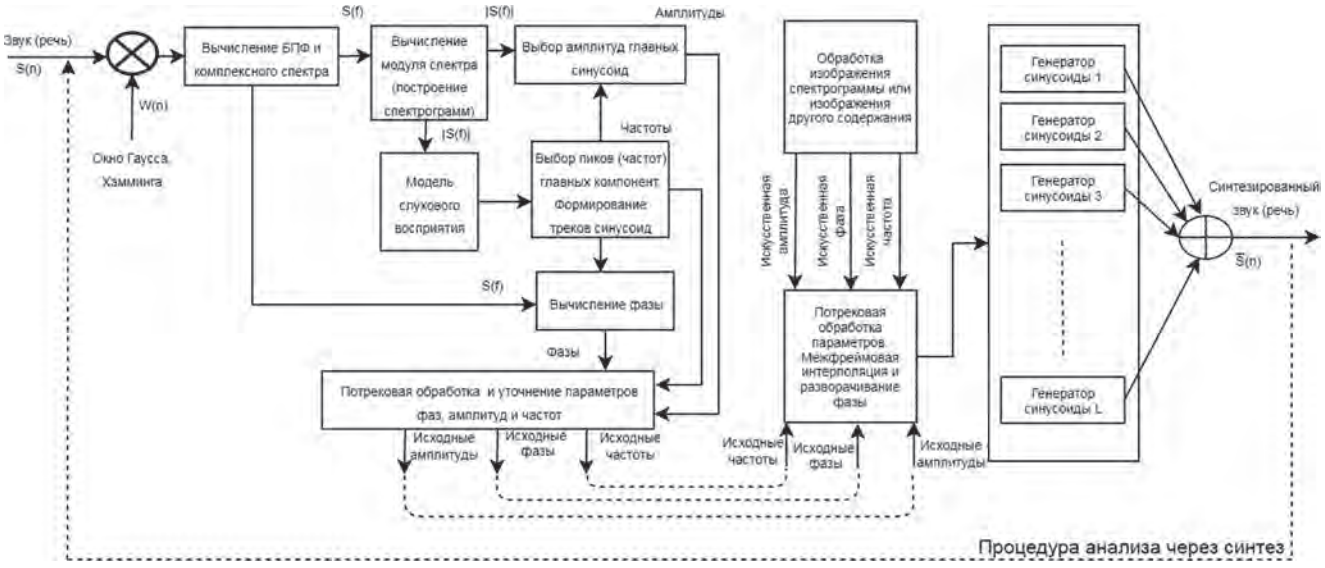


Рис. 4. Детализированная система образного анализа-синтеза акустического и речевого сигнала на основе синусоидальной узкополосной модели с учетом свойств слуха

сигнал во временной области за один детерминированный проход. То есть режим реального времени обработки в автономных системах ЗРИ вполне возможен и реализуем.

Оценка параметров локальных максимумов (пиковых бинов)

Метод однопроходной инверсии спектрограмм (ОИС) начинается с получения и обработки векторов текущего и предыдущего мгновенных амплитудных спектров (срезов), которые представляют собой результат быстрого преобразования Фурье (БПФ) над перекрывающимися и взвешиваемыми окном кадрами фактического или искусственного сигнала во временной области. Выбираемые последовательно кадры взвешиваются с помощью усеченного окна Гаусса размером σ = 0.17, базой БПФ N = 1024 и шагом анализа (перекрытия) S =50 отсчётов, что составляет 6,25 мс при Fd = 8000 Гц и длине кадра L = 1024.

Уточнение позиций (частот) локальных максимумов

Получаемые в процессе КПФ и последующей обработки спектрограмм параметры ЛМ опорных базовых синусоид, по которым впоследствии будет идти реконструкция сигнала с заданными спектральными свойствами, могут быть достаточно «загрублены» из-за некорректного выбора разрешения (базы) БПФ, вида окна и скорости трансформации спектра.

Для определения истинных значений параметров ЛМ, а именно $\{A_i;\ \omega_i;\ \varphi_{0i}\}$ производятся следующие уточняющие действия[18].

На текущем спектральном срезе определяются локальные максимумы (ЛМ) или пики при сравнении величины каждого бина j с соседями j+1 и j−1. Таким образом, если

$$|X(mS,\omega_j)|>|X(mS,\omega_{j-1})|....|X(mS,\omega_j)|>|X(mS,\omega_{j+1})|, \quad (7)$$

тогда позиция j на спектральном срезе считается пиком с амплитудой $|X(mS,\omega_j)|$.

Здесь m — это индекс времени, а

$$\omega_j = \frac{2\pi j}{N} \quad (8)$$

это частота бина j и N – база преобразования Фурье.

Далее для простоты изложения будем использовать следующие греческие буквы для описания этих параметров пикового бина и его соседей:

$$\alpha = |X(mS,\omega_{j-1})|,\ \beta = |X(mS,\omega_j)| \text{ и } \gamma = |X(mS,\omega_{j+1})| \quad (9)$$

Затем производится квадратичная интерполяция для определения истинного положения пика ЛМ на срезе, основанная на обработке позиций пикового бина и его соседей (всего три точки) с использованием формулы:

$$p = 0.5\,\frac{\alpha-\gamma}{\alpha-2\beta+\gamma} \quad (10)$$

Величина p принимает значения в диапазоне [–0.5, 0.5] и представляет собой отклонение позиции истинного пика ЛМ от пикового бина, как показано на рисунке 5. Это важно, так как каждый истинный пик соответствует синусоиде, частота которой не обязательно точно совпадает с центральной частотой БПФ бина, воспринимаемого изначально в качестве ЛМ. Рассматриваемая интерполяция дает оценку истинной пиковой частоты ЛМ.

18 Beauregard, Gerald Harish, Mithila Wyse, Lonce Single Pass Spectrogram Inversion 2015/07/01, pp. 427–431. DOI – 10.1109/ICDSP.2015.7251907

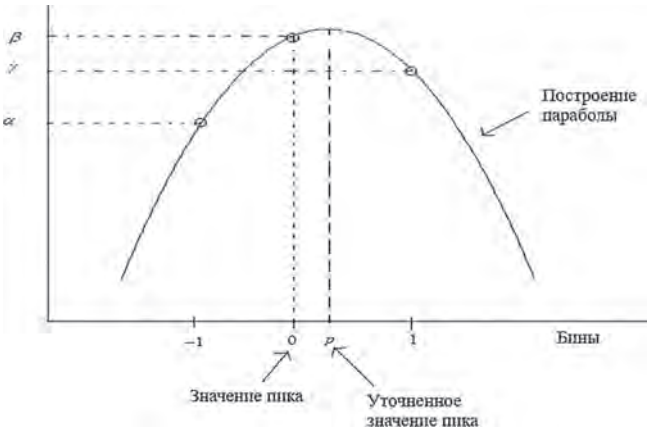


Рис. 5. Оценка значения уточненной амплитуды и частоты истинного пика с использованием квадратичной интерполяции ЛМ и позиций соседних бинов

Частота найденного истинного пика рассчитывается с использованием формулы (8), где j позиция пикового бина, а значение p рассчитывается, как в (10):

$$\omega_j = \frac{2\pi(j+p)}{N} \quad (11)$$

где ω_j — это скорректированная фазовая скорость, связанная с пиковым бином.

Если знаменатель в (10) равен 0, то истинная позиция ЛМ точно совпадает с частотой пикового бина.

Уточнение искусственной фазы ЛМ

Опираясь на результаты[19], создаем и используем фазовый аккумулятор, который хранит и пересчитывает значения фазы, которые должны использоваться для пикового бина j в текущем кадре (срезе) m, относительно фазы его предыдущего состояния. Тогда

$$\phi_{m,j} = \phi_{(m-1),j} + S\omega_j, \quad (12)$$

где S – шаг синтеза, который в большинстве приложений совпадает с размером шага анализа.

Фазовый аккумулятор каждый раз при синтезе нового среза обновляется в соответствии с формулой (11) только для пиковых бинов при формировании фаз ЛМ для нового текущего среза и сдвижке его прежних значений в предыдущий спектральный срез.

Теперь, когда фаза на пиках определена, фазы в оставшихся бинах могут быть рассчитаны в зависимости от значений признака P.

Здесь используется альтернативная стратегия π-фаз, которая может развиваться по двум сценариям: $P < 0$ и $P \geq 0$. В любом из них, два соседних слева и справа к пиковому бина будут принимать его фазу, сдвинутую на π[20].

19 Дворянкин С. В. Речевая подпись. М.: РИО-МТУСИ. 2003. – 184 с.

20 Beauregard, Gerald Harish, Mithila Wyse, Lonce Single Pass Spectrogram Inversion 2015/07/01, pp 427 – 431. DO - 10.1109/ICDSP.2015.7251907

Определение частотных позиций ЛМ, а также начальных фаз и приращения фаз в соответствии с треками движения ЛМ синусоидальных составляющих на спектрограмме сигнала использовались для синтеза нового РС и сравнения его спектрограммы с исходной по метрике Минковского.

Для реализации режима реального времени (РМВ) в условиях экономии вычислительного ресурса, предложено на своих прежних и уточненных позициях в спектральных срезах оставлять ЛМ с определенной по указанным правилам искусственной или оригинальной фазой. Все остальные точки спектра (непиковые бины) предлагается обнулять.

Варианты однопроходной инверсии спектрограмм в РМВ

Теперь, когда были рассчитаны фазы для каждого бина текущего спектрального среза, они могут быть объединены с частотными компонентами амплитудного спектра, формируя всю информацию, необходимую для реконструкции сигнала во временной области.

На последнем «вокодерном» шаге ОАС для получения реального звукового сигнала с заданными свойствами применяется либо гребенка синусоидальных генераторов (описана ранее рис. 4 для уточненных ЛМ), либо вычисляется обратное быстрое преобразование Фурье (для пиковых бинов) с взвешиванием результата усеченным окном Гаусса, чтобы получить выходные кадры, которые затем перекрываются и суммируются.

Блок-схема предлагаемого алгоритма инверсии спектрограмм реального времени, выполняемого с использованием обратного БПФ (ОБПФ) последовательно для каждого текущего среза с ЛМ, показана на рисунке 6.

Показанная на рис. 6 схема ОИС была спроектирована для работы в режиме РМВ и может входить составной частью в блок синтеза системы ОАС на рис. 4.

Под РМВ здесь понимается возможность проведения всех операций по построению одного спектрального среза, его обработки и синтеза по нему фрейма нового сигнал за промежуток времени равный интервалу между текущим и предыдущим спектральными срезами.

Рис. 6. Блок-схема алгоритма однопроходной инверсии спектрограмм с ОБПФ

Выбор метрики оценки качества синтезированных аудио сигналов

Чтобы оценить эффективность алгоритма, вычислялась амплитудная спектрограмма известного аудиосигнала во временной области, при необходимости с сохранением оригинальных фазовых значений.

Затем запускался алгоритм ОИС, чтобы получить значения искусственной фазы для генерации нового РС и получения от него новой спектрограммы, которая сравнивалась с оригиналом, используя известную меру отношения сигнала к ошибке (SER)[21] или другую меру.

В качестве исходной спектрограммы в экспериментах выступали также фотографии произвольного содержания, в частности фото лиц и предметов. Понятно, что исходные фазы здесь отсутствуют, и в процессе ОИС требуется присоединять искусственную фазу к каждому ЛМ.

$$SER=10\log\frac{\sum_{m=-\infty}^{\infty}\frac{1}{2\pi}\int_{\omega=-\pi}^{\pi}X(mS,\omega)^2d\omega}{\sum_{m=-\infty}^{\infty}\frac{1}{2\pi}\int_{\omega=-\pi}^{\pi}[|X(mS,\omega)|-|X'(mS,\omega)|]^2d\omega}. \quad (13)$$

Здесь X – это результат КПФ исходного сигнала, а X' является КПФ сигнала, реконструированного с помощью ОИС, m относится к временному индексу кадров КПФ и ω – индекс круговой частоты. Высокий SER указывает на лучшее соответствие между двумя сравниваемыми спектрами.

Для простоты вычислений в качестве критерия оценки качества предлагаемого алгоритма была выбрана метрика Миньковского (знаменатель формулы (13)), с помощью которой оценивалась степень соответствия эталонного изображения, и изображения спектрограммы синтезированного по эталону сигнала, построенного с использованием усеченной оконной функции Гаусса и базой БПФ N = 1024:

$$\varepsilon=\frac{1}{HW}\{\sum_{i=0}^{H-1}\sum_{j=0}^{W-1}|C(i,j)-\hat{C}(i,j)|^2\}^{1/2} \quad (14)$$

где H и W – высота (512 точек) и ширина изображений. Соответственно, $C(i,j)$ и $\hat{C}(i,j)$ – яркости (от 0 до 255) пикселя с координатами (i,j) на двух сравниваемых изображениях.

Здесь уже малое значение ε указывает на лучшее соответствие между двумя сравниваемыми изображениями спектрограмм.

Особенности синтеза по изображению произвольного содержания содержания с прореживанием полос

Разложение сигнала на базисные функции преобразования Фурье можно также рассматривать как частный случай Гильбертовского описания синусоидальной речевой модели, когда сигнал разбивается на N/2 гармоник, узкополосных процессов с фиксированной частотой.

Чтобы образы этих гармоник не пересекались и не искажали друг друга было предложено осуществлять предварительную сепарацию используемых исходных описаний.

ТБыла дана оценка двум различным видам синтеза (ЛМ и с прореживанием полос) в случае передачи произвольного изображения в виде спектра сигнала через канал звуковой связи. Для этого исходное изображение (Рис. 7) интерпретировалось как спектрограмма некоторого звукового сообщения, по ней производился синтез речи с искусственной фазой для ЛМ. По полученному звуковому файлу строилась его спектрограмма (Рис. 8), которая затем сравнивалась с оригиналом.

Для улучшения качества передаваемой картинки исходное изображение разбивалось на несколько полос (Рис. 9). Чтобы качество итогового изображения, получаемого после склейки полос (Рис. 10), не ухудшилось между полосами делались вертикальные пробелы, пропуски.

Оптимальным оказалось разбиение на 8 полос при базе Фурье N = 1024. При дальнейшем увеличении количества полос качество итогового изображения практически не улучшается. Нетрудно заметить, что качество итогового изображения, полученного в результате синтеза с разбиением на полосы (рис. 11), значительно лучше качества изображения, синтезированного без разбиения на полосы (рис. 8).

Следует также заметить, что качество итогового изображения будет тем лучше, чем более однородно исходное изображение.

Тестирование алгоритмов синтеза

Для тестирования использовались следующие виды аудио данных: речевые сигналы (мужской и женский голос) и фото лица и предметов, представляемые как готовые спектрограммы неких звуков произвольного содержания, как-то в виде матрицы неотрицательных чисел с высотой 512 пикселей. Исходные сигналы в режиме «моно» имели продолжительность от 2 до 8 секунд и оцифровывались с частотой дискретизации 8000 Гц с 16 бит на точку отчета. Также использовались усеченное окно Гаусса длиной в 1024 точки и 50 точечное расстояние между столбцами (шаг анализа) для всех спектрограмм аудиоданных.

В таблице 1 показаны обобщенные результаты сравнения качества различных видов синтеза РС и звука по изображениям спектрограмм в разных вариантах: с использованием всех значений спектрального среза; только по локальным максимумам; по уточненным ЛМ; по ЛМ с прореживанием полос. С использованием оригинальных и-или синтетических фазовых значений. Для сравнения изображений исходной и синтезированной спектрограмм использовалась метрика Минковского.

21 Beauregard, Gerald Harish, Mithila Wyse, Lonce Single Pass Spectrogram Inversion 2015/07/01, pp. 427–431. DOI – 10.1109/ICDSP.2015.7251907

Рис. 7. Исходное изображение перед конвертацией в звуковое сообщение

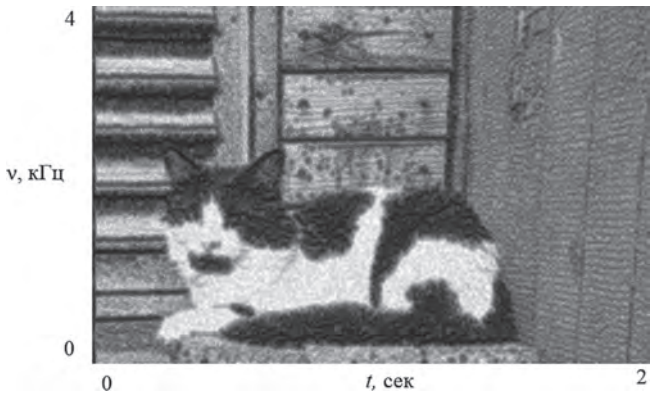


Рис. 8. Спектрограмма звукового сигнала, синтезированного только по ЛМ исходной картинки

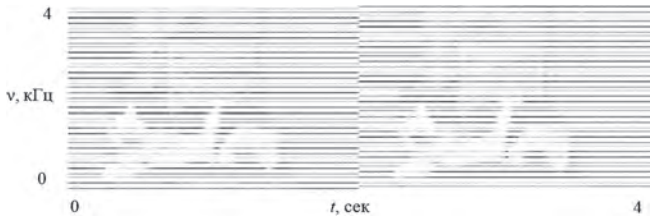


Рис. 10. Спектрограмма звукового сигнала, прореженная на полосы ЛМ (рассечение-разнесение)

Рис. 11. Восстановленное изображение после синтеза и склейки полос

По таблице 1 можно видеть, что алгоритм синтеза по всему спектральному срезу является оптимальным для точного сохранения информации об исходной спектрограмме, а синтез по локальным максимумам обладает наибольшим быстродействием (табл. 2), сохраняя при этом все идентификационные признаки и смысловое содержание речи.

В таблице 1 также отображены результаты проверки работоспособности алгоритма синтеза звука по изображению спектрограммы, в том числе для случаев, когда изображение не является сонограммой, а, например, фотопортретом.

Результаты сравнения времени работы различных видов синтеза для сигнала длительностью в 1 с представлены в таблице 2.

Из приведенных результатов тестирования видно, что синтез изображений произвольного содержания по ЛМ с прореживанием полос, оказался самым качественным, но и самым «медленным». А синтез по ЛМ для РС – самым быстрым с сохранением большинства просодических признаков.

Таким образом, под каждую задачу ЗРИ можно подобрать свой вид синтеза, удовлетворяющий заявляемым требованиям для однопроходной инверсии спектрограмм в реальном масштабе времени.

Разработанные способы и ПО генерации сигналов с требуемыми характеристиками, определяемыми заданными спектрограммами, использовались в ходе проведения экспериментов по проектам «Зрение через слух», «Речеподобные помехи, стойкие к шумоочистке», «Речевая реабилитация» и др., и показали хорошие результаты для данных видов приложений инверсии спектрограмм.

Заключение

Представлена концепция применения образного анализа-синтеза в системах защиты речевой информации (ЗРИ). В рамках предложенной концепции разработаны методы и алгоритмы однопроходной инверсии спектрограмм (ОИС), которые позволяют реализовать технологию «звук – изображение – звук», часто используемую в современных системах ЗРИ в масштабе времени близком к реальному.

Предложены различные виды синтеза звуков и речи по локальным максимумам (ЛМ) изображения исходной спектрограммы, отличающиеся по скорости исполнения и точности реализации. Наиболее быстрый – посрезный синтез по ЛМ опорных синусоид с искусственной фазой без расчета арктангенсов, наиболее точный – синтез по ЛМ базисных функций преобразования Фурье с прореживанием образа исходной спектрограммы на полосы.

Показана возможность получения оценок синтетической фазы, частоты и амплитуды ЛМ на текущем спектральном срезе, необходимых для реконструкции

Таблица 1.

Сравнение изображений спектрограмм до и после синтеза по метрике Минковского
с оригинальной и искусственной фазой для локальных максимумов спектральных срезов

Вид синтеза (предобработка спектрограммы)	Оригинальная фаза	Синтетическая фаза
Технология «Звук-Изображение-Звук - Изображение»		
по всему спектральному срезу РС, включая ЛМ и их соседей	0,003	0,009
только по локальным максимумам треков опорных синусоид	0,010	0,011
по уточненным ЛМ треков опорных синусоид	0,009	0,010
Технология «Изображение-Звук-Изображение»		
по ЛМ спектра изображения - для сонограмм - для фото лица	 информации об оригинальной фазе нет информации об оригинальной фазе нет	 0,011 0,009
по ЛМ с прореживанием полос - для сонограмм - для фото лица	 информации об оригинальной фазе нет информации об оригинальной фазе нет	 0,005 0,007

сигнала по представленной спектрограмме за один проход в РМВ.

Основным преимуществом такого метода фазовой оценки перед другими методами является простота вычислений, низкая ресурсоемкость и повышенная эффективность.

Фазовая реконструкция, выполняемая данным алгоритмом ОИС, имеет следующие преимущества перед другими методами инверсии спектрограмм:

- ✓ опирается на уточненную модель РС, представляемых в виде суммы узкополосных процессов (опорных синусоид), в качестве которых в ряде приложений могут выступать и базисные функции преобразования Фурье при соответствующем рассечении-разнесении исходной спектрограммы;
- ✓ включает в себя более точную квадратичную оценку местоположения пиков ЛМ на столбцах изображений амплитудных спектров сигнала;
- ✓ позволяет оценить фазовое приращение у соседних с пиками ЛМ на текущем спектральном срезе относительно позиций ЛМ на предыдущем;
- ✓ использует фазовый аккумулятор (стек), который работает с произвольными значениями начальных фаз для ЛМ, помогает определять фазовую функцию для трека ЛМ опорных синусоид и не требует вычислять арктангенс фазы;
- ✓ позволяет избавиться от нейросетевых вокодеров, которые сами по себе вычислительно дороги;
- ✓ может работать в режиме реального времени.

Предложенные методы ОИС также выгодно отличаются от методов инверсии спектрограмм типа

Таблица 2.

Время синтеза речевого (звукового) сообщения (мсек) длительностью в 1 с.

Вид синтеза	Оригинальная фаза	Синтетическая фаза
Синтез по всему спектральному срезу для РС	172 ± 8	182 ± 8
Синтез по локальным максимумам для РС	167 ± 8	177 ± 8
Синтез по уточненным локальным максимумам для РС	125 ± 8	134 ± 8
Синтез по ЛМ для фото лица	данных нет	177 ± 8
Синтез ИЗО по ЛМ с прореживанием полос для фото лица	данных нет	682± 8

GLA, которые требуют множества итераций частотного преобразования. Позволяют обеспечить удобные начальные фазы для итеративных методов типа GLA и производных от него, таких как FGLA, RTISI и RTISI-LA и др., что улучшает их работу и снижает количество проходов инверсии спектрограмм,

Методы ОИС обеспечивают хорошую оценку фаз с точки зрения принятой меры ошибки (мера Минковского), используемой для сравнения спектрограмм известного и синтезированного сигнала во временной области.

В рамках ОАС разработанный метод ОИС дополнительно к технологии «звук – изображение – звук» позволяет реализовать технологию «изображение – звук – изображение», формируя аудио сигнал в соответствии с любым априори заданным изображением его спектрограммы, например в виде фотопортрета.

Полученные результаты позволяют реализовать перспективные решения и расширить возможности существующих систем защиты речевой информации, сделать их более эффективными.

Литература

1. *Хорев А. А., Дворянкин С. В., Козлачков С. Б., Василевская Н. В. Анализ предельных возможностей методов шумопонижения и реконструкции речевых сигналов, маскируемых различными типами помех //Вопросы кибербезопасности. 2024. № 1 (59). С. 89–100.*
2. *Дворянкин С. В., Дворянкин Н. С., Устинов Р. А. Речеподобная помеха, стойкая к шумоочистке, как результат скремблирования защищаемой речи // Вопросы кибербезопасности. 2022. № 5 (51). С. 14–27.*
3. *Минаев В. А., Дворянкин С. В., Алюшин А. М. Методы биомаркирования защищаемых объектов // Информация и безопасность. 2023. Т. 26. № 3. С. 321–328.*
4. *Дворянкин С. В., Дворянкин Н. С., Устинов Р. А. Развитие технологий образного анализа-синтеза акустической (речевой) информации в системах управления, безопасности и связи // Безопасность информационных технологий, 2019. Т. 26, № 1. С. 64–76.*
5. *Дворянкин С. В., Зенов А. Е., Устинов Р. А., Дворянкин Н. С. Кодирование изображений спектрограмм для обеспечения переменной скорости передачи аудиоданных с сохранением качества их звучания // Безопасность информационных технологий. 2021. Т. 28. № 4. С. 22–38.*
6. *Дворянкин С. В., Уленгов С. В., Устинов Р. А., Дворянкин Н. С., Антипенко А. О. Системное моделирование речеподобных сигналов и его применение в сфере безопасности, связи и управления // Безопасность информационных технологий. 2019. Т. 26. № 4. С. 101–119.*
7. *Дворянкин С. В., Дворянкин Н. С. Средства, способы и признаки клонирования речи // Сборник статей по материалам IV Международной научно-практической конференции «Информационная безопасность: вчера, сегодня, завтра» под редакцией В. В. Арутюнова. Москва, РГГУ, 2021. С. 103–111.*
8. *Alyushin A. M., Dvoryankin S. V. Acoustic pattern recognition technology based on the Viola-Jones approach for VR and AR systems // В сборнике: Brain-Inspired Cognitive Architectures for Artificial Intelligence: BICA*AI 2020. Proceedings of the 11th Annual Meeting of the BICA Society. Сер. «Advances in Intelligent Systems and Computing» 2021. С. 1–8.*
9. *Kundan Kumar, Rithesh Kumar, Thibault de Boissiere, Lucas Gestin,Wei Zhen Teoh, Jose Sotelo, Alexandre de Brebisson, Yoshua Bengio, and Aaron C Courville. Melgan: Generative adversarial networks for conditional waveform synthesis. In Advances in Neural Information Processing Systems, pages 14881–14892, 2019.*
10. *Ryan Prenger, Rafael Valle, and Bryan Catanzaro. Waveglow: A flow-based generative network for speech synthesis. In IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pages 3617–3621, 2019.*
11. *Engel J. Resnick C. Roberts A. Dieleman S. Norouzi M. Eck D., Simonyan K. Waveglow: A flow-based generative network for speech synthesis. // ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing. 2019. Pp. 3617–3621.*
12. *Y. Masuyama, K. Yatabe, and Y. Oikawa, «Griffin–Lim like phase recovery via alternating direction method of multipliers», IEEE Signal Process. Lett., vol. 26, pp. 184–188, Jan. 2019.*
13. *T. Peer, S. Welker, and T. Gerkmann,«Beyond Griffin–Lim: Improved iterative phase retrieval for speech» in Proc. Int. Workshop Acoust. Signal Enhance. (IWAENC), Sept. 2022, pp. 1–5.*
14. *Y. Masuyama, K. Yatabe, Y. Koizumi, Y. Oikawa, and N. Harada, «Deep Griffin–Lim iteration», in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP), May 2019, pp. 61–65.*
15. *«Deep Griffin–Lim iteration: Trainable iterative phase reconstruction using neural network», IEEE J. Sel. Top. Signal Process., vol. 15, pp. 37–50, Jan. 2021.*
16. *Y. Ren, C. Hu, X. Tan, T. Qin, S. Zhao, Z. Zhao, and T. Y. Liu, «Fastspeech 2: Fast and high-quality end-to-end text to speech», in Proc. Int. Conf. Learn. Represent. (ICLR), May 2021.*
17. *T. Kaneko, H. Kameoka, K. Tanaka, and N. Hojo, «CycleGAN-VC3: Examining and improving CycleGANVCs for mel-spectrogram conversion», in Proc. Interspeech, Oct. 2020, pp. 2017–2021.*
18. *T. Hayashi, W. C. Huang, K. Kobayashi, and T. Toda, «Nonautoregressive sequence-to-sequence voice conversion», in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP), June 2021, pp. 7068–7072.*
19. *R. Prenger, R. Valle, and B. Catanzaro, «Waveglow: A flowbased generative network for speech synthesis» in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP), May 2019, pp. 3617–3621.*
20. *K. Kumar, R. Kumar, T. De Boissiere, L. Gestin, W. Z. Teoh, J. Sotelo, A. de Br´ebisson, Y. Bengio, and A. C. Courville, «Melgan: Generative adversarial networks for conditional waveform synthesis», in Proc. Adv. Neural Inf. Process. Syst. (NeurIPS), vol. 32, Dec. 2019.*
21. *J. Kong, J. Kim, and J. Bae, «Hifi-gan: Generative adversarial networks for efficient and high-fidelity speech synthesis», in Proc. Adv. Neural Inf. Process. Syst. (NeurIPS), Dec. 2020.*
22. *T. Kaneko, K. Tanaka, H. Kameoka, and S. Seki, «ISTFTNET: Fast and lightweight mel-spectrogram vocoder incorporating inverse short-time fourier transform», in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP), Apr. 2022, pp. 6207–6211.*

23. J. J. Webber, C. Valentini-Botinhao, E. Williams, G. E. Henter, and S. King, «Autovocoder: Fast waveform generation from a learned speech representation using differentiable digital signal processing», arXiv:2211.06989, 2022.
24. Y. Okamoto, K. Imoto, S. Takamichi, R. Yamanishi, T. Fukumori, and Y. Yamashita, «Onoma-to-wave: Environmental sound synthesis from onomatopoeic words», APSIPA Trans. Signal, Inf. Process., vol. 11, May 2022.
25. B. D. Giorgi, M. Levy, and R. Sharp, «Mel spectrogram inversion with stable pitch», in Proc. Int. Soc. Music Inf. Retr. Conf. (ISMIR), Dec. 2022, pp. 233–239.

FAST SYNTHESIS OF AUDIO SIGNALS FROM SPECTROGRAM IMAGES IN SPEECH INFORMATION PROTECTION TASKS

Dvoryankin S. V.[22], Dvoryankin N. S.[23], Alyushin A.M.[24]

Purpose of the work: *development of methods and algorithms for spectrogram inversion: determination of the waveform of a signal using the previously known data of its amplitude spectral sweeps in the absence of phase information – for real-time generation of audio signals with specified frequency-temporal properties with their subsequent application in speech information protection systems.*

Research methods: *applied system analysis, digital spectral-temporal analysis, digital signal and image processing, image analysis of sonograms.*

Research results: *methods and algorithms of synthesis of sound and speech signals by a priori given spectrogram, realized within the framework of the concept of image analysis-synthesis, working in real time and providing good qualitative estimates of the phase of peak values of spectral slices in one fully deterministic pass, are proposed. They can be used alone or in obtaining initial phase estimates to improve the results of iterative algorithms like Griffin-Lim et al. The estimates of positions and phase of spectral peaks obtained from the processed spectrogram images are determined more accurately using quadratic interpolation, and the recalculation of the phase increment by time steps is performed in a specially introduced phase accumulator, without requiring the calculation of arctangents.*

Scientific novelty: *a new method of spectrogram inversion based on dissection-dissection of the original spectrogram image is proposed to obtain more accurate spectral descriptions of the audio signal synthesized from it, better corresponding to the original than known iterative methods of spectral inversion.*

Practical value: *a computationally efficient real-time algorithm for single-pass spectrogram inversion has been developed. The obtained results will allow to expand the capabilities of existing systems of speech information protection and to design more effective ones on the basis of the described approaches.*

Keywords: *information security, spectrogram inversion, image analysis, protection against unauthorized access, speech-like signal, sinusoidal speech model.*

References

1. Khorev A. A., Dvoryankin S. V., Kozlachkov S. B., Vasilevskaya N. V. Analiz predel'nykh vozmozhnostei metodov shumoponizheniya i rekonstruktsii rechevykh signalov, maskiruemykh razlichnymi tipami pomekh //Voprosy kiberbezopasnosti. 2024. № 1 (59). S. 89–100.
2. Dvoryankin S. V., Dvoryankin N. S., Ustinov R. A. Rechepodobnaya pomekha, stoikaya k shumoochistke, kak rezul'tat skremblirovaniya zashchishchaemoi rechi // Voprosy kiberbezopasnosti. 2022. № 5 (51). S. 14–27.
3. Minaev V. A., Dvoryankin S. V., Alyushin A. M. Metody biomarkirovaniya zashchishchaemykh ob"ektov // Informatsiya i bezopasnost'. 2023. T. 26. № 3. S. 321–328.
4. Dvoryankin S. V., Dvoryankin N. S., Ustinov R. A. Razvitie tekhnologii obraznogo analiza-sinteza akusticheskoi (rechevoi) informatsii v sistemakh upravleniya, bezopasnosti i svyazi // Bezopasnost' informatsionnykh tekhnologii, 2019. T. 26, № 1. C. 64–76.
5. Dvoryankin S. V., Zenov A. E., Ustinov R. A., Dvoryankin N. S. Kodirovanie izobrazhenii spektrogramm dlya obespecheniya peremennoi skorosti peredachi audiodannykh s sokhraneniem kachestva ikh zvuchaniya // Bezopasnost' informatsionnykh tekhnologii. 2021. T. 28. № 4. S. 22–38.
6. Dvoryankin S. V., Ulengov S. V., Ustinov R. A., Dvoryankin N. S., Antipenko A. O. Sistemnoe modelirovanie rechepodobnykh signalov i ego primenenie v sfere bezopasnosti, svyazi i upravleniya // Bezopasnost' informatsionnykh tekhnologii. 2019. T. 26. № 4. S. 101–119.
7. Dvoryankin S. V., Dvoryankin N. S. Sredstva, sposoby i priznaki klonirovaniya rechi // Sbornik statei po materialam IV Mezhdunarodnoi nauchno-prakticheskoi konferentsii «Informatsionnaya bezopasnost': vchera, segodnya, zavtrA» pod redaktsiei V. V. Arutyunova. Moskva, RGGU, 2021. S. 103–111.

22 Sergey V. Dvoryankin, Dr.Sc. (of Tech.), Professor, Professor of the Department of Strategic Information Studies, National Research Nuclear University MEPhI, Head of the Laboratory for the Protection and Processing of Audiovisual Information, Moscow State Linguistic University. Moscow. Russia. E-mail: svdvoryankin@mephi.ru. https://orcid.org/0000-000-6908-0676
23 Nikita S. Dvoryankin, postgraduate student, National Research Nuclear University MEPhI. Moscow. Russia. E-mail: nik.dvrn@gmail.com
24 Alexander M. Alyushin, Senior Lecturer, Department of Informatics and Control Processes, National Research Nuclear University MEPhI, Researcher, Laboratory of Protection and Processing of Audiovisual Information., Moscow State Linguistic University. Moscow. Russia. E-mail: alyshin@list.ru

8. *Alyushin A. M., Dvoryankin S. V. Acoustic pattern recognition technology based on the Viola-Jones approach for VR and AR systems. В сборнике: Brain-Inspired Cognitive Architectures for Artificial Intelligence: BICA*AI 2020. Proceedings of the 11th Annual Meeting of the BICA Society. Сер. «Advances in Intelligent Systems and Computing» 2021. С. 1–8.*
9. *Kundan Kumar, Rithesh Kumar, Thibault de Boissiere, Lucas Gestin,Wei Zhen Teoh, Jose Sotelo, Alexandre de Brebisson, Yoshua Bengio, and Aaron C Courville. Melgan: Generative adversarial networks for conditional waveform synthesis. In Advances in Neural Information Processing Systems, pages 14881–14892, 2019.*
10. *Ryan Prenger, Rafael Valle, and Bryan Catanzaro. Waveglow: A flow-based generative network for speech synthesis. In IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pages 3617–3621, 2019.*
11. *Engel J. Resnick C. Roberts A. Dieleman S. Norouzi M. Eck D., Simonyan K. Waveglow: A flow-based generative network for speech synthesis. // ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing. 2019. Pp. 3617–3621.*
12. *Y. Masuyama, K. Yatabe, and Y. Oikawa, «Griffin–Lim like phase recovery via alternating direction method of multipliers», IEEE Signal Process. Lett., vol. 26, pp. 184–188, Jan. 2019.*
13. *T. Peer, S. Welker, and T. Gerkmann,«Beyond Griffin–Lim: Improved iterative phase retrieval for speech» in Proc. Int. Workshop Acoust. Signal Enhance. (IWAENC), Sept. 2022, pp. 1–5.*
14. *Y. Masuyama, K. Yatabe, Y. Koizumi, Y. Oikawa, and N. Harada, «Deep Griffin–Lim iteration», in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP), May 2019, pp. 61–65.*
15. *«Deep Griffin–Lim iteration: Trainable iterative phase reconstruction using neural network», IEEE J. Sel. Top. Signal Process., vol. 15, pp. 37–50, Jan. 2021.*
16. *Y. Ren, C. Hu, X. Tan, T. Qin, S. Zhao, Z. Zhao, and T. Y. Liu, «Fastspeech 2: Fast and high-quality end-to-end text to speech», in Proc. Int. Conf. Learn. Represent. (ICLR), May 2021.*
17. *T. Kaneko, H. Kameoka, K. Tanaka, and N. Hojo, «CycleGAN-VC3: Examining and improving CycleGANVCs for mel-spectrogram conversion», in Proc. Interspeech, Oct. 2020, pp. 2017–2021.*
18. *T. Hayashi, W. C. Huang, K. Kobayashi, and T. Toda, «Nonautoregressive sequence-to-sequence voice conversion», in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP), June 2021, pp. 7068–7072.*
19. *R. Prenger, R. Valle, and B. Catanzaro, «Waveglow: A flowbased generative network for speech synthesis» in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP), May 2019, pp. 3617–3621.*
20. *K. Kumar, R. Kumar, T. De Boissiere, L. Gestin, W. Z. Teoh, J. Sotelo, A. de Br´ebisson, Y. Bengio, and A. C. Courville, «Melgan: Generative adversarial networks for conditional waveform synthesis», in Proc. Adv. Neural Inf. Process. Syst. (NeurIPS), vol. 32, Dec. 2019.*
21. *J. Kong, J. Kim, and J. Bae, «Hifi-gan: Generative adversarial networks for efficient and high-fidelity speech synthesis», in Proc. Adv. Neural Inf. Process. Syst. (NeurIPS), Dec. 2020.*
22. *T. Kaneko, K. Tanaka, H. Kameoka, and S. Seki, «ISTFTNET: Fast and lightweight mel-spectrogram vocoder incorporating inverse short-time fourier transform», in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP), Apr. 2022, pp. 6207–6211.*
23. *J. J. Webber, C. Valentini-Botinhao, E. Williams, G. E. Henter, and S. King, «Autovocoder: Fast waveform generation from a learned speech representation using differentiable digital signal processing», arXiv:2211.06989, 2022.*
24. *Y. Okamoto, K. Imoto, S. Takamichi, R. Yamanishi, T. Fukumori, and Y. Yamashita, «Onoma-to-wave: Environmental sound synthesis from onomatopoeic words», APSIPA Trans. Signal, Inf. Process., vol. 11, May 2022.*
25. *B. D. Giorgi, M. Levy, and R. Sharp, «Mel spectrogram inversion with stable pitch», in Proc. Int. Soc. Music Inf. Retr. Conf. (ISMIR), Dec. 2022, pp. 233–239.*

СИСТЕМОТЕХНИКА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ В ИНФОРМАЦИОННОЙ СФЕРЕ

Толстой А. И.[1]

DOI: 10.21681/2311-3456-2024-5-47-57

Аннотация. *В статье рассмотрены основы методологии обеспечения безопасности (ОБ) объектов, использующих современные информационные технологии (Объектов), базирующиеся на концепции, принципах и методах системотехники. В рамках системотехники был развит процессный, системный и управленческий подходы к ОБ Объектов, основанные на разработанных процессных моделях Объекта как части Организации, самого Объекта и его систем ОБ. В работе обосновано выделены среди процессов ОБ Объекта четыре группы процессов – это обеспечение безопасности информации, устойчивости, информационно-психологической безопасности персонала и физической защиты Объекта с учетом необходимости обеспечить состояние защищенности основных активов Объекта и формулирования отдельных целей ОБ Объекта. В каждой из этих групп в рамках развития процессного подхода были выделена часть процессов, реализация которых направлена на достижение необходимого состояния защищенности активов Объекта, и часть процессов управления процессами из первой части, которые должны обеспечить необходимую результативность на стадиях их планирования, реализации, контроля и совершенствования. При этом показан адаптивный характер управления такими процессами. С учетом выделенных групп процессов была предложена структура систем, входящих в СОБ Объекта, и структура системы процессов ее поддержки (динамическое и статическое представление СОБ соответственно), а также структура комплексной системы безопасности Объекта. Использование системотехники при ОБ Объекта позволило на единой методологической базе обосновать направление подготовки профессионалов в области ОБ Объектов, определив их квалификацию (инженер-системотехник) и возможный перечень специальностей, входящих в это направление. Применение системотехники в рамках решении задач ОБ Объекта позволило осуществить системный (целостный) подход, необходимый для проведения исследований, проектирования, реализации и развития систем обеспечения безопасности конкретных Объектов. Предлагаемые в работе решения носят обобщенный характер и не противоречат существующему в настоящее время подходу, связанному с обеспечением информационной безопасности.*

Ключевые слова: *методология, концепция, принципы, метод, модель, процесс, система, актив, управление, безопасность информации, устойчивость, информационно-психологическая безопасность, физическая безопасность.*

Введение

Для объектов, имеющих отношение к обработке информации с использованием современных информационных технологий (ИТ), решение проблемы сохранения ее основных свойств (конфиденциальности, целостности и доступности) чаще всего сводится к принятию мер защиты информации (ЗИ) или к обеспечению информационной безопасности (ИБ). Признанной основой решения этой проблемы является принятая в настоящее время методология, базирующаяся на процессном, управленческом и системном подходах к обеспечению информационной безопасности (ОИБ)[2]. Проецируя определения понятия «ИБ», данное в Доктрине «Информационная безопасность РФ»[3] на уровень объекта, были даны определения понятий «ИБ объекта» как состояния защищенности его активов от угроз в информационной сфере, «процесс ОИБ объекта» как действия, направленного на достижения такого состояния, и «система ОИБ (СОИБ) объекта» как совокупности связанных процессов ОИБ [1, 2].

Анализ СОИБ объекта показал [2], что эта система существенно зависит от особенностей объекта, которому она относится (сложность объекта, интеграция современных информационных технологий на аппаратном, программном и информационном уровне), и от особенностей процессов ОИБ (связанности, разнородности, сложности). При этом необходимо отметить, что в некоторых случаях цели функционирования СОИБ и объекта могут быть близки (например, поддержка качества реализации основных процессов (бизнес-процессов), или противоположны (сохранение свойств информации для СОИБ и скорость обработки информации для объекта). Дополнительным фактором, который необходимо учитывать, является непременное участие людей (например персонала организации), имеющего отношение к качественному

1 Толстой Александр Иванович, кандидат технических наук., доцент, Национальный исследовательский ядерный университет «МИФИ», Москва, Россия. E-mail: AITolstoj@mephi.ru, http://orcid.org/0000-0001-9265-1510

2 ГОСТ Р ИСО/МЭК 27000-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология.

3 Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента РФ от 05.12.2016 N 646.

функционированию и использованию объекта, относящегося к организации и его СОИБ, а также влияние окружающей среды на функционирование объекта и его СОИБ. Таким образом и сам объект, и его СОИБ можно отнести к сложным системам, объединяющим сложные системы [3], а также к социотехническим системам [3,4,5], требующим свои подходы к их исследованию, проектированию и эксплуатации.

Если рассмотреть особенности такой предметной области, как системная инженерия [6] (чаще называемая в русскоязычных информационных источниках системотехникой [7]), которая связанна с проектированием, созданием и эксплуатацией структурно сложных, крупномасштабных, человеко-машинных и социотехнических систем [6], а также особенности объектов системотехники, представляющих собой человеко-машинные системы, состоящие из разнородных элементов и связей, включая и окружающую среду [7], то саму систему обеспечения ИБ объекта можно обосновано считать объектом системотехники.

Это утверждение положено в основу исследований, результаты которого приводятся в данной работе. Особое внимание уделено применимости принципов системотехники к исследованию систем обеспечения безопасности объектов в информационной сфере (далее Объектов) в части формирования процессной модели организации (далее Организации), к которой относится Объект, и ее системы обеспечения безопасности (СОБ Объекта), а также формирования модели поддержки действий в отношении СОБ Объекта.

1.Основы системотехники и обеспечение безопасности Объекта

Формирование системотехники обеспечения безопасности Объекта непосредственно связано с основами системотехники. При этом важно уточнить особенности используемых понятий, рассмотреть современные концепции системотехники, ее принципы, методы и предмет в контексте выбранного объекта системотехники: СОБ конкретного объекта. В данной работе предлагаются следующие определения базовых понятий:

Безопасность объекта в информационной сфере *– это состояние защищенности активов объекта от угроз в информационной сфере, которому соответствует допустимый уровень риска нарушения безопасности объекта*.

Информационная сфера *– это совокупность информационного пространства, объединяющего объекты, обрабатывающие информацию с использованием современных ИТ, и субъекты, реализующие деструктивное воздействие на активы объекта, с учетом их взаимного расположения, и информационной среды, в которой взаимодействуют объекты и субъекты.*

Процесс обеспечения безопасности объекта в информационной сфере *– это деятельность, направленная на достижения необходимого состояния защищенности активов объекта от угроз в информационной сфере.*

Система обеспечения безопасности объекта в информационной сфере *– это совокупность связанных процессов, направленных на достижение необходимого состояния защищенности активов объекта от угроз в информационной сфере.*

1.1. Понятие «системотехника»

Понятие «системотехника» многогранно и имеет комплексный характер [6,7]. Из множества определений этого понятия можно выделить следующие общие факторы [7]:

1. *Сфера деятельности*, направленная на организацию процесса создания, использования и развития сложных инженерных систем.

Сфера деятельности, относящаяся к обеспечению безопасности (ОБ) Объекта, — это информационная сфера. Предметом деятельности является решение задач по ОБ конкретного объекта. Это комплексные задачи, решение которых предполагает кооперацию специалистов различных профилей с целью интеграции частей СОБ в единое целое.

2. *Область знания:* комплексная научно-техническую дисциплина, объединяющая средства, методы, принципы анализа и организации инженерной деятельности, а также средства, методы, приемы и процедуры проектирования и исследования сложных инженерных систем.

Область знания, относящаяся к предметной области ОБ Объекта, связана с методами и средствами современных математических, технических, естественнонаучных и общественных дисциплин, необходимых для исследования и проектирования СОБ Объекта.

3. *Конкретно-методологическую позицию*, связанную с целостным рассмотрением инженерной системы, процесса ее исследования, проектирования, создания и развития.

Основным методом системотехники является системный подход с его конкретными видами реализации: системным анализом, исследованием операций и кибернетикой [8].

Таким образом, системотехника – это научное направление, изучающее общесистемные свойства системотехнических комплексов, процессы их создания, совершенствования, использования и ликвидации в целях получения максимального социального эффекта [8].

Применение системотехники в рамках решения задач ОИБ конкретного Объекта позволяет осуществить системный (целостный) подход к рассмотрению СОБ Объекта при ее исследовании, проектировании, реализации и развитии.

1.2. Концепции системотехники

Для системотехники важное значение имеет системное представление ее объекта, обладающее чертами, присущими всем (или многим) сложным инженерным объектам. Выделяют пять основных системных представлений [7]: процессуальное, функциональное, макроскопическое, иерархическое и микроскопическое.

Исходя из этого, СОБ может быть представлена динамически как совокупность процессов, обеспечивающих состояние защищенности активов Объекта, статически как предмет, обладающий определенными внешними или внутренними свойствами (характеристиками) или функционально, когда внутреннее строение СОБ может быть представлено в виде структуры, реализующей совокупность связанных функций (действий) для достижения определенной цели (например, достижения целостности, доступности или конфиденциальности информации).

В основании системотехники лежит ряд концепций — общих абстрактных представлений, связанных с пониманием её предмета, а также совокупность принципов, то есть исходных, принимаемых за истину, правил, которые используются в качестве основы для рассуждений и/или для принятия решений [6].

Основные концепции системотехники включают следующие понятия: система, жизненный цикл и заинтересованные стороны [6].

Среди особенностей, которые имеет система, рассматриваемая системотехникой, необходимо в дополнение к уже отмеченным выше выделить признаки, которые полностью можно отнести и к СОБ Объекта [6]: структурная и функциональная сложность, большие информационные потоки, функционирование в условиях существенной неопределённости и воздействия среды на неё (объект функционирует в информационной сфере при деструктивном воздействии угроз, имеющих вероятностный характер проявления).

Использование понятия жизненного цикла системы признано фундаментальной основой практики системотехники [9]. При этом жизненный цикл системы (system life cycle) связывают с ее развитием во времени, начиная от замысла и заканчивая списанием . На каждом этапе жизненного цикла система имеет относительно стабильный набор характеристик. При моделировании жизненного цикла используются совокупности процессов жизненного цикла.

Для описания жизненного цикла СОБ Объекта можно применить процессный подход [3], основанный на циклической модели Деминга [10], предполагающий такие этапы жизненного цикла, как планирование, реализация, контроль и совершенствование процессов СОБ.

В системотехнике критически важной задачей является выявление ключевых заинтересованных сторон и их интересов, анализ их баланса с учётом механизмов их возникновения и необходимости гармонизации точек зрения, а также оценка относительной степени влияния разных заинтересованных сторон на принимаемые решения. является в системной инженерии критически важной задачей [6].

Заинтересованная сторона (stakeholder) или правообладатель[4] — это сторона, имеющая право, долю или претензии на систему или на владение ее характеристиками, удовлетворяющими потребности и ожидания этой стороны. Заинтересованные стороны преследуют различные цели, которые должны быть гармонично учтены на основе баланса их интересов, в том числе через регулирование отношений: между группами заинтересованных сторон; между заинтересованными сторонами и объектом интереса.

При ОБ Объекта заинтересованными сторонами могут быть владелец Объекта (Организации), владелец информации, партнеры Организации, регуляторы отношений в области ОБ, само государство. Важность выявления и учета интересов заинтересованных сторон подтверждена, например, при обеспечении кибербезопасности в киберпространстве[5].

1.3. Принципы системотехники

В процессе развития системотехники сложились её основные принципы [6, 11, 12]. Среди них наиболее важными для области ОБ Объектов будут:

1) Переход от редукционистского к системному подходу [6, 11].
2) Переход от структурного к процессному подходу [6].
3) Доказательно обоснованное принятие решений на основе фактов и с учётом риска — наиболее важным фактором при принятии решений является наличие доказательно обоснованного факта, а не плана, графика или календарного события [12].
4) Использование метода синтеза при выборе, описании и проектировании «правильных» составных частей системы, их соединении между собой так, чтобы достигалось необходимое и правильное сочетание для достижения необходимых свойств целого [11].

4 ГОСТ Р ИСО/МЭК 15288-2005 ИТ. Системная инженерия. Процессы жизненного цикла систем.

5 ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity.

5) Применение адаптивной оптимизация характеристик сложной системы к новым ситуациям и изменениям, происходящим в самой системе, во внешней среде и в других системах, взаимодействующих с целевой системой [11].
6) Постепенное уменьшение энтропии. Процессы системотехники должны реализовываться на протяжении всего жизненного цикла системы, в результате чего энтропия, характеризующая целевую систему, постепенно уменьшается с переходом от состояния беспорядка (высокая энтропия) к состоянию порядка (низкая энтропия) в конце цикла [11].
7) Достижение разумной ситуации для получения результатов, которые в данных условиях позволяют в наибольшей степени удовлетворить критически важные заинтересованные стороны [11].
8) Переход от методов жёсткого планирования к использованию гибких прогнозных методов [6].
9) Переход от монодисциплинарного к междисциплинарному подходу [6].

Принципы системотехники 1), 2) и 3) соответствуют современной методологии обеспечения ИБ, которая предполагает реализацию системного, процессного и риск-ориентированного подходов[2], что можно использовать и при ОБ Объектов.

Принцип 4) предполагает обоснованную структуризацию СОБ Объекта с формулированием требований к ее составным частям и требований, которые должны быть выполнены при синтезе этих частей для достижения необходимой результативности ОБ конкретного Объекта.

Наиболее важный аспект использования принципа 5) при ОБ Объекта – это учет особенностей самого Объекта при создании его СОБ, особенностей Организации, частью которой является Объект, а также особенностей внешней среды, в которой функционирует Организация, Объект и СОБ [1, 2].

Реализация принципа 6), направленная на постоянное совершенствование СОБ Объекта, позволяет достичь обоснованной прозрачности и упорядоченности действий для достижения требуемой результативности ОБ Объекта.

При ОБ Объекта удовлетворение требований заинтересованных сторон (правообладателей[4]), о которых говорилось выше, невозможно без реализации принципа 7).

Реализация СОБ Объекта предполагает противодействие актуальным угрозам нарушения безопасности Объекта, моделирование которых носит прогнозный характер, что можно сделать только при использовании принципа 8).

Особенности объектов в информационной сфере и их СОБ носят междисциплинарный характер, чему полностью соответствует принцип 9).

1.4. Методы системотехники

Все известные методы (процессы) системотехники (системной инженерии) предполагают итеративное применение процедур синтеза, анализа, оценки [6]:

1. Синтез включает формирование определённой совокупности требований к объекту системотехники со стороны заинтересованных сторон, описанных на языке функционирования. Основными элементами обеспечения синтеза являются команда разработчиков, компьютерно-ориентированные инструменты синтеза, а также результаты прикладных исследований и возможности использования известных технологий.
2. Анализ вариантов системных решений, относящихся к объекту системотехники, а также определение или предсказание его параметров. В целом, применение анализа — это необходимая, но не достаточная составляющая процедуры принятия решения о выборе проектного варианта объекта.
3. Оценка подразумевает, что каждый вариант решения (или альтернатива) оценивается в сравнении с другими вариантами, а также проверяется на соответствие требованиям заинтересованных сторон.

Набор методов системотехники в обобщенном виде, необходимых для создания результативной СОБ Объекта, может включать, как минимум, следующие действия:

- обеспечение надёжного проектной базы, включающей исходную информацию и требования, а также необходимые инструменты для совместной работы множества специалистов над мультидисциплинарной информацией в ходе создания СОБ Объекта и управления её жизненным циклом;
- точную оценку доступной информации и определение недостающей, необходимую для создания СОБ Объекта;
- проведение системного анализа для разработки проектных решений, отражающих поведение СОБ Объекта, которые должны соответствовать всем требованиям;
- проведение анализа компромиссных решений по создания СОБ Объекта для поддержки процесса принятия решений;
- создание исполняемых моделей для верификации и валидации работы СОБ Объекта.

Необходимо отметить, что перечисленные выше действия требуют проведения исследований, направленных на формализацию процессов создания СОБ Объекта, которые могут составить комплекс методов системотехники, относящихся к ОБ конкретных Объектов.

2. Процессный подход к обеспечению безопасности Объекта

Процессный подход в системотехнике как один из ее принципов [6] определяет требования к деятельности любой организации и ее объектов в виде ориентации процессов, реализуемых в организации, на конечный результат [13]. При этом понятие «процесс» определяется как совокупность взаимосвязанных или взаимодействующих видов деятельности, преобразующей контекст на входе в контекст на выходе процесса и требующей определенных ресурсов и управляющих воздействий (рис. 1) для получения намеченного результата[4].

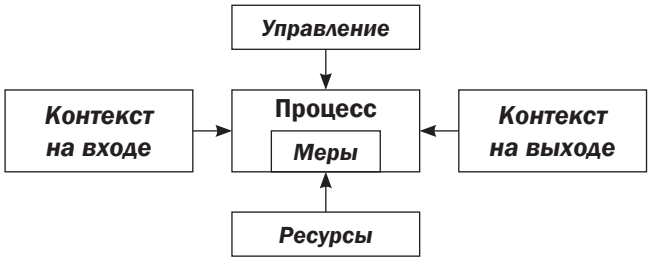


Рис. 1. Обобщенная структурная схема процесса

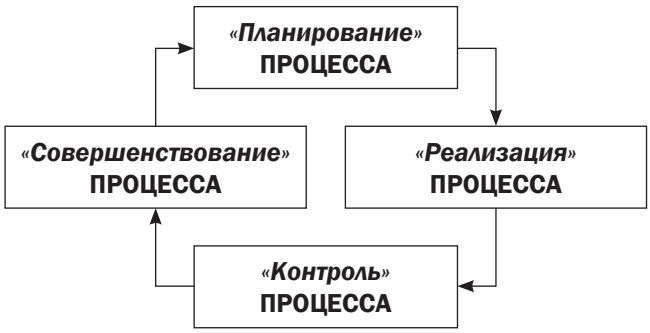


Рис. 2. Модель Деминга

При этом в отношении конкретного процесса достижение намеченного результата определяется в соответствии с циклической моделью Деминга [10] результативностью управления процессом на стадиях его «планирования», «реализации», «контроля» и «совершенствования» (рис. 1, рис. 2).

2.1. Процессная модель Организации

Если сам объект рассматривать как часть организации, то в соответствии с принципом системотехники 5) процессы обеспечения безопасности Объекта должны рассматриваться в связи с процессами Организации и другими процессами, реализуемыми в ней [13]. В данном случае представляется целесообразным прежде всего рассмотреть процессную модель Организации, состоящую из отдельных процессов, отнесенных к определенным объектам Организации (рис. 3).

Интересы любой организации достигаются через деятельность, которую в терминах процессного подхода можно представить в виде совокупности следующих трех групп высокоуровневых процессов [13]: основные процессы (процессы основной деятельности, формирующие бюджет организации, или бизнес-процессы); вспомогательные процессы; процессы управления.

К основным процессам можно отнести (рис. 3) деятельность по оказанию бизнес-услуг, по производству продукции, по выполнению обязательств по договору, по обработке информации ограниченного доступа (если необходима соответствующая лицензия) и др.

Вспомогательные процессы классифицируются по видам обеспечения основных процессов. Например, к вспомогательным процессам можно отнести (рис. 3) деятельность по бухгалтерскому облуживанию, по планированию деятельности организации, по осуществлению контроля и др.

Рис. 3. Структура процессной модели Организации

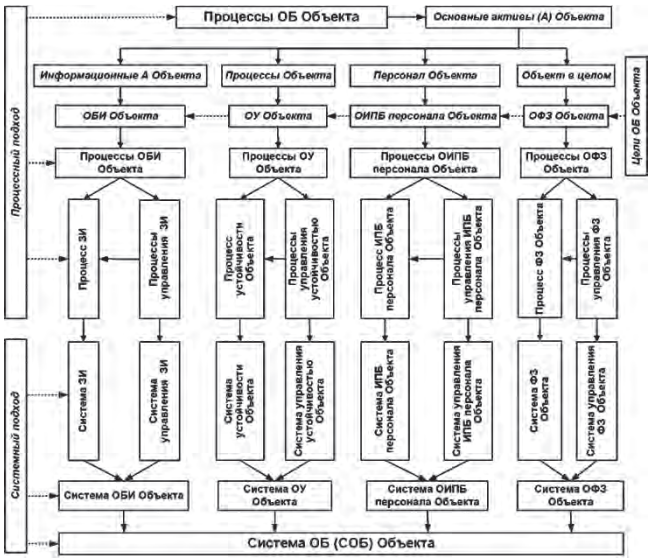


Рис. 4. Структура процессной модели СОБ Объекта

Процессы ОБ относятся к вспомогательным процессам [13], которые, прежде всего, связывают с объектами, относящимся к основными или вспомогательными процессам (рис. 3). Причем, как правило,

такими объектами являются те, которые реализуют процессы автоматизации обработки информации (тоже вспомогательные процессы) с использованием современных информационных технологий (ИТ-сервис). К таким объектам можно отнести информационные системы, автоматизированные системы (АС), объекты информатизации, АС управления (АСУ), АСУ технологическим процессом (АСУ ТП), объекты систем интернет-вещей, киберфизические системы и т.д.

Процессы управления в организации играют особую роль. Совокупность процессов управления в организации образуют процессы, относящиеся к различным объектам организации и к различным процессам организации. В соответствии с процессным подходом реализацией процесса управления в отношении к конкретному процессу достигается намеченный результат (результативность процесса). Это распространяется и на процессы ОБ.

2.2. Процессная модель обеспечения безопасности Объекта

Обеспечение безопасности Объекта в соответствии с принципом 2) системотехники необходимо связать с совокупностью процессов ОБ, относящихся к СОБ Объекта. Их структуру предлагается представить в виде процессной модели, показанной на рис. 4.

Совокупность процессов ОБ Объекта предлагается сформировать с учетом принципа системотехники 4) и необходимости достижения результативности при синтезе СОБ Объекта (основной метод системотехники), разделив их на четыре группы с учетом определения основных активов Объекта: информационные активы, процессы Объекта, персонал объекта и объект в целом. Это позволило разделить область ОБ Объекта на:

- обеспечение безопасности информации (ОБИ), связанной с сохранением необходимого состояния защищенности информации, обрабатываемой на Объекте;
- обеспечение функциональной устойчивости (ОУ) Объекта (его процессов);
- обеспечение информационно-психологической безопасности (ОИПБ) персонала Организации, имеющего отношение к Объекту, при деструктивном воздействии на него информации;
- обеспечение физической защиты (ОФЗ) Объекта с учетом его расположения (помещение, этаж, здание, территория Организации).

В данном случае ОБИ на Объекте, ОУ Объекта, ОИПБ персонала Объекта и ОФЗ Объекта можно использовать не только как совокупности процессов, но и как отдельные цели действий на Объекте, направленных на ОБ Объекта.

В каждой подобласти, которые формируют область ОБ Объекта, будет своя группа процессов безопасности (ПБ): процессы защиты информации, обрабатываемой на Объекте (ПЗИ); процессы устойчивости Объекта (ПУ); процессы ИПБ персонала Объекта (ПИПБ); процессы ФЗ Объекта (ПФЗ).

В соответствии с процессным подходом (рис. 2, рис. 3) и принципом 2) системотехники, реализация каждого процесса предполагает использование

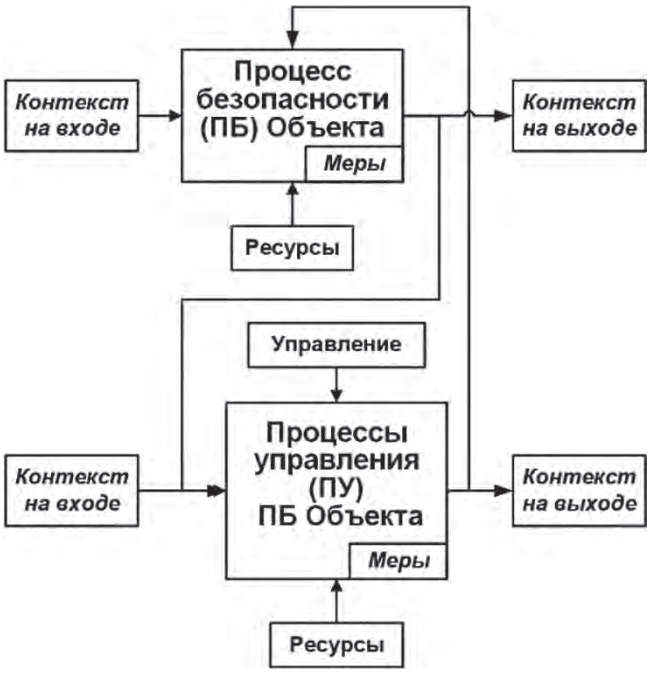


Рис. 5. Процессный подход к ОБ Объекта

Рис. 6. Процессный подход к поддержке СОБ Объекта

своих мер (технических и/или организационных), а результативность каждого процесса на стадиях его планирования, реализации, контроля и совершенствования требует применения соответствующих процессов управления: процессом ЗИ (УПЗИ); процессом устойчивости Объекта (УПУ); ИПБ персонала Объекта (УПИПБ); ФЗ Объекта (УПФЗ).

Необходимо отметить, что реализация процессов управления конкретным процессом ОБ Объекта будет зависит не только от особенностей Объекта и его окружения, но и от результатов реализации самого процесса (рис. 5). Речь идет об адаптивном управлении, что в полной мере соответствует принципу 5) системотехники. Процессам управления процесса ОБ Объекта необходимы свои меры, ресурсы и свое управление. В данном случае можно констатировать факт, что реализуется не только процессный, но и управленческий подход.

3. Системный подход к обеспечению безопасности Объекта

В соответствии со сформулированными концепциями системотехники [6,7]. основным ее понятием является «система», что позволяет утверждать, что при рассмотрении проблем обеспечения безопасности объектом исследования будет СОБ Объекта, которая может быть рассмотрена динамически и статически.

3.1. Динамическое представление СОБ Объекта

Динамический подход к СОБ – это объединение связанных процессов ОБ Объекта, целью которых является сохранение основных активов Объекта. Анализ структуры предложенной в данной работе процессной модели СОБ Объекта (рис. 4) приводит к структуризации СОБ Объекта на подсистемы, выделив в ней систему ОБИ (СОБИ), систему ОУ (СОУ), систему ОИПБ персонала (СОИБП) и систему ОФЗ Объекта:

СОБ = СОБИ + СОУ + СОИПБ + СОФЗ.

Каждая подсистема состоит системы, объединяющей соответствующие процессы безопасности – ПБ (ПЗИ, ПУ, ПИПБ, ПЗИ), и системы, в которые включаются процессы управления процессами безопасности – УПБ (УПЗИ, УПУ, УПИПБ, УПЗИ):

СОБИ=СПЗИ+СУПЗИ; СОУ=СПУ+СУПУ;
СОИПБ=СПИПБ+СУПИПБ; СОФЗ=СПФЗ+СУПФЗ.

С учетом этого можно обосновано утверждать, что при динамическом представлении СОБ Объекта целесообразно рассматривать ее как совокупность системы процессов безопасности (СПБ) и системы управления процессами безопасности (СУПБ):

СОБ = СПБ + СУПБ,

где: **СПБ = СПЗИ+СПУ+СПИПБ+СУПИПБ+ СПФЗ;**
СУПБ=СУПЗИ+СУПУ+СУПИПБ+СУПФЗ.

Связь процессов безопасности (ПБ) из СПЗИ, СПУ, СПИБП и СПФЗ с соответствующими процессами управления (ПУ) процессом безопасности, входящими в системы СУПЗИ, СУПУ, СУПИБП и СУПФЗ, определяет процессный подход к ОБ Объекта (рис. 5).

В зависимости от целей ОБИ Объекта при решении пракритских задач может быть учтены отдельные подсистемы или различные их комбинации вплоть до учета всех подсистем, что соответствует известному методу системотехники – применению процедур синтеза [6].

3.2. Статическое представление СОБ Объекта

Статический подход к СОБ Объекта связан с представлением этой системы в виде предмета, обладающего определенными внешними или внутренними свойствами (характеристиками). При этом важным является поддержка СОБ Объекта (как предмета) на стадиях ее проектирования, реализации, контроля и совершенствования. Причем поддержку СОБ Объекта в виде действий (процессов) и управления этими действиями предлагается описать в рамках процессного подхода, иллюстрируемого рисунком 6, а жизненный цикл СОБ Объекта, как фундаментальной основы практики системотехники [9], также может быть описан моделью Деминга (рис. 2).

Для формирования совокупности процессов поддержки СОБ Объекта можно воспользоваться опытом системного подхода к управлению ИБ[6], который дает основание разделить процессы поддержки (ПП) СОБ Объекта на следующие группы (ГПП): «Контекст» (А), «Руководство» (Б), «Планирование» (В), «Ресурсы» (Г), «Эксплуатация» (Д), «Контроль» (Е), «Улучшение» (Ж). Перечень типовых ПП, распределенных по этим группам, с привязкой к результату реализации конкретного процесса (контекст на выходе – Квых), этапу жизненного цикла (ЭЖЦ) СОБ Объекта («Планирование» – П; «Реализация» – Р; «Контроль» – К; «Совершенствование» – С) и к соответствующим процессам управления – ПУ (рис. 6), приведен в табл. 1 со следующими обозначениями в отношении СОБ Объекта: УД – управление документированием; УА – правление активами Объекта; УР – управление рисками; УОНОБ – управление обеспечением непрерывности обеспечения безопасности (ОНОБ) Объекта; УФиМР – управление финансовыми и материальными ресурсами (ФиМР); УП – управление персоналом Организации; УКП – управление компетентностью персонала Организации; УПБ – управление процессами ОБ Объекта; УИнБ – управление инцидентами безопасности Объекта; УИз – управление изменениями структуры Объекта и систем, относящихся к его безопасности.

6 ГОСТ Р ИСО/МЭК 27001-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности.

Таблица 1.

Типовые процессы поддержки СОБ Объекта

ГПП	Типовые ПП	Квых	ЭЖЦ	ПУ ПП
А	Определение контекста на входе (внешнего и внутреннего)	Описание особенностей Объекта и Организации с учетом внешних и внутренних факторов	П	УД
	Описание процессов, реализуемых Объектом и Организацией	Процессные модели Организации и Объекта	П	УД
	Идентификация активов Объекта	Описание активов Объекта и их уязвимостей	П	УА, УД
	Определение потребностей и ожиданий заинтересованных сторон в отношении к ОБ Объекта	Описание потребностей и ожиданий заинтересованных сторон в отношении к ОБ Объекта	П	УД
	Определение требований к СОБ и области ее функционирования	Описание требований к СОБ Объекта и области ее функционирования	П	УД
Б	Определение ролей в отношении ОБ Объекта, порядка их распределения и назначения в Организации	Ролевая модель Организации в отношении ОБ Объекта	П	УД
	Разработка политики ОБ Организации	Политика ОБ Организации	П	УД
В	Анализ угроз безопасности Объекта, оценка и оценивание рисков нарушения безопасности Объекта	Перечень актуальных угроз безопасности Объекта	П	УД, УР
	Описание угроз безопасности Объекта	Модель угроз и модель нарушителя безопасности Объекта	П	УД
	Определение ПБ СОБ, обработка рисков нарушения безопасности Объекта	Перечень ПБ СОБ Объекта	П	УД, УР
	Разработка политик ОБ Объекта	Политики ОБ Объекта	П	УД
	Разработка программы ОНБ Объекта	Программа ОНБ Объекта	П	УОНБ
Г	Выделение финансовой и материальной (ФиМ) поддержки СОБ	Финансовая и материальная поддержка СОБ	П, Р, К, С	УФиМР, УД
	Подбор персонала Организации для ОБ Объекта	Персонал Организации для ОБ Объекта		УП
	Проведение инструктажа и обучения персонала для ОБ Объекта	Поддержка необходимого уровня осведомленности и компетентности персонала для ОБ Объекта		УКП
	Документирование действий, направленных на поддержку СОБ Объекта	Формирование базы внутренних документов, относящихся к ОБ Объекта		УД
Д	Реализация ПБ Объекта	Результаты выполнения политик ОБ Объекта	Р	УПБ, УД
	Реализация процессов управления инцидентами нарушения безопасности (ИнБ) Объекта	Результаты выполнения политики управления ИнБ Объекта	Р	УИнБ
	Реализация процессов ОНОБ Объекта	Результаты выполнения программы ОНОБ Объекта	Р	УОНОБ, УД
Е	Мониторинг событий безопасности Объекта	Выявление ИНБ Объекта	К	УИнБ, УД
	Аудит СОБ Объекта	Выявление нарушений положений политик ОБ Объекта	К	УК, УД
	Самооценка ОБ Объекта			
	Анализ ОБ Объекта со стороны руководства			
Ж	Принятия решения по совершенствованию СОБ	Планы по совершенствованию СОБ	С	УИз, УД
	Реализация процессов по совершенствованию СОБ	Выполнение планов по совершенствованию СОБ	П или Р	УИз, УД

Анализ информации, приведённой в табл. 1, позволяет сформировать систему поддержки СОБ (СПОБ) Объекта, включив в нее систему процессов поддержки СОБ (СППОБ) и систему управления процессами поддержки СОБ (СУППОБ):

СПОБ = СППОБ + СУППОБ.

3.3. Комплексная система обеспечения безопасности Объекта

Следующий этап применения системотехники при обеспечении безопасности Объекта связан с объединением динамического и статического подходов к СОБ Объекта, что позволяет сформировать комплексную систему безопасности Объекта (КСБ), объединяющую систему обеспечения безопасности (СОБ) и систему ее поддержки (СПОБ): **КСБ = СОБ + СПОБ**.

Если выделить в КСБ в отдельные системы процессы обеспечения безопасности и процессы их поддержки (СПБ и СППОБ), процессы управления процессами безопасности и процессы управления поддержки СОБ (СУПБ и СУППОБ), то можно определить КСБ следующим образом:

КСБ = КСПБ + КСУБ,

где: **КСПБ = СПБ + СППОБ; КСУБ = СУПБ + СУППОБ**.

Результатом применения в рамках системотехники системного подхода является обоснованное разделение всех процессов безопасности Объекта на две группы (КСПБ и КСУБ). Причем формирование второй группы полностью соответствует современному управленческому подходу к обеспечению безопасности конкретных объектов (например, для обеспечения ИБ[2]) и отражает фундаментальные особенности безопасности [3]. Структура КСУБ показана на рис. 7.

Рис. 7. Структура комплексной системы управления безопасностью (КСУБ) Объекта

КСУБ Объекта, входящего в Организацию, обеспечивает системный подход к созданию, внедрению, функционированию, мониторингу, анализу, поддержке и улучшению процессов безопасности Объекта (КСПБ) для достижения бизнес-целей Организации. В данном случае предлагается следующее определения понятия КСУБ Объекта:

Комплексная система управления безопасностью (КСУБ) Объекта *– это часть общей системы управления Организации, основанная на риск-ориентированном подходе (на оценке бизнес-рисков), предназначенная для разработки, внедрения, эксплуатации, постоянного контроля, анализа, поддержания и улучшения безопасности Объекта, и включающая необходимые для этого организационную структуру, политику, планирование действий, обязанности, установившийся порядок, процедуры, процессы и ресурсы.*

4. Подготовка профессионалов в области обеспечения безопасности Объекта

Реализация системотехнического подхода к ОБ Объектов предполагает привлечение специалистов различных профилей, подготовка которых тоже должна иметь системный характер. Речь идет об отдельном направлении инженерной подготовки «Обеспечение безопасности объектов в информационной сфере», с единой квалификацией «инженер-системотехник». Это направление может объединять, как минимум, четыре специальности: «Обеспечение безопасности информации», «Обеспечение устойчивости объектов в информационной сфере», «Обеспечение информационно-психологической безопасности объектов в информационной сфере», «Обеспечение физической защиты объектов в информационной сфере». Эти специальности будут иметь общий цикл фундаментальных дисциплин (математика, физика, информатика, основы системотехники, основы управления, основы психологии), общий цикл общепрофессиональных дисциплин (методология обеспечения безопасности объектов, современные информационные технологии, управление обеспечением безопасности объектов, объекты в информационной сфере) и цикл профессиональных дисциплин (отражают специфику отдельной специальности). Причем каждая специальность может иметь специализации, разделение которых возможно на основе выбора отдельного вида объекта в информационной сфере.

Следует отметить, что в настоящее время существует укрупненное направление подготовки специалистов по защите информации 10.00.00 «Информационная безопасность». Название направления и номенклатура специальностей, входящих в это направление, сформировались в контексте развития этого образовательного направления в условиях отсутствия устоявшейся понятийной базы данной предметной области. Например, понятие «информационная безопасность» прежде всего отражает

аспекты, связанные с безопасностью объекта от воздействия информации, что соответствует только информационно-психологической безопасности. Следствием этого является отсутствие у данного направления необходимой методологической базы.

Выводы

В работе впервые рассмотрены основы методологии обеспечения безопасности объектов, использующих современные информационные технологии (Объектов), базирующиеся на понятиях, концепции, принципах и методах системотехники.

В рамках системотехники был развит процессный, системный и управленческий подходы к ОБ Объектов, основанные на разработанных процессных моделях Организации, Объекта как части Организации и его систем ОБ.

В работе дано обоснование выделения среди процессов ОБ Объекта четырех групп процессов: обеспечение безопасности информации, обеспечение устойчивости Объекта, обеспечение информационно-психологической безопасности персонала Объекта и обеспечение физической защиты Объекта с учетом необходимости обеспечить состояние защищенности основных активов Объекта (информационных активов, процессов, персонала и Объекта в целом соответственно) и формулирования отдельных целей ОБ Объекта. В каждой из этих групп в рамках развития процессного подхода были выделена часть процессов, реализация которых направлена на достижения необходимого состояния защищенности активов Объекта, и часть процессов управления процессами из первой части, которые должны обеспечить необходимую результативность реализации процессов из первой части на стадиях их планирования, реализации, контроля и совершенствования. При этом показан адаптивный характер управления такими процессами.

С учетом выделенных групп процессов была предложена структура систем, входящих в СОБ Объекта (динамическое представление СОБ). Ее анализ показал, что важным дополнением к СОБ Объекта с учетом системотехнического подхода является планирование, реализация, контроль и совершенствование процессов поддержки СОБ Объекта как предмета (статическое представление СОБ), что привело к формированию системы поддержки СОБ (СПОБ) со своими процессами поддержки и процессами их управления и к формированию комплексной системы безопасности (КСБ) Объекта, состоящей из СОБ и СПОБ, которую также можно представить совокупностью комплексной системы процессов безопасности (КСПБ) и комплексной системы управления безопасностью (КСУБ). Учитывая важность КСУБ Объекта в работе была определена ее структура и было сформулировано определение понятия, относящиеся к КСУБ.

Использование системотехники при ОБ Объекта позволило на единой методологической базе обосновать направление подготовки профессионалов в области ОБ Объектов, определив их квалификацию (инженер-системотехник) и возможный перечень специальностей, входящих в это направление. Таким образом результаты работы также имеют практическую значимость для образовательной области, особенно на этапе проходящей в настоящее время реформы системы высшего образования.

Применение системотехники в рамках решении задач ОБ Объекта позволило осуществить системный (целостный) подход, необходимый для проведения исследований, проектирования, реализации и развития систем обеспечения безопасности конкретных Объектов. Предлагаемые в работе решения носят обобщенный характер и не противоречат существующему в настоящее время подходу, связанному с обеспечением информационной безопасности.

Литература

1. *Толстой, Александр И. Обеспечение безопасности объектов в информационной сфере. Безопасность информационных технологий, [S.l.], т. 31, № 3, с. 105–123, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1677. DOI: http://dx.doi.org/10.26583/bit.2024.3.05.*
2. *Толстой, Александр И. Систематика понятий в области информационной безопасности. Безопасность информационных технологий, [S.1], т. 30, № 1, с.130–148, 2023. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1478. DOI: http://dx.doi.org/10.26583/bit.2023.1.10.*
3. *Обеспечение информационной безопасности бизнеса / В. В. Андрианов, С. Л. Зефиров, В. Б. Голованов, Н. А. Голдуев. Под общей ред. А. П.Курило. — 2-е изд., перераб. и доп. — М.: Альпина Паблишерз, 2011. — 373 с.*
4. *Кравченко Сергей. И. Безопасность социотехнических систем// НБИ технологии. 2018. Т. 12. № 2, с. 20-24. DOI: https://doi.org/10.15688/NBIT.jvolsu.2018.2.3.*
5. *Корганова О. Г., Панфилова И. Е. Модель управления информационными рисками социотехнической системы на основе поведенческих особенностей человека // Сборник научных трудов НГТУ. – 2020 – № 1–2 (97). – С. 89–98. – DOI: 10.17212/2307-6879-2020-1-2-89-98.*
6. *Батоврин В. К., Голдберг Ф. Н., Александров П. С., Малер Е. А. Системная инженерия / Гуманитарный портал: Концепты [Электронный ресурс]// Центр гуманитарных технологий, 2002–2023 (последняя редакция: 08.12.2023). URL: https://gtmarket.ru/concepts/7110.*
7. *Горохов В. Г. Методологический анализ системотехники. – Москва: Радио и связь, 1982. 162 с.*
8. *Николаев, В. И. Системотехника: методы и приложения / В. И. Николаев, В. М. Брук. – Л.: Машиностроение, Ленингр. отд-ние, 1985. – 199 с.*
9. *Blanchard B. S., Fabrycky W. J. Systems Engineering and Analysis. — Prentice Hall, 2006.*

10. Нив Г. Пространство доктора Деминга. М.: Альпина Бизнес Букс, 2007.
11. Hitchins D. What are the General Principles Applicable to Systems? — INCOSE INSIGHT. — V. 12, Issue 4. — December 2009. — pp. 59–64).
12. Boehm B. et al. Principles for Successful Systems Engineering. — Procedia Computer Science — № 8, 2012. — pp. 297–302.
13. Аудит информационной безопасности / А. П. Курило, С. Л. Зефиров, В. Б. Голованов и др. – М.: Издательская группа «БДЦ-пресс», 2006. – 304 с.

SYSTEM ENGINEERING FOR ENSURING SECURITY OF OBJECTS IN THE INFORMATION SPHERE

Tolstoy A. I.[7]

Abstract. *The article considers the fundamentals of the methodology for ensuring the security of objects using modern information technologies (Objects), based on the concepts, principles and methods of systems engineering. Within the framework of systems engineering, the process, system and management approaches to ensuring the security of Objects were developed, based on the developed process models of the Object as a part of the Organization, the Object itself and its security ensuring systems (SES). In the work, four groups of processes are substantiated among the processes of ensuring the security of the Object – this is ensuring of information security, resilience, information and psychological security of personnel and physical protection of the Object, taking into account the need to ensure the secure state of the main assets of the Object and the formulation of separate goals of ensuring the security of the Object. In each of these groups, within the framework of the development of the process approach, a part of the processes were identified, the implementation of which is aimed at achieving the required secure state of the assets of the Object, and a part of management processes for the processes from the first part, which should ensure the necessary effectiveness at the stages of their planning, implementation, control and improvement. At the same time, the adaptive nature of the management of such processes is shown. Taking into account the identified groups of processes, a structure of systems included in the Object's SES and a structure of the system of its support processes (dynamic and static representation of the SES respectively), as well as a structure of the Object's integrated SES were proposed. The usage of systems engineering in the Object's security ensuring allowed us to substantiate the direction of training professionals in the field of Object's security ensuring on a single methodological basis, defining their qualifications (systems engineer) and a possible list of specialties included in this direction. The usage of systems engineering in solving Object's security ensuring problems allowed us to implement a systemic (integrated) approach necessary for conducting research, designing, implementing and developing SESs for specific Objectss. The solutions proposed are generalized and do not contradict the currently existing approach related to ensuring information security.*

Keywords: *methodology, concept, principles, method, model, process, system, asset, management, information security, resilience, information and psychological security, physical security.*

References

1. Tolstoy, Alexandr I. Obespechenie bezopasnosti ob'ektov v informatcionnoi sferi. Bezopasnost informacionnih tehnologiy, v. 31, no 3, p. 105–123, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1677. DOI: http://dx.doi.org/10.26583/bit.2024.3.05.
2. Tolstoy, Alexandr I. Sistematika poniytii v oblasti informacionnoy bezopasnosti. Bezopasnost informacionnih tehnologiy, [S.l.], v. 30, no. 1, p. 130–148, 2023. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1478. DOI: http://dx.doi.org/10.26583/bit.2023.1.10.
3. Obespechenie informacionnoi bezopasnosti biznesa / V. V. Andrianov, S. L. Zefirov, V. B. Golovanov, N. A. Golduev.- M.: Alpina Паблишерз, 2011. – 373 p.
4. Kravchenko S. I. Bezopasnost sociotehnicheskih system// NBI tehnologii. 2018. v. 12. № 2, p. 20–24. DOI: https://doi.org/10.15688/NBIT.jvolsu.2018.2.3
5. Korganova O. G., Panfilova I. E. Model upravleniya informatsionnymi riskami sotsiotekhnicheskoi sistemy na osnove povedencheskikh osobennostei cheloveka [Model of information risk management of a sociotechnical system based on human behavioral features]. Sbornik nauchnykh trudov Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta = Transaction of scientific papers of the Novosibirsk state technical university, 2020, no. 1–2 (97), pp. 89–98. DOI: 10.17212/2307-6879-2020-1-2-89-98.
6. Batovrin V. K., Goldberg F. N., Aleksandrov P. S., Maler E. A. Sistemnaia inhzeneria / Gumanitarnii portal: Koncepti [Elektrronnii resurs] // Centr gumanitarnih tehnologii, 2002–2023 (posledniy redakciya 20.08/2024). URL: https://gtmarket.ru/concepts/7110.
7. Gorohov V. G, Metodologicheskiy analiz sistemotehniki. – Radio i sviyz, 1982. 162 p.
8. Nikolaev V. I., Bruk V. M. Sistemotehnika: metodi i prilozheniy. – L.: Mashinostroenie, 1985.– 199 p.
9. Blanchard B. S., Fabrycky W. J. Systems Engineering and Analysis. – Prentice Hall, 2006.
10. Niv G. Prostranstvo doktora Deminga. M.: Alpina Niznes Buks, 2007
11. Hitchins D. What are the General Principles Applicable to Systems? – INCOSE INSIGHT. – V. 12, Issue 4. – December 2009.– pp. 59–64).
12. Boehm B. et al. Principles for Successful Systems Engineering. – Procedia Computer Science – № 8, 2012. – pp. 297–302.
13. Audit informacionnoy bezopasnosti / A. P.Kurilo, S. L. Zefirov, V. B. Golovanov i dr. – M.: Izdatelskaya gruppa «BDC-press», 2006.– 304 p.

7 Alexandr I. Tolstoy, Ph.D, Associate Professor, National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow. E-mail: AITolstoj@mephi.ru, http://orcid.org/0000-0001-9265-1510

ЭВОЛЮЦИЯ И НАПРАВЛЕНИЯ РАЗВИТИЯ ТЕХНОЛОГИЙ МАСКИРОВАНИЯ КОНФИДЕНЦИАЛЬНЫХ РЕЧЕВЫХ СООБЩЕНИЙ

Дураковский А. П.[1], Дворянкин С. В.[2], Дворянкин Н. С.[3]

DOI: 10.21681/2311-3456-2024-5-58-66

Цель исследования: *анализ методов и алгоритмов технического закрытия речевой информации в сетях и системах голосовой связи, оценка направлений и перспектив развития технологий речевого маскирования с машинным обучением.*

Методы исследования: *прикладного системного анализа, цифрового спектрально-временного анализа, цифровой обработки сигналов и изображений, образного анализа спектрограмм, машинного обучения.*

Результаты исследования: *обозначены проблемы обеспечения безопасности конфиденциальной голосовой связи в современных условиях. Приведен обзор методов речевой защиты, применяемых на практике в общедоступных каналах голосовой связи. Рассмотрены традиционные и перспективные алгоритмы маскирования речевых сообщений, способы их реализации. Отмечены преимущества последних.*

Научная новизна: *предложены новые способы технического маскирования речи на основе модификации и реконструкции изображений динамических спектрограмм с использованием методов машинного обучения.*

Практическая значимость: *предложены эффективные алгоритмы речевого маскирования. Полученные результаты позволят расширить возможности существующих решений по защите речевой информации в системах и сетях голосовой связи и проектировать более эффективные на основе изложенных подходов.*

Ключевые слова: *информационная безопасность, защита речевой информации, образный анализ-синтез, техническое закрытие речи, речеподобный сигнал, машинное обучение.*

Введение

Современное состояние проблемы защиты речевой информации (РИ) характеризуется постоянным расширением арсенала средств негласного съема и перехвата акустических (речевых) сигналов, технические характеристики и способы применения которых неуклонно совершенствуются[4,5,6].

В связи с этим особый интерес представляют исследования, направленные на выявление принципиально новых подходов к защите речевой информации от НСД, позволяющих существенно усложнить процесс несанкционированного перехвата речевых и попутных полезных акустических фоновых сигналов из каналов голосовой связи (КГС).

Безопасность голосовой связи при передаче конфиденциальных речевых сообщений по каналам коммуникаций основывается на использовании большого количества методов и средств технического закрытия речевого сигнала (РС)[7]. Они преобразуют характеристики речи таким образом, что она становится неразборчивой, непонятной, неузнаваемой для подслушивающего лица, перехватившего обработанное речевое сообщение. Или вообще скрывается факт самой передачи речевого сообщения, которое тем не менее в таком скрытном виде доходит до своего абонента, адресата.

Сегодня внимание исследователей и потребителей обращено на быстрые алгоритмы маскирования, адаптированные под большинство мобильных устройств и приложений, способные в режиме реального времени преобразовывать речевую информацию в защищенный формат[8], прежде всего делая ее неразборчивой или с полным отсутствием в канале передачи признаков исходной защищаемой речи.

1 Дураковский Анатолий Петрович, кандидат технических наук, доцент, доцент кафедры стратегических информационных исследований НИЯУ МИФИ, директор Аттестационно-испытательного центра информационной безопасности и систем защиты информации НИЯУ МИФИ, г. Москва, Россия. E-mail: apdurakovskiy@mephi.ru

2 Дворянкин Сергей Владимирович, доктор технических наук, профессор, профессор кафедры стратегических информационных исследований НИЯУ МИФИ, заведующий лабораторией защиты и обработки аудиовизуальной информации МГЛУ, г. Москва, Россия. E-mail: svdvoryankin@mephi.ru. Https://orcid.org/0000-0001-6908-0676

3 Дворянкин Никита Сергеевич, аспирант НИЯУ МИФИ, г. Москва, Россия. E-mail: nik.dvrn@gmail.com

4 Дворянкин С. В. Маскирование речевой информации: перспективные методы и средства. С. В. Дворянкин, А. А. Мишуков // Спецтехника и связь. – 2009. – № 3.

5 Мишуков, А. А. Образный анализ и маскирование речевой информации / А. А. Мишуков, Р. А. Устинов, Н. С. Дворянкин // Информационные технологии, связь и защита информации МВД России. – 2012. – Вып. 2.

6 Карпов, А. П. Разработка маскиратора аналоговых речевых сигналов / А. П. Карпов // Вестник Пензенского государственного университета. – 2016. – № 1 (13). – С. 62–64.

7 Дворянкин С. В., Девочкин Д. В. Методы закрытия речевых сигналов в телефонных каналах. // Защита информации. Конфидент. – 1995. – №5. – 45–59с.

8 Сперанский В. С., Клинцов О. И. Методы технического закрытия речевых сообщений // T-Comm. 2011. №9. URL: https://cyberleninka.ru/article/n/metody-tehnicheskogo-zakrytiya-rechevyh-soobscheniy (дата обращения: 15.06.2024).

Традиционные способы технического закрытия речи, области применения

Различают два основных класса способов защиты речевого сигнала в каналах коммуникаций от НСД. Первый, аналогово-цифро-аналоговый или просто аналоговый, относится к техническому закрытию и заключается в создании смеси защищаемого РС с помехой (маскировании) и-или в перемешивании (скремблировании) фрагментов исходного РС некоторым образом, делая речь неразборчивой. Это делается путем изменения соотношений между временем, амплитудой и частотой исходного сигнала.

Второй класс способов, криптографический, состоит в преобразовании речевого сигнала в цифровую форму, к которой применимы стандартные методы дискретного шифрования[9].

По некоторым оценкам в последнее время сфера применения маскирующих и скремблирующих алгоритмов технического закрытия, казалось бы, начала сокращаться. Это объяснялось улучшением качества каналов голосовой связи (КГС), ростом производительности и удешевлением привлекаемых вычислительных ресурсов, появлением экономичных «легковесных» криптографических алгоритмов, что существенно продвинуло применение в засекреченной цифровой связи речевых шифраторов.

Тем не менее, аналогово-цифро-аналоговое скремблирование до сих пор может и используется там, где применение цифровых систем закрытия речи затруднено из-за наличия возможных ошибок при передаче и сжатии данных в каналах связи с плохой пропускной способностью. Например, наземные линии связи с плохими техническими характеристиками, отечественные каналы связи для телефонов общего пользования, каналы дальней радиосвязи, особенно КВ-диапазона[10].

Таким образом, речевые маскираторы и скремблеры до сих пор применяются там, где невозможно, по ряду причин, использовать шифраторы. Кроме того, концептуальные принципы, понятия и решения, заложенные в скремблирующие и маскирующие алгоритмы, используемые в КГС, также, можно распространить на другие области защиты речевой информации. Например, на шумоподавление и реконструкцию искаженных РС, речеподобные помехи в системах активной акустической защиты помещений для конфиденциальных переговоров [1, 2, 3].

И наконец, с ростом и удешевлением вычислительного ресурса существующий научный задел создает основу разработки нового поколения устройств технического закрытия РС (новые маскираторы), имеющих более высокую степень защищенности близкую к шифраторам, улучшенные качество и разборчивость восстановленной речи близкое к аналоговым скремблерам, достаточную экономичность и простоту реализации, скрытность передачи РС и практическое отсутствие признаков защищаемой речи, по которым в отложенном режиме она могла бы частично быть восстановлена злоумышленником (ЗЛ) [3, 4].

Классификация существующих методов технического закрытия речи

Существующие средства защиты речевой информации в КГС, такие как маскираторы и скремблеры, уменьшают возможности устройств несанкционированного перехвата и прослушивания РС. Они позволяют пользоваться открытыми каналами связи, защищая передаваемую РИ от несанкционированного доступа (НСД) со стороны ЗЛ, работать в асинхронным режиме, обеспечивая при этом хорошее качество звучания РС в каналах с помехами и плохой пропускной способностью. Однако они менее стойкие, чем речевые шифраторы, хотя более экономичны при изготовлении и применению.

Классификация наиболее часто встречаемых и хорошо изученных видов скремблеров представлена в работе[11]. Помимо описанных там традиционных методов технического закрытия (скремблирования) в существующих устройствах речевого закрытия применяются различные методы и алгоритмы цифровой обработки сигналов [4, 5] как известные, на основе цифровых фильтров и преобразования Фурье, так и оригинальные, например, связанные с обработкой изображений узкополосных спектрограмм [3].

Более широкая классификация существующих методов технического закрытия (скремблирования и маскирования) представлена в работе[12] (см. рис. 1).

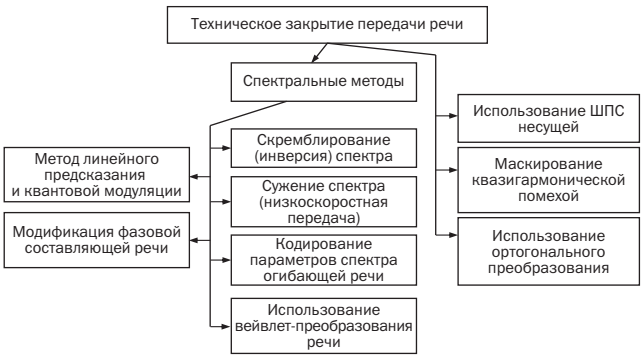


Рис. 1. Классификация современных методов технического закрытия

9 Барсуков В. С., Дворянкин С. В., Шеремет И. А. Безопасность связи в каналах телекоммуникаций. – М.: Электронные знания, 1992–1993. – 122 с.

10 Петраков А. В., Лагутин В. С. Утечка и защита информации в телефонных каналах. – М.: Энергоатомиздат, 1998. 317 с.

11 Петраков А. В., Лагутин В. С. Утечка и защита информации в телефонных каналах. – М.: Энергоатомиздат, 1998. 317 с.

12 Сперанский В. С., Клинцов О. И. Методы технического закрытия речевых сообщений // T-Comm. 2011. №9. URL: https://cyberleninka.ru/article/n/metody-tehnicheskogo-zakrytiya-rechevyh-soobscheniy (дата обращения: 15.06.2024).

Разнообразие представленных на рисунках методов речевого закрытия подтверждает тезис о том, что в настоящее время, в связи с развитием средств вычислительной техники, широким распространением общедоступных каналов передачи аудиоданных в цифровом медиа пространстве, появлением доступных решений в сфере применения методов машинного обучения к аудио обработке, – сформировалась необходимость в разработке эффективных и экономичных средствах технической защиты речевых сообщений, передаваемых в цифровом виде. Эту нишу вполне могли бы занять средства защиты РИ в КГС, построенные на основе новых методов маскирования речевых сообщений и удовлетворяющие современным требованиям.

Требования к перспективным маскираторам речи

Востребованный сегодня тип маскираторов – это асинхронные устройства защиты РИ, имеющие в своей основе такие методы и алгоритмы как: создание полезной смеси защищаемого РС с аддитивной помехой (в том числе речеподобной); изменение спектральной огибающей исходного РС; не требующие обязательной схемы (блока) синхронизации, которая необходима как при скремблировании, так и при дискретизации с шифрованием; практическое отсутствие в маскируемом сигнале признаков исходного РС, по которым методами шумопонижения и реконструкции может быть восстановлена речевая разборчивость [6–17].

В этой связи особый интерес представляют возможности перспективных разрабатываемых маскираторов с использованием решений машинного обучения и технологий синтеза речеподобных сигналов (РПС) с заданными свойствами, объединяющие лучшие характеристики существующих маскираторов и скремблеров и добавляющие новые варианты их использования [6–17].

Методологической основой создания такого рода устройств может послужить уже выше упоминавшийся образный анализ-синтез РС [3, 4].

Последние методы, основанные на технологии образного анализа-синтеза, заключающегося в переходе от волнового представления РС к изображению динамических узкополосных спектрограмм – графическим образам (ГО), их обработке методами цифровой обработки изображений для решения прикладных задач и обратном переходе (синтезе) от нового изображения к новой волновой форме РС, – неплохо подходят для организации различных новых видов асинхронного маскирования РС, в том числе и ранее не известных.

Выбор показателей качества для объективной оценки алгоритмов асинхронного маскирования речи обусловлен наличием особенностей, возникающих при передаче РС по каналу связи.

Требования к алгоритмам асинхронного маскирования речи можно разбить на две основные группы:

- требования по ограничению доступа злоумышленника к речевой информации;
- требования по обеспечению качественного приема речевой информации получателем при наименьших, аппаратных затратах.

Первая группа требований подразумевает создание наихудших условий для прослушивания линии связи злоумышленником, а вторая – обеспечение хорошего качества восстановленной речи при приемлемых технических характеристиках. Качество восстановленной речи, в свою очередь включающее понятия речевой разборчивости (РР) и ее узнаваемости, определяется устойчивостью алгоритма к различному виду помех, а также к рассогласованиям характеристик маскиратора и демаскиратора.

Очевидно, что злоумышленник будет поставлен в наихудшие условия, если не сможет обнаружить сам факт передачи речи в прослушиваемой линии связи. Тогда основными факторами, характеризующими снижение признаков речи в передаваемом сигнале, являются:

- уровень остаточной разборчивости прослушиваемого РС;
- однородное маскирование всех участков и элементов речи (определяются отсутствием пауз в прослушиваемом РС, а также отсутствием резких скачков громкости и тембра);
- «сглаживание» границ между акустически однородными участками РС.

Для определения речевой разборчивости (РР) в отдельном речевом канале среди используемых при организации сеанса связи целесообразно использовать показатели словесной речевой разборчивости, определенные для защищаемых помещений (ЗП) конфиденциальных переговоров от утечки, представленные в таблице 1[13].

Таблица 1.

Цели и критерии эффективности защиты речевой информации

Цель защиты	Критерий эффективности защиты
Скрытие факта ведения переговоров	$W_n \le 10\%$
Скрытие предмета переговоров	$W_n \le 20\%$
Скрытие содержания переговоров	$W_n \le 30\%$

13 Дворянкин С. В., Макаров Ю. К., Хорев А. А. Обоснование критериев эффективности защиты речевой. информации// Защита информации. Инсайд. – С. Петербург.: 2007. – № 2 – с. 18 – 25.

Для сохранения конфиденциальности переговоров в ЗП считается, что если уровень расчетной словесной разборчивости не превышает *20%* (см. табл. 1), то возможный технический канал утечки речевой информации (ТКУРИ) не требует проведения защитных мероприятий[14]. А если расчетная словесная разборчивость превышает *80%* (что соответствует *100%* фразовой), то перехватываемая ЗЛ по каналу ТКУРИ речевая информация будет полностью понятна нарушителю. Эти же выводы можно отнести и к телекоммуникационным каналам речевой связи, защищаемым от НСД. При необходимости в целях достижения еще большего уровня защиты РИ в каждом из используемых каналов можно дополнительно к известным использовать и новые алгоритмы речевого технического маскирования и наоборот, к новым добавлять старые.

Перспективные методы технического закрытия речевых сообщений

Как уже отмечалось методы цифрового шифрования часто достигают высокого уровня безопасности, но даже в современных системах связи со сжатием речи цифровое шифрование не всегда пригодно для использования. Цифровое шифрование, применяемое перед сжатием, может привести к снижению производительности связи, так как ошибки, вызванные методами сжатия с потерями, могут послужить причиной того, что речевые данные не могут быть правильно расшифрованы. Использование цифрового шифрования после сжатия речи требует серьёзных внутренних аппаратных и программных модификаций. Поэтому имеет смысл обратить внимание на новые методы и подходы, появляющиеся в техническом маскировании.

Современное техническое закрытие может быть удобно для защиты конфиденциальности речи в речевых коммуникациях. Какой-либо новый метод технического закрытия может быть использован перед отправкой речи в сети и системы связи без их модификаций, а на другом, приемном конце речевой коммуникации речь может быть восстановлена даже при наличии ошибок сжатия и ошибок канала.

Если алгоритм технического закрытия хорошо продуман, он будет способен даже обеспечить отсутствие признаков исходной речи, по которым она может быть восстановлена, высокую безопасность систем связи, сохраняя приемлемое качество расшифрованной речи при сравнительно низкой стоимости.

Рассмотрим примеры таких перспективных маскираторов.

14 Дворянкин С. В., Макаров Ю. К., Хорев А. А. Обоснование критериев эффективности защиты речевой. информации// Защита информации. Инсайд. – С. Петербург.: 2007. – № 2 – с. 18 – 25.

1. «Сепараторы»: рассечение-разнесение и расслоение речевой информации

Процесс управления РР в данном случае можно представить в виде некоего преобразования: рассечения и-или расслоения («слайдирования») графического образа (ГО) исходного РС на ряд других, мало похожих или совсем непохожих на исходный ГО, по которым синтезируются неразборчивые речеподобные сигналы (РПС), передаваемые в свои каналы связи на передающем конце, и сшивку или объединение их ГО с последующим синтезом в новый разборчивый сигнал на приемном.

Здесь речевой сигнал (РС) каждого из абонентов конфиденциальных переговоров рассматривается как совокупность и-или как сумма нескольких речеподобных сигналов, каждый из которых имеет свою РР со значением менее заданного уровня (нормы) и может быть передан другому собеседнику по своему отдельному каналу.

$$S(t) = \sum_{K} s_k(t) \qquad W_{s_k} \le W_n \qquad S(t) = \bigcup_{K} s_k(t) \qquad (1)$$

где $S(t)$ – исходный РС, $s_k(t)$ – речеподобные составляющие исходного РС, W_{s_k} – текущая РР для каждой речевой составляющей, а W_n – нормированное значение РР.

Такой отдельный РС, будучи возможно перехваченным в одном из контролируемых ЗЛ каналов связи уже не будет понятен нарушителю. У легального же пользователя на приемном конце все полученные по разным путям элементарные сигналы снова объединяются (сшиваются, склеиваются) по определенным правилам в один, теперь уже разборчивый сигнал.

Общая схема такой защищенной голосовой связи для двух абонентов и одно¬временно используемых ими 4-х каналов (3-и сотовых операторов «большой тройки» плюс канал VoIP) показана на рис. 2. Понятно, что эта модель может быть расширена на большее число используемых каналов и участников переговоров.

Класс методов разделения исходного РС на неразборчивые речеподобные составляющие весьма широк: от полосовой фильтрации по группам равно артикуляционных полос до спектрально-временной обработки фонетической функции (динамической огибающей спектра), определяющей РР:

$$P(\omega, t) = \log\left[\frac{S(\omega, t)}{S(\omega, t - \tau)}\right] \qquad (2)$$

где $P(\omega, t)$ – фонетическая функция Пирогова, а $S(\omega, t)$ и $S(\omega, t - \tau)$ – модули кратковременных спектров в соответствующие моменты времени.

Плюс от сеанса к сеансу можно организационно изменять набор участвующих в модели сплиттера

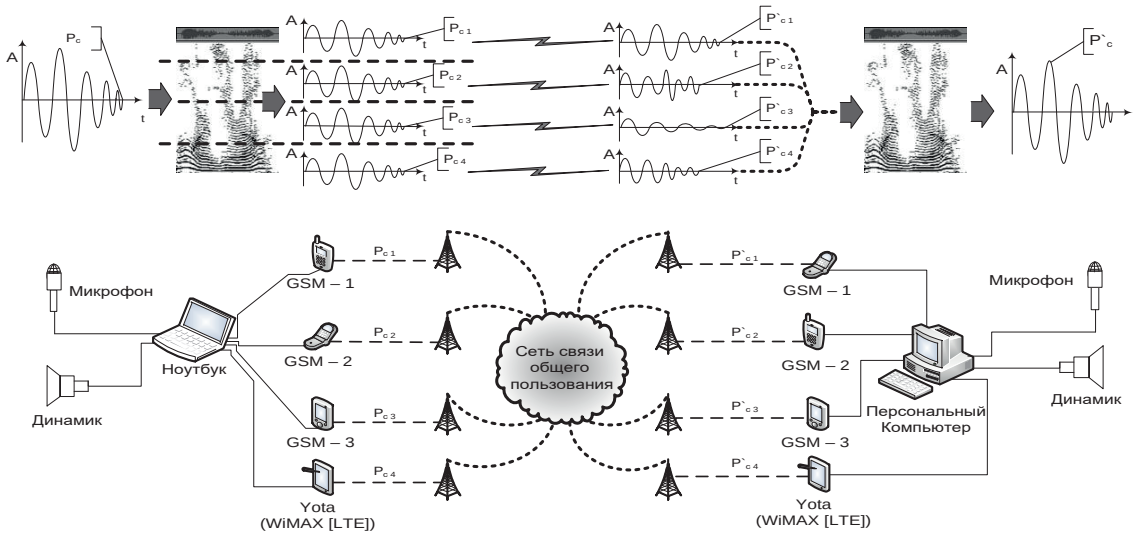


Рис. 2. Общая схема многоканальной системы защищенной речевой связи, маскированной разделением и расслоением

каналов, добавляя каналы новых операторов связи (например, фиксированную телефонную связь, другие сервисы VoIP и сотовой связи) и исключая «старых», предыдущих.

2. «Реконструкторы», восстанавливающие РР из принятой части РИ

Эти маскираторы используют только отделенную для передачи неразборчивую часть исходной речевой информации, по которой на приемном конце КГС с использованием заранее сформированного речевого корпуса диктора может быть реконструирована вся спектрограмма защищаемого сигнала и произведена ее инверсия по восстановлению его волновой формы и РР. Остаточная неразборчивая часть исходного РС, подлежащая передаче, может быть получена путем фильтрации РС или микшированием его с шумом или каким-то другим способом. Важно, чтобы осталось не менее 3-х гармоник на принятом материале, по которым потом будет возможна реконструкция спектрограммы и синтез клона исходного РС.

То есть после нахождения основного тона на полученном остаточном речевом материале необходимо восстановить гармоническую структуру речи, найти все гармоники с частотой, кратной частоте основного тона, с использованием следующего соотношения:

$$\omega_i = i \cdot \omega_{\text{осн}},\ i \in \left[\frac{\nu}{2 \cdot \omega_{\text{осн}}}\right], \qquad (3)$$

где ω_i – круговая частота i-ой гармоники.

Суть используемого алгоритма восстановления гармонической структуры РС[15] посредством поиска кратных основному тону гармоник на одном временном срезе сонограммы заключается в следующем:

а) каждый частотно-временной срез рассчитывается и анализируется независимо от других посредством кратковременного анализа Фурье;
б) на каждом временном слое определяется частота основного тона параболическим способом (частоту основного тона измеряем как количество (ν/N) Гц, ν – частота дискретизации звукового сигнала);
в) на временном срезе находится точка с частотой, наиболее близкой к частоте основного тона, которая помечается условным красным маркером;
г) на этом же временном слое находятся точки с частотой, наиболее близкой к удвоенной, утроенной,... и т.д. частоте основного тона; выбранные точки также помечаются;
д) амплитуда всех непомеченных точек полагается равной нулю.

Результат работы описанного выше алгоритма изображен на рис. 3, где представлены результаты параболической коррекции линий гармоник по вершинам парабол спектральных разверток. Как видно, после проведенной коррекции треки даже верхних гармоник (красные линии наверху) являются непрерывными и совпадают с точными исходными значениями на изображении узкополосной спектрограммы.

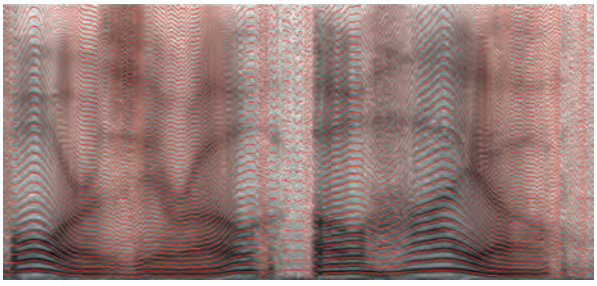


Рис. 3. Сонограмма и линии гармоник (красные треки) после коррекции частоты основного тона по вершинам парабол спектральных разверток.

15 Дворянкин С. В., Алюшин В. М. Метод реконструкции гармонической структуры спектральных описаний искаженной шумами и помехами речи. // Известия Института инженерной физики. 2013. № 2 (28). С. 57–62.

Дополнительным критерием проверки правильности нахождения основного тона являлась максимизация суммы амплитуд первых 7 кратных гармоник:

$$\sum_{K}^{7} |X[i \cdot x_в]| \longrightarrow max,$$

где $[a]$ – целая часть числа a.

Предложенный метод работает в случае зашумленного сигнала при условии, что треки только некоторых первых гармоник «видны» на фоне шумов (рис. 4).

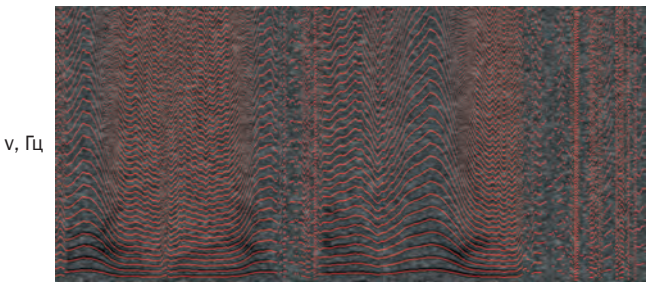


Рис. 4. Сонограмма и линии гармоник зашумленного речевого сообщения

Как показали эксперименты, при зашумлении речевого сообщения белым шумом треки гармоник и восстановленная по ним гармоническая структура находятся корректно даже при отношении сигнал/шум до –12 Дб. При зашумлении речевого сообщения естественными помехами, гармоническая структура может корректно восстанавливаться при отношении сигнал/шум до –8 ... –5 Дб.

Оставшаяся в шумах часть РС неразборчива, но РР может быть восстановлена по реконструированной гармонической структуре и соответствующей ей формантной из речевого корпуса диктора.

Разработанный метод и алгоритм нахождения основного тона вокализованных участков РС позволяет восстанавливать гармоническую структуру сигнала (рис. 6) даже в случае, если часть спектральных описаний сигнала, содержащих линию основного тона и несколько верхних и нижних гармоник (рис. 4, 5), были «утеряны», зашумлены.

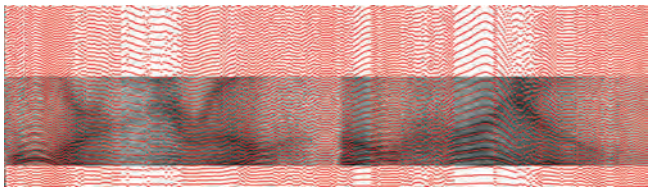


Рис. 5. Гармоническая структуры РС, восстановленная по спектральным описаниям с частичной потерей информации.

3. «Заместители» с заменой (подменой) опорных элементов речи

Заместители это маскираторы с подменой исходных автоматически распознающихся фонем (или других элементов речевого потока) на фонемы иного несуществующего языка из речевой базы данных виртуального диктора и обратно.

Рассмотрим один из таких методов обеспечения конфиденциальности речи на основе маскировки звука и материала известного речевого корпуса [6]. Структурная схема предлагаемого метода приведена на рис. 6.

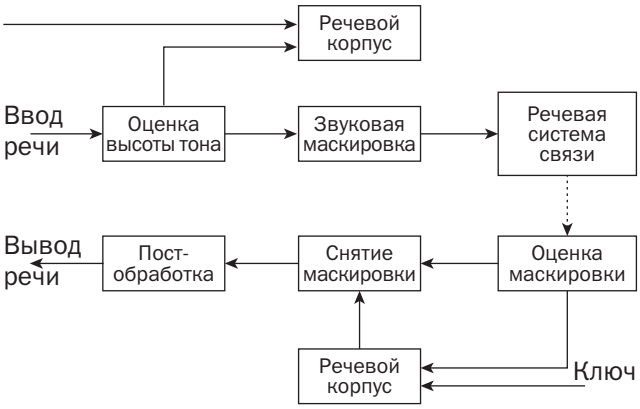


Рис. 6. Структурная схема метода обеспечения конфиденциальности речи на основе маскировки звука и ресурса корпуса речи

Здесь входная речь сначала сегментируется на кадры, и для каждого кадра выполняется оценка высоты тона по описанному выше алгоритму[16], которая выступает как часть идентификатора для нахождения нужных кадров из речевого корпуса.

Другой частью идентификатора является секретный ключ, который раздается каждому пользователю. В целях безопасности секретные ключи могут меняться через определенные промежутки времени или каждый раз. Помимо ключей, сам корпус также может быть заменен по расписанию для обеспечения безопасности связи.

Каждый кадр входной речи маскируется соответствующими кадрами в корпусе. Для каждого целевого кадра речи выбирается один или несколько кадров речи из корпуса, причем выбранные кадры должны иметь ту же высоту тона, что и входной кадр. Чем больше кадров корпуса используется для маскировки каждого целевого речевого кадра, тем лучшего эффекта маскировки можно достичь несмотря на то, что сам алгоритм маскировки будет сложнее[17]. Чтобы высота тона не менялась, маскирование ограничивается линейными аддитивными операциями. Затем маскированная речь вводится в коммуникационные системы вместо оригинальной речи.

16 Дворянкин С. В., Алюшин В. М. Метод реконструкции гармонической структуры спектральных описаний искаженной шумами и помехами речи. // Известия Института инженерной физики. 2013. № 2 (28). С. 57–62.

17 Алдошина И. А. Лекции по психоакустике. / Архив журнала «Звукорежиссер» : 1999-2002. URL: https://prazdnikson.ru/i-aldoshina-lektsii-po-psihoakustike (дата обращения: 16.06.2024).

На принимающей стороне эффект маскировки снимается с принимаемой замаскированной речи также в соответствии с индексом высоты тона. Принимающая сторона должна иметь тот же корпус и секретный ключ, как и передающая сторона, чтобы из корпуса можно было выбрать те же маскирующие кадры и затем правильно восстановить речь в кадре с помощью обратного алгоритма демаскировки звука.

Для успешного восстановления речи алгоритм должен быть спроектирован с определенной допуском к погрешности высоты тона на случай, если из-за ошибок канала связи высота тона может несколько отличаться до и после передачи.

Целью постобработки является снижение влияния погрешности высоты тона и улучшение качества восстановленной речи. Так, простое удаление неправильно принятого кадра не принесет очевидного ущерба качеству речи. Для лучшего качества речи удаленный речевой кадр также может быть скомпонован из данных соседних кадров и восстановлен.

В этом методе неразборчивость замаскированной речи поможет сохранить конфиденциальность коммуникации даже в том случае, если передаваемая речь была перехвачена ЗЛ, а секретность речевого корпуса и секретные ключи определяют стойкость к взлому системы. Таким образом, можно обеспечить высокий уровень безопасности речевой связи.

В данном методе, как и в предыдущих, звуковая маскировка выполняется перед отправкой речи в коммуникационную систему, а восстановление речи выполняется на ее выходе. Никаких модификаций коммуникационной системы не требуется. Тогда сквозная защита конфиденциальности речи может быть реализована с небольшими затратами.

Даже если в системах речевой связи используется сжатие с потерями, предложенный метод работоспособен. Результаты экспериментов показали, что предложенный метод достигает хорошей производительности, когда в системах связи используются алгоритмы кодирования формы речевой волны[18].

4. «Трансляторы» – переводчики речи на незнакомый язык

Частный случай маскираторов заместителей, активно развивающийся. В работе [7] представлена нейронная сеть, которая может напрямую переводить речь с одного языка на другой, не опираясь на промежуточное текстовое представление. Сеть проходит сквозное обучение и учится сопоставлять спектрограммы речи с целевыми спектрограммами на другом языке, соответствующими переведенному контенту в другом каноническом голосе. Далее так переведенная речь синтезируется по новой спектрограмме, используя голос диктора-источника, носителя неизвестного языка.

Эксперименты на двух наборах данных для перевода речи с испанского на английский напрямую, без опоры на промежуточное текстовое представление. показали, что предложенная модель незначительно уступает базовому каскаду из модели перевода речи в текст и модели синтеза текста в речь, что свидетельствует о применимости подхода для решения сложной задачи защиты конфиденциальности речевых коммуникаций в реальном времени.

5. «Смесители» – устройства информационного маскирования

Маскирование, возникающее, когда целевая речь сопровождается одним мешающим фактором – голосом или несколькими голосами и звуками, часто называют информационным (ИМ). Как правило, ИМ больше, когда интерферирующий голос громок и разборчив, чем когда он тих и неразборчив (например, речь на незнакомом языке). Но относительный вклад акустико-фонетической и лингвистической интерференции часто трудно оценить из-за акустических различий между интерферирующими сторонами (например, разными собеседниками) [8].

Тем не менее, ИМ находит свое распространение в системах активной защиты ЗП, при формировании речеподобных помех, адаптивными защищаемому РС [2]. Правда здесь не нужен процесс демаскирования.

В КГС удобно использовать независимые голосовые помехи, в качестве которых может использоваться звуковое вещание нескольких (не менее трех) новостных программ ведущимися разными дикторами.

Получаемая таким образом помеховая смесь формируется одновременно на всех концах защищаемой системы голосовой связи. Количество радиостанций, частоты их вещания, тип дикторов и др. независимые параметры определяют секретные ключи для организации процессов маскирования и демаскирования без их распределения. Содержимое таких ключей может неоднократно меняться в процессе речевого обмена.

Важно, чтобы помехи были подобраны таким образом, чтобы процесс демаскирования на приёмном конце КГС сводился к упрощенным компенсации и коррекции её следов на основе образного анализа изображения зашумленной спектрограммы [1].

6. «Маркеры и подложки» – встроенные в сигналы и сообщения спектрограммы

Могут выступать в качестве речевой подписи, цифровых водяных знаков для подтверждения подлинности конфиденциальных данных и-или скрытной передачи речи. Признаки исходной защищаемой речи в явном виде отсутствуют.

Используются в популярных носителях информации разных видов как встроенные в них изображения

18 Ding Qi, Nan Longmei, Xu jinfu. A Speech Privacy Protection Method Based on Sound Masking and Speech Corpus. 8th International Congress of Information and Communication Technology (ICICT – 2018).

полутоновых и бинарных сонограмм (речевой подписи), не влияющими на качество передаваемых–сохраняемых носителями данных, с последующей инверсией спектрограмм и реконструкцией по ним РС по запросу [3].

С помощью скрытно и–или открыто представляемой речевой подписи на информносителях можно не только передавать–сохранять конфиденциальную информацию, но и обеспечивать ее аутентичность, формируя сигналы со спектром идентичным биопризнаку пользователя.

Заключение

Рассмотрена классификация существующих маскираторов и устройств технического закрытия речи нового типа. Выработаны требования к перспективным устройствам маскирования, из которых особо отмечены асинхронность, гибридность, скорость и гибкость работы, отсутствие признаков открытой исходной речи.

Для оценки уровня защищенности маскируемого канала голосовой связи предлагается использовать показатель словесной разборчивости с нормами и критериями, принятыми для защищаемых помещений конфиденциальных переговоров.

За основу разрабатываемых компьютерных технологий обеспечения безопасности (приема, передачи и хранения) конфиденциальных речевых сообщений через управление их разборчивостью можно принять технологию образного анализа РС, заключающаяся в переходе, посредством кратковременного преобразования Фурье, от волнового представления РС к изображению динамических узкополосных спектрограмм – графических образов (ГО), их обработке методами цифровой обработки изображений, распознавания образов и методов машинного обученияИ для решения поставленных прикладных задач и обратном переходе (синтезе) от нового изображения, посредством инверсии спектрограмм, к новой волновой форме.

Новые виды речевых маскираторов, разрабатываемых на основе предложенной технологии образного анализа, будут обладать рядом неоспоримых преимуществ по сравнению с аналогами: достаточно невысокой стоимостью, относительно высокой стойкостью, максимальной оперативностью, отсутствием остаточной разборчивости, повышенным качеством восстановленного сигнала, устойчивой работой на каналах среднего и низкого качества.

Литература

1. *Хорев А. А., Дворянкин С. В., Козлачков С. Б., Василевская Н. В. Анализ предельных возможностей методов шумопонижения и реконструкции речевых сигналов, маскируемых различными типами помех //Вопросы кибербезопасности. 2024. № 1 (59). С. 89–100.*
2. *Дворянкин С. В., Дворянкин Н. С., Устинов Р. А. Речеподобная помеха, стойкая к шумоочистке, как результат скремблирования защищаемой речи // Вопросы кибербезопасности. 2022. № 5 (51). С. 14–27.*
3. *Дворянкин С. В., Дворянкин Н. С., Устинов Р. А. Развитие технологий образного анализа-синтеза акустической (речевой) информации в системах управления, безопасности и связи // Безопасность информационных технологий =IT Security. Том 26, № 1. 2019. С. 64–76. DOI: http://dx.doi.org/10.26583/bit.2019.1.07*
4. *Голиков А. М. Исследование методов аналогового скремблирования: Учебно-методическое пособие по лабораторной работе [Электронный ресурс] / А. М. Голиков. – Томск: ТУСУР, 2019. – 25 с.*
5. *Столбов М. Б. Основы анализа и обработки речевых сигналов / М. Б. Столбов – СПб.: НИУ ИТМО, 2021. – 101 с.*
6. *Tom Backstrom. Privacy in Speech Technology. arXiv:2305.05227v1 [eess.AS] 9 May 2023/*
7. *Ye Jia, Ron J. Weiss, Fadi Biadsy, Wolfgang Macherey, Melvin Johnson, Zhifeng Chen, Yonghui Wu Direct speech-to-speech translation with a sequence-to-sequence model. arXiv:1904.06037v1 [cs.CL] 12 Apr 2019.*
8. *Robert J. Summers, Brian Roberts. Informational masking of speech by acoustically similar intelligible and unintelligible interferers. The Journal of the Acoustical Society of America 147(2):1113-1125. February 2020. DOI:10.1121/10.0000688*
9. *Jennifer Williams, Karla Pizzi, Paul-Gauthier Noé , Sneha Das. Exploratory Evaluation of Speech Content Masking. arXiv:2401.03936v1 [eess.AS] 8 Jan 2024.*
10. *Sonia Yasmin, Vanessa C. Irsik, Ingrid S. Johnsrude, Björn Herrmann. The Effects of Speech Masking on Neural Tracking of Acoustic and Semantic Features of Natural Speech. Neuropsychologia doi: 10.1016/j.neuropsychologia.2023.108584. doi:https://doi.org/10.1101/2023.02.10.527537.*
11. *Y. Chen, Y. Assael, B. Shillingford, D. Budden, S. Reed, H. Zen, Q. Wang, L. C. Cobo, A. Trask, B. Laurie et al., «Sample efficient adaptive text-to-speech», in Proc. ICLR, 2019.*
12. *Y. Jia, M. Johnson, W. Macherey, R. J. Weiss, Y. Cao, C. -C. Chiu, N. Ari et al., «Leveraging weakly supervised data to improve endto-end speech-to-text translation», in Proc. ICASSP, 2019.*
13. *A. Haque, M. Guo, and P. Verma, «Conditional end-to-end audio transforms», in Proc. Interspeech, 2018. [23] J. Zhang, Z. Ling, L. -J. Liu, Y. Jiang, and L. -R. Dai, «Sequenceto-sequence acoustic modeling for voice conversion», IEEE/ACM Transactions on Audio, Speech, and Language Processing, 2019.*
14. *F. Biadsy, R. J. Weiss, P. J. Moreno, D. Kanevsky, and Y. Jia, «Parrotron: An end-to-end speech-to-speech conversion model and its applications to hearing-impaired speech and speech separation», arXiv:1904.04169, 2019.*
15. *J. Shen, P. Nguyen, Y. Wu, Z. Chen et al., «Lingvo: a modular and scalable framework for sequence-to-sequence modeling», 2019.*
16. *K. Irie, R. Prabhavalkar, A. Kannan, A. Bruguier, D. Rybach, and P. Nguyen, «Model unit exploration for sequence-to-sequence speech recognition», arXiv:1902.01955, 2019.*
17. *W. -N. Hsu, Y. Zhang, R. J. Weiss, H. Zen, Y. Wu, Y. Wang, Y. Cao, Y. Jia, Z. Chen, J. Shen et al., «Hierarchical generative modeling for controllable speech synthesis», in Proc. ICLR, 2019.*

EVOLUTION AND DIRECTIONS OF DEVELOPMENT OF TECHNOLOGIES FOR MASKING CONFIDENTIAL SPEECH MESSAGES

Durakovskiy A. P.[19], Dvoryankin S. V.[20], Dvoryankin N. S.[21]

Purpose of the research: *analysis of methods and algorithms of technical closure of speech information in networks and systems of voice communication, evaluation of directions and prospects of development of speech masking technologies with machine learning.*

Research methods: *applied systems analysis, digital spectral-time analysis, digital signal and image processing, image analysis of spectrograms, machine learning*

Research results: *the problems of ensuring the security of confidential voice communication in modern conditions are outlined. The review of speech protection methods used in practice in public voice communication channels is given. Traditional and perspective algorithms of masking of speech messages, methods of their realization are considered. The advantages of the latter over the ones are noted.*

Science significance: *New methods of technical speech masking based on modification and reconstruction of dynamic spectrogram images using artificial intelligence are proposed*

Practical: *effective speech masking algorithms are proposed. The obtained results will allow to expand the possibilities of existing solutions for protection of speech information in voice communication systems and networks and to design more effective ones based on the described approaches.*

Keywords: *information security, speech information protection, image analysis-synthesis, technical speech closure, speech-like signal, machine learning.*

References

1. *Horev A. A., Dvoryankin S. V., Kozlachkov S. B., Vasilevskaya N. V. Analiz predel'nyh vozmozhnostej metodov shumoponizheniya i rekonstrukcii rechevyh signalov, maskiruemyh razlichnymi tipami pomekh. //Voprosy kiberbezopasnosti. 2024. № 1 (59). S. 89–100.*
2. *Dvoryankin S. V., Dvoryankin N. S., Ustinov R. A. Rechepodobnaya pomekha, stojkaya k shumoochistke, kak rezul'tat skremblirovaniya zashchishchaemoj rechi. // Voprosy kiberbezopasnosti. 2022. № 5 (51). S. 14–27.*
3. *Dvoryankin S. V., Dvoryankin N. S., Ustinov R. A. Razvitie tekhnologij obraznogo analiza-sinteza akusticheskoj (rechevoj) informacii v sistemah upravleniya, bezopasnosti i svyazi // Bezopasnost' informacionnyh tekhnologij =IT Security. Tom 26, № 1. 2019. C. 64–76. DOI: http://dx.doi.org/10.26583/bit.2019.1.07*
4. *Golikov A. M. Issledovanie metodov analogovogo skremblirovaniya: Uchebno-metodicheskoe posobie po laboratornoj rabote [Elektronnyj resurs] / A. M. Golikov. – Tomsk: TUSUR, 2019. – 25 s.*
5. *Stolbov M. B. Osnovy analiza i obrabotki rechevyh signalov / M. B. Stolbov – SPb.: NIU ITMO, 2021. – 101 s.*
6. *Tom Backstrom. Privacy in Speech Technology. arXiv:2305.05227v1 [eess.AS] 9 May 2023/*
7. *Ye Jia, Ron J. Weiss, Fadi Biadsy, Wolfgang Macherey, Melvin Johnson, Zhifeng Chen, Yonghui Wu Direct speech-to-speech translation with a sequence-to-sequence model. arXiv:1904.06037v1 [cs.CL] 12 Apr 2019.*
8. *Robert J. Summers, Brian Roberts. Informational masking of speech by acoustically similar intelligible and unintelligible interferers. The Journal of the Acoustical Society of America 147(2):1113-1125. February 2020. DOI:10.1121/10.0000688*
9. *Jennifer Williams, Karla Pizzi, Paul-Gauthier Noé , Sneha Das. Exploratory Evaluation of Speech Content Masking. arXiv:2401.03936v1 [eess.AS] 8 Jan 2024.*
10. *Sonia Yasmin, Vanessa C. Irsik, Ingrid S. Johnsrude, Björn Herrmann. The Effects of Speech Masking on Neural Tracking of Acoustic and Semantic Features of Natural Speech. Neuropsychologia doi: 10.1016/j.neuropsychologia.2023.108584. doi:https://doi.org/10.1101/2023.02.10.527537.*
11. *Y. Chen, Y. Assael, B. Shillingford, D. Budden, S. Reed, H. Zen, Q. Wang, L. C. Cobo, A. Trask, B. Laurie et al., «Sample efficient adaptive text-to-speech», in Proc. ICLR, 2019.*
12. *Y. Jia, M. Johnson, W. Macherey, R. J. Weiss, Y. Cao, C. -C. Chiu, N. Ari et al., «Leveraging weakly supervised data to improve endto-end speech-to-text translation», in Proc. ICASSP, 2019.*
13. *A. Haque, M. Guo, and P. Verma, «Conditional end-to-end audio transforms», in Proc. Interspeech, 2018. [23] J. Zhang, Z. Ling, L. -J. Liu, Y. Jiang, and L. -R. Dai, «Sequenceto-sequence acoustic modeling for voice conversion», IEEE/ACM Transactions on Audio, Speech, and Language Processing, 2019.*
14. *F. Biadsy, R. J. Weiss, P. J. Moreno, D. Kanevsky, and Y. Jia, «Parrotron: An end-to-end speech-to-speech conversion model and its applications to hearing-impaired speech and speech separation», arXiv:1904.04169, 2019.*
15. *J. Shen, P. Nguyen, Y. Wu, Z. Chen et al., «Lingvo: a modular and scalable framework for sequence-to-sequence modeling», 2019.*
16. *K. Irie, R. Prabhavalkar, A. Kannan, A. Bruguier, D. Rybach, and P. Nguyen, «Model unit exploration for sequence-to-sequence speech recognition», arXiv:1902.01955, 2019.*
17. *W. -N. Hsu, Y. Zhang, R. J. Weiss, H. Zen, Y. Wu, Y. Wang, Y. Cao, Y. Jia, Z. Chen, J. Shen et al., «Hierarchical generative modeling for controllable speech synthesis», in Proc. ICLR, 2019.*

19 Anatoly P. Durakovskiy, Ph.D. (in Tech.), Associate Professor of the Department of Strategic Information Studies of MEPhI, Director of the Attestation and Testing Centre for Information Security and Information Protection Systems of MEPhI. Moscow. Russia. E-mail: apdurakovskiy@mephi.ru

20 Sergey V. Dvoryankin, Dr. Sc. (of Tech.), Professor, Professor of the Department of Strategic Information Studies, National Research Nuclear University MEPhI, Head of the Laboratory for the Protection and Processing of Audiovisual Information, Moscow State Linguistic University. Moscow. Russia. E-mail: svdvoryankin@mephi.ru, https://orcid.org/0000-0001-6908-0676

21 Nikita S. Dvoryankin, postgraduate student, National Research Nuclear University MEPhI. Moscow. Russia. E-mail: nik.dvrn@gmail.com

КОМПЛЕКСНЫЕ РЕШЕНИЯ ДЛЯ МИНИМИЗАЦИИ ВНУТРЕННИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Морозов В. Е.[1], Милославская Н. Г.[2]

DOI: 10.21681/2311-3456-2024-5-67-78

Цель работы: *определение состава современных решений, в совокупности позволяющих создать систему комплексного управления информационной безопасностью организации.*

Методы исследования: *анализ релевантных научных публикаций, концептуальное моделирование, экспертная оценка, синтез системы комплексного управления информационной безопасностью.*

Полученные результаты: *в статье детализируются составляющие процесса управления информационной безопасностью (ИБ) и обсуждается возможный состав ориентированной на минимизацию внутренних угроз системы комплексного управления ИБ организации. Показано, что подобная система должна включать следующие ключевые элементы: подсистему централизованного мониторинга событий и расследования инцидентов ИБ, подсистему контроля защищенности данных и выявления уязвимостей в доступе к ним, а также подсистему контроля информационных потоков и противодействия утечкам защищаемой информации. Указанные подсистемы могут быть реализованы при помощи SIEM-, DCAP- и DLP-систем соответственно. Рассматриваются основные концепции и технологии, на базе которых разработаны данные решения, их архитектура, особенности функционирования и аналитические возможности на примере программных комплексов, разработанных компанией «СёрчИнформ» («СёрчИнформ SIEM», «СёрчИнформ FileAuditor» и «КИБ СёрчИнформ»). Анализ совокупности характеристик и опыта применения названных продуктов показывает, что при условии их интеграции они способны обеспечить полномасштабную защиту деятельности организации на всех уровнях.*

Практическая значимость *заключается в обосновании достаточности указанного состава системы управления ИБ для решения задачи минимизации внутренних угроз.*

Ключевые слова: *DLP, DCAP, SIEM, внутренние угрозы информационной безопасности, инцидент информационной безопасности, мониторинг, событие информационной безопасности, управление информационной безопасностью.*

Введение

Эксперты во всем мире ежегодно фиксируют значительный рост числа инцидентов информационной безопасности (ИБ)[3], среди которых фигурируют регулярно обнаруживаемые в открытом доступе «утёкшие» персональные данные, «сливы» внутренних документов различных компаний[4], случаи заражения вредоносным кодом с последующим уничтожением данных и многое другое. Сам по себе данный факт уже давно не вызывает ни у кого удивления – это сформировавшаяся устойчивая тенденция, наблюдающаяся в течении ряда последних лет. Однако, начиная с 2022 г., в Российской Федерации рост числа инцидентов ИБ приобрел по-настоящему взрывной характер. Помимо рядовых граждан от киберпреступлений часто страдает и критическая информационная инфраструктура (КИИ), которой граждане, к слову, активно пользуются – транспортной, финансовой, медицинской, энергетической, промышленной [1,2]. Одной из основных причин большого числа уязвимостей в программном обеспечении (ПО) объектов КИИ является уход иностранных вендоров, которые перестали поддерживать свои решения, ранее установленные у российских заказчиков. В то же время отечественные аналоги еще только начинают свое движение навстречу российским клиентам [3]. А если прибавить к увеличившейся интенсивности атак дефицит квалифицированных ИБ-специалистов, то становится очевидно, что в службах ИБ и государственных корпораций, и коммерческих компаний не последнюю роль должны играть комплексные решения, позволяющие защитить данные сразу по нескольким направлениям в сочетании с эффективным управлением ИБ.

Источники угроз ИБ многообразны и могут находиться как снаружи защищаемого периметра организации, так и внутри него. Принято считать, что именно внутренние угрозы представляют наибольшую опасность, так как именно на них приходится большинство фиксируемых инцидентов ИБ. Случайные ошибки персонала, бездействие, мошенничество,

1 Морозов Виктор Егорович, кандидат психологическин наук, доцент. ООО «Либрасофт», Минск, Республика Беларусь. E-mail: v.morozov@searchinform.ru
2 Милославская Наталья Георгиевна, доктор технических наук, Ph.D. in Cybersecurity, доцент. НИЯУ МИФИ, Москва, Россия. E-mail: NGMiloslavskaya@mephi.ru

3 Тренды кибератак на промышленность и телеком [Электронный ресурс] // Solar. URL: https://rt-solar.ru/analytics/reports/4361/ (дата обращения: 05.08.24).
4 Рахметов, Р. Что такое DLP системы и как они применяются [Электронный ресурс] // Security Vision. URL: https://www.securityvision.ru/blog/chto-takoe-dlp-sistemy-i-kak-oni-primenyayutsya/ (дата обращения: 05.08.24).

Рис. 1. Составляющие процесса управления ИБ

инсайдерские действия регулярно приводят к многомиллионному ущербу для компаний, работающих в сфере высоких технологий, финансов, связи.

Управление ИБ в общем случае представляет собой циклический процесс, который включает в себя сбор и анализ данных об уровне ИБ в организации, оценку рисков ИБ, планирование мер по их обработке, реализацию и внедрение соответствующих мер обеспечения ИБ (ОИБ) [4], распределение ролей и ответственности, оперативную работу по осуществлению мероприятий по защите, мониторинг функционирования мер ОИБ, оценку их эффективности и соответствующую коррекцию в зависимости от результатов деятельности (рис. 1). В техническом плане управление ИБ можно разделить на использование локальных подсистем мониторинга и управления отдельными средствами защиты информации и создание комплексных систем управления ИБ[5] [5–8].

В настоящее время на рынке программных продуктов, ориентированных на ОИБ, представлено достаточно большое число классов различных решений[6], среди которых следует выделить следующие: *SOAR* (*Security Orchestration, Automation and Response*), *SIEM* (*Security Information and Event Management*), *DLP* (*Data Loss Prevention*), *XDR* (*Extended Detection and Response*), *EDR* (*Endpoint Detection and Response*), *DFIR* (*Digital Forensics and Incident Response*). В последние годы к ним добавились еще и системы, разработанные в рамках подхода *DCAP/DAG* (*Data-Centric Audit and Protection/Data Access Governance*)[7]. Тем не менее, сложно представить себе ситуацию, чтобы в одной организации использовались сразу все перечисленные системы. Да и практика чаще всего подталкивает к разумным ограничениям: далеко не каждая компания готова выделить достаточные финансовые и технические ресурсы для приобретения и эксплуатации всего вышеперечисленного. Поэтому нередко встают вопросы об оптимальном наборе ИБ-решений, о перечне ключевых систем, о проектировании и организации целевой архитектуры ИБ, учитывающей специфику конкретной организации или проекта, и т.п.

Все сказанное выше вольно или невольно подталкивает к определению своего рода базового набора средств, актуальных сегодня для любой организации и позволяющих достичь комплексности ОИБ. При этом не стоит забывать, что на практике крайне важно оценить конкретные потребности и цели организации, прежде чем выбирать средства, которые лучше всего будут удовлетворять этим потребностям.

Для начала попробуем выделить ключевые элементы системы комплексного управления ИБ. К ним следует отнести:

- подсистему централизованного мониторинга событий и расследования инцидентов ИБ (может быть реализована при помощи *SIEM*-решения);
- подсистему контроля защищенности данных и выявления уязвимостей в доступе к ним (может быть реализована при помощи *DCAP*-решения);
- подсистему контроля информационных потоков и противодействия утечкам защищаемой информации (может быть реализована при помощи *DLP*-решения).

С нашей точки зрения, именно они могут играть роль фундамента, на котором с соблюдением принципа разумной достаточности может быть построено «здание ОИБ» в конкретной организации.

Программные продукты компании «СёрчИнформ», впрочем, как и другие аналогичные, вполне вписываются в рассмотренную модель и позволяют

5 Комплексные системы управления информационной безопасностью [Электронный ресурс] // Rubytech. URL: https://rubytech.ru/products/informatsionnaya-bezopasnost/napravleniya-informatsionnoy-bezopasnosti/kompleksnye-sistemy-upravleniya-informatsionnoy-bezopasnostyu/ (дата обращения: 05.08.24).

6 How to Enhance Your Cybersecurity Platform: XDR vs EDR vs SIEM vs IRM vs SOAR vs DLP [Электронный ресурс] // Apriorit. URL: https://www.apriorit.com/dev-blog/enhancing-cybersecurity-platform-xdr-edr-siem-irm-soar-dlp (дата обращения: 05.08.24).

7 Дудоров И. Системы DCAP: как защитить самое главное [Электронный ресурс] // Anti-malware. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Data-Centric-Audit-and-Protection (дата обращения: 08.08.24).

в полной мере реализовать указанные элементы системы комплексного управления ИБ на уровне организации. В равной степени это касается вопросов недопущения реализации угроз со стороны внутренних нарушителей при помощи *DLP*-системы «КИБ СёрчИнформ»[8], контроля защищенности данных и выявления уязвимостей в доступе к ним путем применения *DCAP*-системы «СёрчИнформ FileAuditor»[9], выявления аномалий в информационных потоках и оповещения о критических событиях в режиме онлайн при помощи *SIEM*-системы «СёрчИнформ SIEM»[10]. Все названные решения легко сочетаются между собой. При совместном использовании они способны обеспечить полномасштабную защиту деятельности организации на всех уровнях.

Противодействие утечкам защищаемой информации

Современные *DLP*-системы, эволюционируя, вбирали в себя наиболее удачные функции [9–12]. Следствием этого стала чрезвычайная их схожесть между собой. Поэтому ниже приведена обобщенная архитектура *DLP*-системы на примере «КИБ СёрчИнформ» (КИБ). В других системах могут быть отличия – работа без баз данных (БД) или выполнение анализа на агенте, а не на сервере.

Источником информации, как правило, являются действия, которые работник совершает, перемещая различные данные. Вся активность пользователя перехватывается условными «сборщиками» (снифферами, сетевыми анализаторами, модулями перехвата). За понятием «сборщик» обычно кроется один или несколько способов перехвата информации: сетевой перехват, перехват путем интеграции со сторонними продуктами [с почтовыми и прокси-серверами], агентский перехват и перехват путем установки *DLP*-системы «в разрыв». В задачи, решаемые «сборщиками» информации, входит и ее парсинг – извлечение структурированной информации из неструктурированных или полуструктурированных данных. Из перехваченных пакетов парсеры извлекают метаданные (дату, время, *IP*-адрес, доменную «учетку» пользователя) и текст (переписки, вложения). Парсеры могут отбрасывать «ненужную» с точки зрения ИБ информацию, например, медиаконтент (картинки, видеофайлы).

Далее информация записывается на хранение в БД. *DLP*-системы в основном используют *SQL*-подобные БД, поскольку они наиболее распространены. Но встречаются решения и на Oracle, PostgreSQL, SQLite. «КИБ СёрчИнформ» использует MSSQL и PostgreSQL.

После записи информации в БД с ней уже можно работать – делать запросы и анализировать выдачу. Однако, БД не оптимизированы для быстрого поиска текстовой информации. А основная информация, перехватываемая и обрабатываемая *DLP*-системами, – именно текст. В контексте решения описываемых задач для превращения «сырых» данных в оптимизированные для быстрого поиска структуры используется индексация. Индекс содержит информацию о слове, которое нужно найти (где оно встречается, какая у него позиция в документе относительно других слов и т.д.).

После индексации по перехваченной информации можно проводить быстрый поиск. В любой *DLP*-системе для анализа используются три типа средств: «просмотрщик», средство автоматизации, средство отчетности. «Просмотрщик» обеспечивает выполнение ручного поиска (например, при расследовании инцидентов, проверке правил, по которым *DLP*-система будет автоматически (по расписанию) проверять перехваченную информацию и т.п.). Средство автоматизации предназначено для автоматизации проверок в *DLP*-системе: специалист по ИБ создает правило, в котором указывает что, где и как часто нужно искать (формируется расписание) и кого уведомлять в случае нарушения политики. Средство отчётности нужно для предоставления информации о возможных нарушениях в той или иной форме.

Реальная архитектура «КИБ СёрчИнформ» значительно сложнее по сравнению со схематичными связями, описанными выше. Информацию с компьютера сотрудника перехватывают платформы NetworkController и EndpointController. Первая отвечает за сетевой перехват, вторая – за агентский (рис. 2). Возможности сетевой платформы могут быть расширены за счет перехвата путем интеграции (количество каналов перехвата не увеличивается, но появляется возможность перехвата шифрованных данных). Когда информация записана в БД MSSQL, к ее обработке приступает SearchServer. С помощью этого «движка» из информации, которая содержит текст, формируются индексы. При этом информация, которая изначально не содержит текст, индексацию не проходит и доступна для поиска в виде БД. Все компоненты КИБ имеют клиент-серверную архитектуру. Серверную часть представляет одна из платформ для перехвата данных, клиентскую – приложения для поиска и просмотра перехваченных данных в ходе проведения служебных расследований.

Модули перехвата, которые входят в состав системы, обеспечивают возможность контроля практически всех популярных каналов обмена информацией (рис. 3).

8 СёрчИнформ КИБ [Электронный ресурс] // SearchInform. URL: https://searchinform.ru/products/kib/ (дата обращения: 05.08.24).

9 СёрчИнформ FileAuditor [Электронный ресурс] // SearchInform. URL: https://searchinform.ru/products/fileauditor/ (дата обращения: 05.08.24).

10 СёрчИнформ SIEM [Электронный ресурс] // SearchInform. URL: https://searchinform.ru/products/siem/ (дата обращения: 05.08.24).

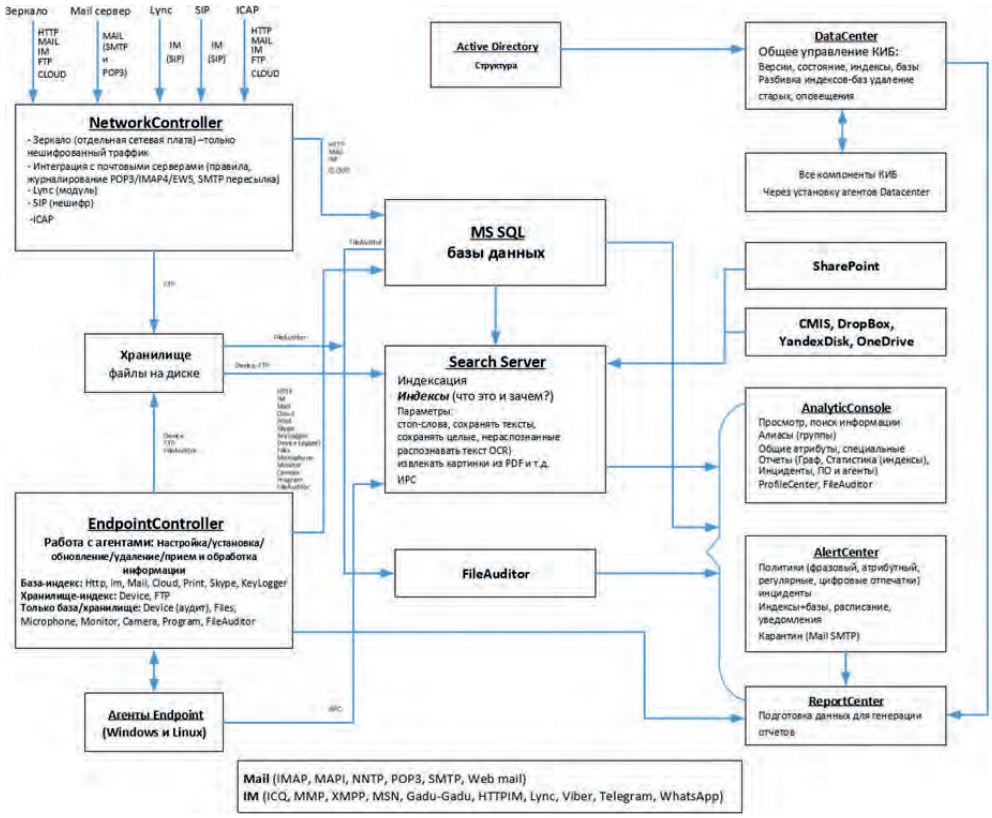


Рис. 2. Взаимодействие компонентов «КИБ СёрчИнформ»

КИБ разработан с учетом специфики работы крупных компаний. Основные достоинства системы:

- *Наиболее полный контроль информационных потоков.* КИБ контролирует все критичные для бизнеса каналы коммуникаций – Exchange, Lync, Skype, корпоративную телефонию, файловые сервера, Sharepoint, Office365, Cisco Messenger, Telegram, Zoom, Viber, WhatsApp, Slack, веб-почту, облачные хранилища, социальные сети, блоги, форумы. Комплексный контроль сетевых каналов делает возможным их безопасное использование. Отсутствие блокировок позитивно сказывается на бизнес-процессах и повышает эффективность коммуникации сотрудников;
- *Продвинутые технологии анализа.* Помимо «классических» технологий анализа (морфология, словари, регулярные выражения, цифровые отпечатки, OCR), в КИБ включены и собственные разработки компании, повышающие эффективность системы. Например, детектирование текстов, близких по смыслу или содержанию к эталонным. Поиск изображений, визуально похожих на эталон. Поиск по любым аудиозаписям (технология преобразования аудио в текст) и контентный поиск по видеозаписи действий пользователя (можно просматривать видео только интересующих действий, например, работы с конфиденциальным документом). Есть возможность построения контентных маршрутов для любых перехваченных файлов, а также профилирование пользователей на основе перехвата их переписок;
- *Качественные средства расследования.* КИБ дает службе ИБ средства для проведения детального наблюдения – позволяет делать аудио- и видеозапись действий пользователя, фиксировать любые

Рис. 3. Модули перехвата «КИБ Сёрчинформ»

его действия с файлами или папками, журналами регистрации событий (логами), устройствами, ПО. Также доступно аудио- и видеонаблюдение за нарушителями в реальном времени. Это помогает в расследовании инцидентов – *DLP*-система позволяет в точности воспроизвести нарушение и установить круг причастных лиц, что отсутствует во многих аналогичных системах и не позволяет полноценно разобраться в контексте нарушения. Также присутствуют средства журналирования действий сотрудников ИБ-службы в консолях AlertCenter, AnalyticConsole, DataCenter, EndpointController, NetworkController, *SIEM*. Тем самым снимается вопрос «кто будет контролировать контролеров». Эти журналы нельзя отредактировать;

- *Универсальное средство защиты информации.* КИБ работает как полноценная *DLP*-система, а также предоставляет дополнительные средства для ОИБ. В нее встроены, например, шифрование записываемых на внешний носитель документов, разграничение доступа к файловой системе, полноценный контроль терминальных серверов, аудит оборудования и ПО. Кроме того, КИБ может выступать как обработчиком информации, так и источником, что открывает широкие возможности по интеграции с другими системами;
- *Возможность контроля продуктивности пользователей в приложениях и на сайтах.* Она расширяет область применения *DLP*-систем, помогая повысить уровень общей дисциплины в компании, определить слабые места в бизнес-процессах. Это избавляет заказчика от необходимости закупать и сопровождать две различные системы с пересекающимися задачами и устанавливать два различных агентских модуля на каждый персональный компьютер (ПК) – все доступно в одном решении;
- *Продвинутые функции агента.* Агент *DLP*-системы «вычитывает» информацию об устройствах на ПК (видеоадаптеры, запоминающие устройства, мониторы и др.) и установленных программах, а затем сообщает службе ИБ об изменениях в конфигурации компьютеров. Помимо этого, агент выявляет сторонние программы контроля и *DLP*-системы на компьютерах пользователей;
- *Профайлинг.* Эта уникальная система компании «СёрчИнформ» автоматически анализирует переписку сотрудника в почте, мессенджерах и соцсетях и составляет его психологический портрет. Профайлинг указывает на сильные и слабые стороны сотрудника, находит точки давления, определяет склонность к преступлениям (с указанием, к каким именно);
- *Отслеживание и визуализация связей между сотрудниками.* Интерактивный граф отношений даёт наглядное представление о круге общения и контактах по основным каналам коммуникаций внутри компании и с внешними адресатами;
- *Разграничение прав доступа к информации.* Мощная ролевая модель дает возможность гибкой настройки прав доступа к перехваченной информации;
- *Наличие продуктов компании в реестре отечественного ПО.* КИБ имеет сертификат ФСТЭК по уровню доверия 4 (запись в реестре под № 4144). Средства защиты информации, соответствующие 4 уровню доверия, подлежат применению в значимых объектах КИИ 1 категории, в государственных информационных системах (ИС) 1 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами (АСУ ТП) 1 класса защищенности, в информационных системах (ИС) персональных данных (ПДн) при необходимости обеспечения 1 уровня защищенности ПДн, в ИС общего пользования 2 класса[11].

Контроль защищенности данных и выявления уязвимостей в доступе к ним

Решения класса *DCAP* предназначены для обнаружения, категоризации и защиты структурированных, неструктурированных и полуструктурированных данных. Речь идет об информации на ПК сотрудников, а также той, что разбросана по сетевым папкам, облачным хранилищам, БД и т.д. Реальная ситуация, когда все учтено и находится под контролем, характеризуется тем, что критичные данные не содержатся в единой базе, видоизменяются в каждой БД по-своему, а по пути еще и сохраняются пользователями на персональных устройствах, в облаках и общедоступных папках. В результате персональные, платежные, учетные данные, файлы с коммерческой тайной, чертежи и прочие технические документы бесконтрольно множатся, что создает как бизнес-риски, так и риски ИБ. *DCAP*-решения появились как ответ на описанные проблемы.

Несмотря на различия в функционале, *DCAP*-системы в «базовой» комплектации должны выполнять следующие функции:

- обнаруживать и классифицировать данные;
- проводить мониторинг прав доступа;
- отслеживать операции с данными;
- обеспечивать защиту данных, запрещая нежелательные операции с ними.

Успеху DCAP в значительной степени способствовало принятие законов о защите ПДн: регуляторы

11 Сертификаты и лицензии [Электронный ресурс] // SearchInform. URL: https://searchinform.ru/docs/ (дата обращения: 05.08.24).

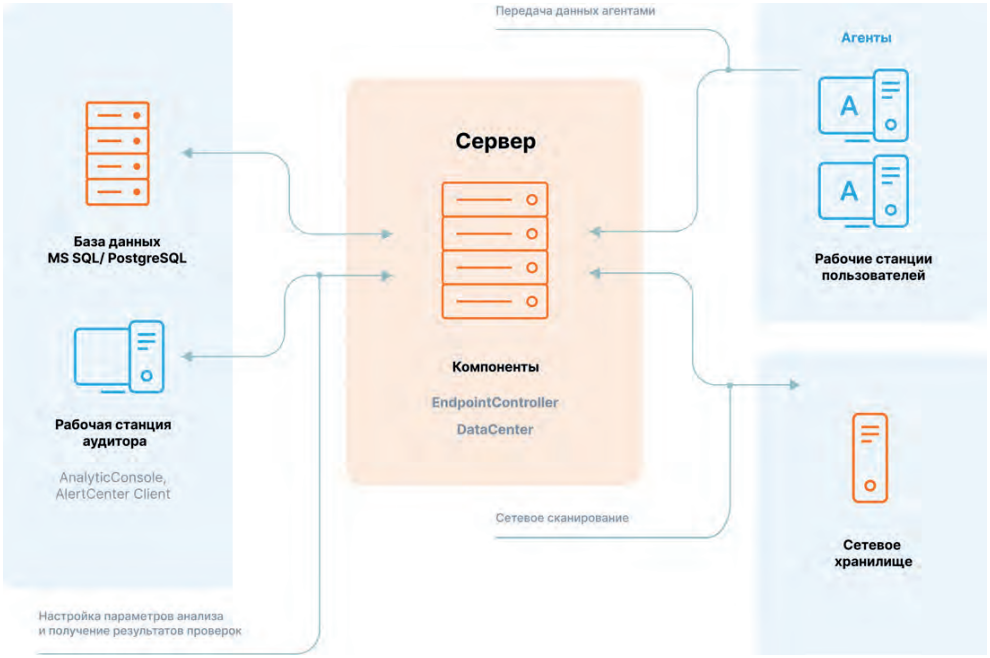


Рис. 4. Схема работы «FileAuditor»

твердо обозначили намерение жестко наказывать за утечку, справедливо считая, что вовремя обнаруженная «бесхозная» либо общедоступная информация позволяет избежать больших проблем. Первой среди отечественных разработчиков свое *DCAP*-решение «FileAuditor» выпустила компания Сёрч-Информ в 2019 г.

«FileAuditor» решает следующие задачи:

- *Классификация данных.* Позволяет выделить из общего документооборота информацию, подлежащую защите, и определить ее ценность. Структурированные данные легче защитить: для каждой группы данных (например, финансовая информация, ноу-хау) в «FileAuditor» можно разработать отдельный набор правил в соответствии с внутренними политиками ИБ и требованиями регуляторов;
- *Защита данных.* Программа проводит регулярный аудит мест хранения и обнаруживает конфиденциальные документы в любом месте корпоративной ИС – на ПК сотрудников, в сетевых папках и на файловых серверах;
- *Аудит доступа к данным.* Бизнес-информация становится уязвимой, когда ею делятся. Чем больше людей имеют доступ к данным, тем выше риск потерять ценные сведения. «FileAuditor» позволяет отслеживать группы сотрудников, которые создают, хранят или обрабатывают данные ограниченного доступа;
- *Контроль за действиями пользователей.* «FileAuditor» следит за тем, какие операции с конфиденциальными данными совершают пользователи и сверяется с политикой ИБ. Например, систему насторожит удаление критичных данных, перемещение конфиденциальных документов в общедоступные папки.

ИБ-специалист может задать для поиска документов конкретный текст, атрибут, директории, компьютер или их сочетание, что позволяет контролировать в первую очередь критичные данные.

Как уже было сказано, «FileAuditor» позволяет отслеживать наличие критичной информации на компьютерах пользователей и права доступа к файлам. Сканирование ресурсов согласно настроенным правилам, предоставление дерева папок/файлов, а также прав доступа к ним может осуществляться либо с помощью агента, либо с помощью службы анализа данных на сервере (рис. 4). Стоит упомянуть, что на агенте используется облегченная версия поискового «движка» – miniSearchServer, что приводит к ограничению аналитических функций (например, нет возможности распознавать текст из картинок, используются не все поддерживаемые типы поиска, а лишь некоторые из них и т.д.). С другой стороны, таким способом обеспечивается компромисс между скоростью, гибкостью и объемом потребных ресурсов.

Особого внимания заслуживает интеграция «FileAuditor» с КИБ, что позволяет автоматизировать выполнение ряда задач. Например, в «FileAuditor» можно настроить правило на поиск новых важных документов. Результаты поиска или аудита отображаются на отдельной вкладке приложения «Консоль аналитика». ИБ-специалист получает наглядную информацию – тип найденного файла в общей классификации и правило, под действие которого попадает данный файл и т.д. (рис. 5).

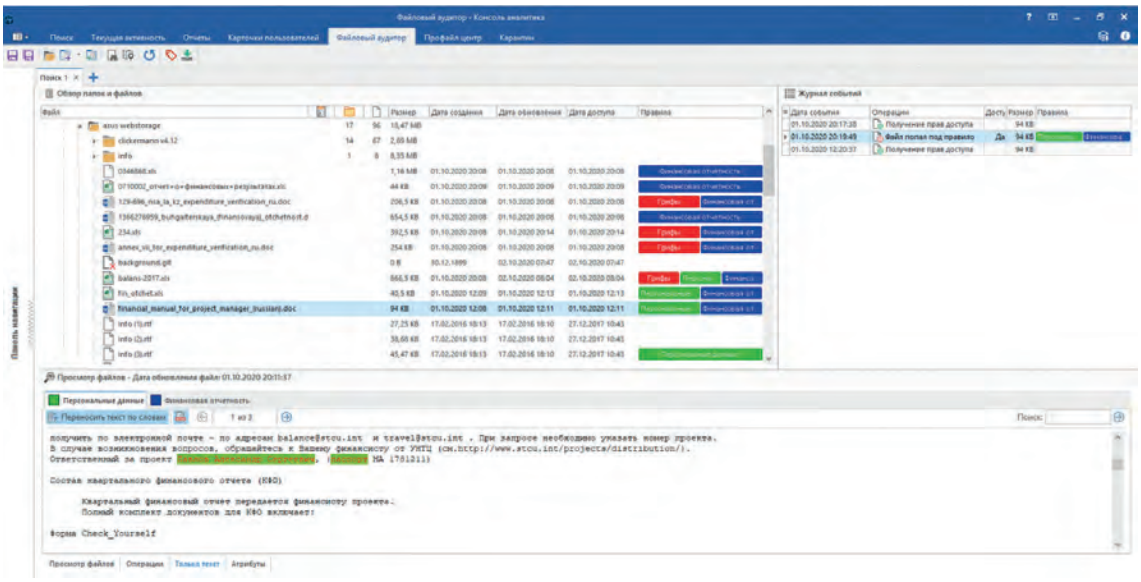


Рис. 5. «FileAuditor»: результаты поиска

Кроме того, «FileAuditor» позволяет практически мгновенно узнать, где лежат важные для организации документы, чтобы убедиться, что доступ к этим данным имеют только те сотрудники, которые в нем нуждаются (рис. 6).

А с помощью приложения AlertCenter можно оперативно получать соответствующие уведомления.

Управление событиями ИБ

В целом задача *SIEM*-систем – попытаться представить сетевую активность в удобном для восприятия виде. Эти системы появились как результат комбинации двух видов решений: *SIM* (*Security Information Management*) – управление информацией о безопасности и *SEM* (*Security Event Management*) – управление событиями безопасности. В общем случае *SIEM*-система призвана собирать, анализировать и представлять информацию из сетевых устройств и средств ОИБ. Также в эту систему должны входить приложения для управления идентификацией и доступом, уязвимостями приложений и БД. Как правило, *SIEM*-система реализует следующие функции: отправку предупреждений на основе предопределенных настроек, формирование отчетов и логирование для упрощения мониторинга ИБ, просмотр данных на разных уровнях детализации. Для этого *SIEM*-система собирает логи разных приложений, обрабатывает и кладет их в централизованное хранилище,

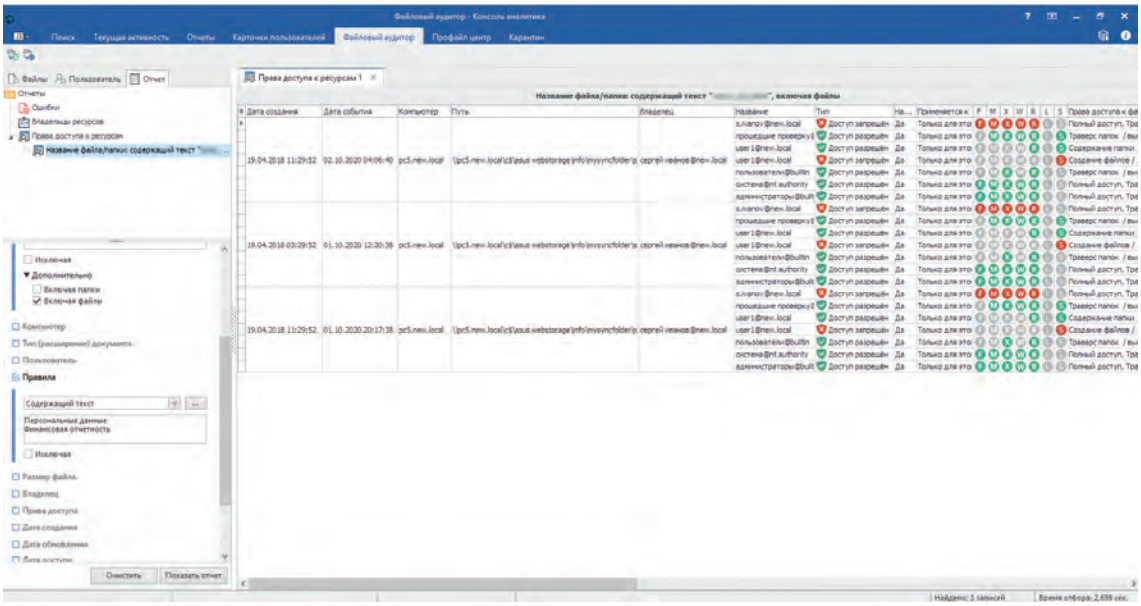


Рис. 6. «FileAuditor»: права доступа

DOI: 10.21681/2311-3456-2024-5-67-78

с которым удобно работать. Использование *SIEM*-системы позволяет увидеть более полную картину активности сети и события ИБ. В том числе и тогда, когда обычные средства обнаружения по отдельности не видят атаки, но она может быть обнаружена при тщательном анализе и корреляции информации из различных источников [13–15].

К типовым сценариям использования *SIEM*-системы можно отнести:

- отслеживание аутентификации и обнаружение компрометации учетных записей (аккаунтов) пользователей и администраторов;
- отслеживание случаев заражения и обнаружение вредоносного ПО;
- мониторинг подозрительного исходящего трафика и передаваемых по сети данных, обнаружение кражи данных и других подозрительных внешних соединений;
- отслеживание системных изменений и других административных действий во внутренних системах и их соответствия разрешенной политике ИБ;
- отслеживание атак на веб-приложения и их последствий, обнаружение попыток компрометации веб-приложений путем анализа разных отчетов.

«СёрчИнформ SIEM» представляет собой решение, предназначенное для сбора и автоматического анализа событий из различных корпоративных систем для выявления угроз и нарушений политик ИБ [15]. Источниками событий могут быть журналы контроллеров доменов, БД агентов «Сёрчинформ КИБ», сетевое оборудование, ПО и др. Система отслеживает события и автоматически, по настроенным правилам, выявляет потенциально опасные связи и цепочки таких событий. Правила анализа и формирования взаимосвязей между событиями предустановлены в систему, их остается только настроить «под себя».

Сбор данных для *SIEM*-системы, а также их нормализация и первоначальный анализ осуществляется в реальном времени с помощью коннекторов, обеспечивающих связь со всеми компонентами информационной инфраструктуры (рис. 7). Коннекторы собирают и анализируют события из различных источников данных. Например, WinEventConnector собирает и анализирует логи контроллеров домена, KavEventConnector подключается к БД Kaspersky Security Center и читает записи в ней, CiscoConnector собирает события сетевых устройств Cisco.

Коннекторы «СёрчИнформ SIEM» можно условно разделить на три группы:

1) сами собирающие события путем подключения к логам, журналам или базам источников данных (WinEventConnector, KAVConnector, ExchangeConnector и др.);
2) получающие события Syslog из различных аппаратных устройств или приложений (SyslogConnector, NetFlowConnector, LinuxConnector, CiscoConnector и др.);
3) собирающие события от установленного агента *SIEM*-системы (1CConnector, CWAConnector).

В БД «СёрчИнформ SIEM» под управлением СУБД MongoDB хранятся все события и инциденты, которые подпадают под заданные правила. Создание БД является необходимым условием для корректной работы *SIEM*-системы, независимо от перечня используемых коннекторов.

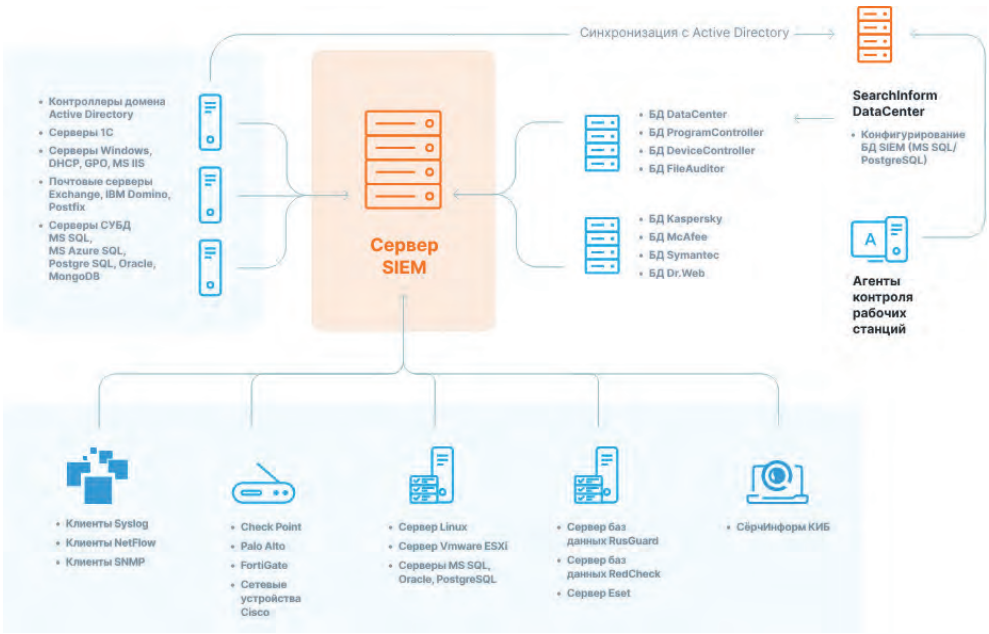


Рис. 7. Схема работы «СёрчИнформ SIEM»

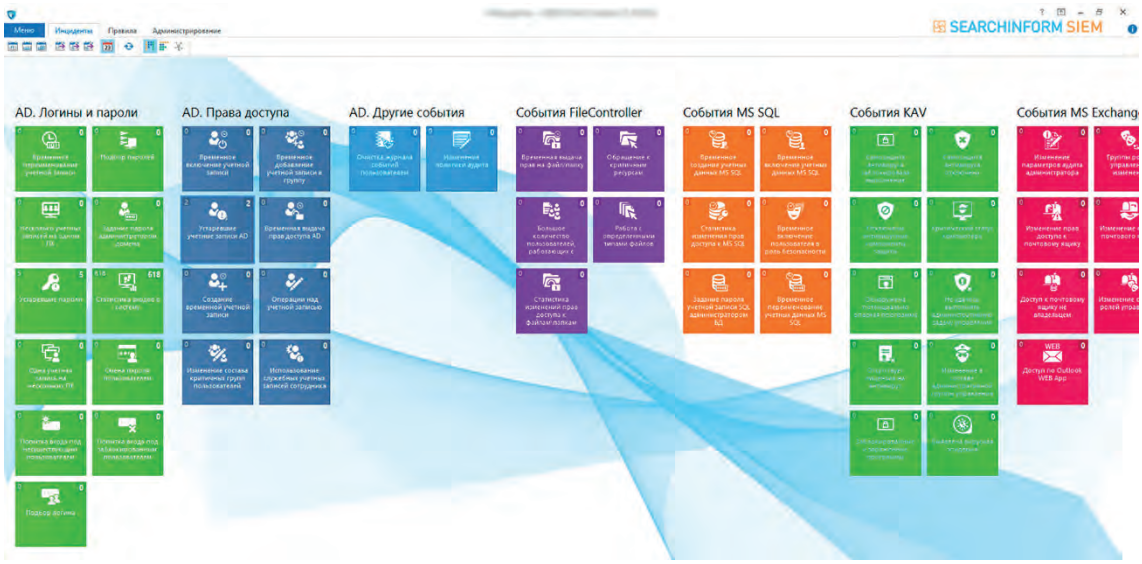


Рис. 8. «СёрчИнформ SIEM»: экран отображения инцидентов (правила визуализируются в виде плиток)

Сканер сети осуществляет сканирование локального сегмента корпоративной сети по заданным настройкам, в результате чего создается «слепок» объектов, который может использоваться для мониторинга, анализа и помощи в администрировании этой сети.

Для отображения связей объектов сети (компьютеров и пользователей), а также количества успешных/неуспешных подключений пользователей к компьютерам используется карта подключений. Она представляет собой граф, формируемый на основе событий по правилу «Статистика входов в систему» (WinEventConnector).

Правила *SIEM*-системы – набор параметров, которые определяют взаимосвязь между событиями, а также относят события к категории инцидентов ИБ (рис. 8). Между событиями и инцидентами ИБ есть отличия, причем события могут быть одинаковыми для всех организаций, а инциденты – только то, что сама организация таковыми посчитает. Например, событием считается каждый сеанс ввода пароля, а инцидентом ИБ – ввод пароля как минимум пять раз подряд за минуту. В системе есть предустановленные шаблоны правил по каждому коннектору, на основании которых можно создавать пользовательские правила.

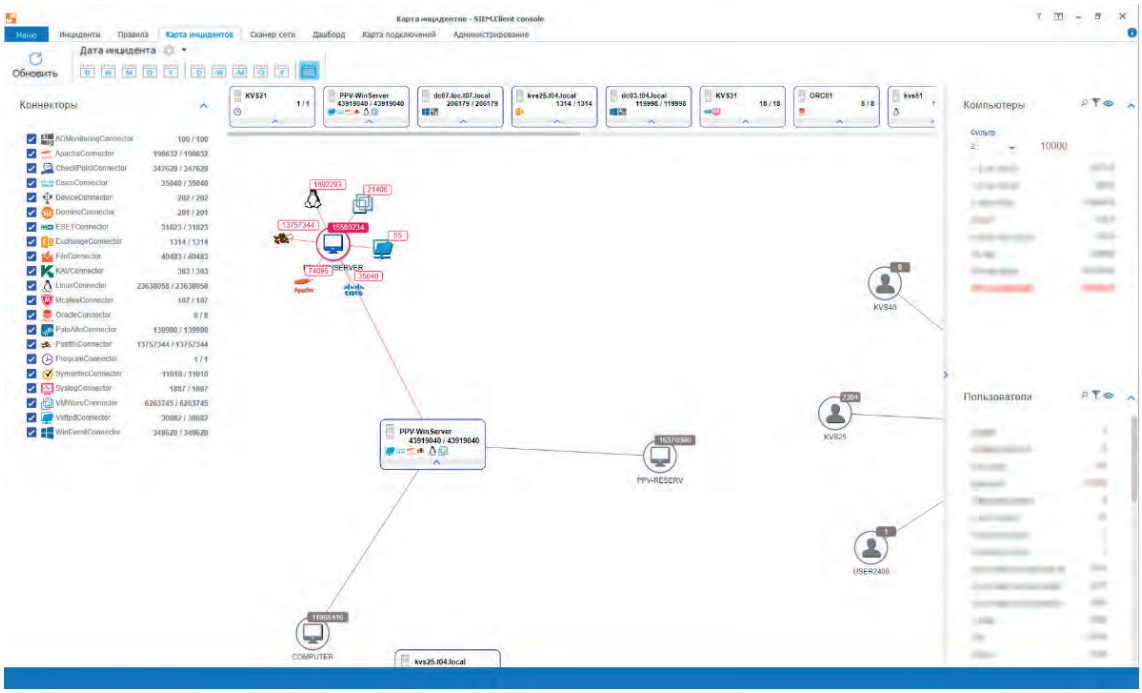


Рис. 9. «СёрчИнформ SIEM»: карта инцидентов

DOI: 10.21681/2311-3456-2024-5-67-78

Кросс-корреляцией называется перекрестное выявление зависимостей/корреляций между данными из разных источников, что позволяет более широко использовать возможности *SIEM*-системы, выявляя атаки и неполадки в сети по комплексным признакам. При помощи сервиса кросс-корреляции в «Сёрч-Информ SIEM» пользователь может сам создать необходимые ему правила на основании сопоставления событий из нескольких источников.

Карта инцидентов – граф, который интерпретирует структуру сети и объектов в ней (компьютеров и пользователей) в привязке к серверам с установленными коннекторами. На одноименной вкладке отображается общее количество инцидентов ИБ по каждому коннектору для определенного пользователя/компьютера (рис. 9). События на графе отображаются постепенно, порциями по 100 000; их можно детализировать.

Для отображения данных, собранных системой, в удобном формате, упрощения их анализа, отслеживания тенденций событий используется инфопанель «Дашборд» – панель ключевых показателей. На соответствующую вкладку можно добавить неограниченное количество виджетов. Каждый новый виджет создается на основе базового, но может иметь индивидуальные настройки (определенный набор пользователей, компьютеров, коннекторов и др.). По умолчанию имеется 12 базовых виджетов:

- топ дат по количеству событий;
- топ пользователей по количеству событий;
- копирование файлов на съемные устройства;
- события Syslog;
- использование учетных записей;
- обнаружение вирусов на ПК (Kaspersky Internet Security);
- обнаружение вирусов на ПК (SymantecEndpoint-Protection);
- обнаружение вирусов на ПК (McAfeeInternetSecurity);
- обнаружение вирусов на ПК (EsetSmartSecurity);
- обнаружение вирусов на ПК (Dr. Web);
- количество событий по датам;
- попытки входа.

С учетом всего вышесказанного многие организации рассматривают использование *SIEM*-системы в качестве дополнительного и очень важного элемента защиты от целенаправленных атак.

Выводы

С увеличением числа кибератак в ситуации растущей геополитической нестабильности становится ясно, что на сегодняшний день эффективное управление инцидентами ИБ превратилось в обязательную составляющую защиты информационно-технологических систем компаний самого различного масштаба. По результатам проведенного анализа содержания и роли процессов ОИБ в эффективной работе современных ИС следует сделать вывод о том, что для мониторинга событий, обнаружения угроз, соответствия требованиям и автоматизации процессов безопасности оптимальным набором характеристик обладает комплексное решение, интегрирующее в себе функционал *SIEM*-, *DCAP*- и *DLP*-систем.

Совместное использование рассмотренных в статье в качестве примера продуктов «СёрчИнформ SIEM», *DLP* «СёрчИнформ КИБ» и *DCAP* «FileAuditor» повышает уровень ИБ организации. *SIEM*-система выявляет аномальное поведение и определяет способ получения доступа к информации. *DLP*-система оценивает содержимое всех коммуникаций. *DCAP*-система отслеживает действия с данными, запрещая нежелательные операции. Высокоинтегрированная связка данных систем дает возможность максимально полно расследовать нарушения ИБ и собрать необходимую доказательную базу.

Комплексные системы защиты информации наиболее востребованы в государственных структурах, которые из-за специфики закупок с большей охотой приобретут одну интегрированную систему, чем несколько продуктов разного класса, назначения и, к тому же, предлагаемых разными вендорами. Проведенные исследования позволяют дать практические рекомендации для эффективного ОИБ и показывают, что предлагаемые подходы к управлению ИБ обеспечат поддержание требуемого уровня защищенности ИС предприятия в условиях динамически изменяющихся и развивающихся угроз.

Литература

1. *Страхов А. А., Дубинина Н. М. Об утечке данных и DLP-системах // Криминологический журнал. 2022. № 4. С. 226–232. DOI: 10.24412/2687-0185-2022-4-226-232.*
2. *Страхов А. А., Дубинина Н. М. О безопасности персональных данных // Криминологический журнал. 2024. № 1. С. 255–263. DOI: 10.24412/2687-0185-2024-1-255-263.*
3. *Токарев М. Н., Вершинин А. Н. Импортозамещение программного обеспечения // Международный журнал гуманитарных и естественных наук. 2023. № 6-3 (81). С. 156–162. DOI: 10.24412/2500-1000-2023-6-3-156-162.*
4. *Федоров А. В., Жихарев А. Г., Кальченко Д. М. Обеспечение информационной безопасности в органах исполнительной власти. Проблемы и решения // Научный результат. Информационные технологии. 2024. Т. 9, №1. С. 19-28. DOI: 10.18413/2518-1092-2024-9-1-0-3.*
5. *Полтавцева М. А. Модель активного мониторинга как основа управления безопасностью промышленных киберфизических систем // Вопросы кибербезопасности. 2021. № 2(42). С. 51-60. DOI: 10.21681/2311-3456-2021-2-51-60.*

6. Сизов В. А., Киров А. Д. Проблемы внедрения SIEM-систем в практику управления информационной безопасностью субъектов экономической деятельности // Открытое образование. 2020. Т. 24. № 1. С. 69–79. DOI: 10.21686/1818-4243-2020-1-69-79.
7. Сунаева Г. Г., Петрова К. А. Внедрение комплаенс-контроля в условиях цифровизации экономики // Вестник УГНТУ. Наука, образование, экономика. Серия экономика. № 2 (40), 2022. С. 16–23. DOI: 10.17122/2541-8904-2022-2-40-16-23.
8. Алексеев А. В., Куприянов Д. О., Стефанович И. Д., Заведеев Ю. М. Анализ интеллектуальных технологий управления ИБ морских интегрированных автоматизированных систем // Труды Крыловского государственного научного центра. 2021. № S1. С. 196–198. DOI: 10.24937/2542-2324-2021-1-S-I-196-198.
9. Morozov V., Miloslavskaya N. DLP Systems as a Modern Information Security Control. In: Samsonovich A., Klimov V. (eds) Biologically Inspired Cognitive Architectures (BICA) for Young Scientists. BICA 2017. Advances in Intelligent Systems and Computing, 2018 Vol. 636, Q4 pp. 296–301. DOI: 10.1007/978-3-319-63940-6_42
10. Зарубин А. В., Смирнов М. Б., Харитонов С. В., Денисов Д.В. Основные драйверы и тенденции развития DLP-систем в Российской Федерации // Прикладная информатика. 2020. Т. 15. № 3. С. 75–90. DOI: 10.377 91/2687-0649-2020-15-3-75-90.
11. Ying, Z., Wu, B. DLP: towards active defense against backdoor attacks with decoupled learning process. Cybersecurity 6, 9 (2023). DOI: 10.1186/s42400-023-00141-4.
12. Попугаева В. А., Шарыпова Т. Н. Особенности рынка DLP-систем // Colloquium-Journal. 2022. № 12-1 (135). С. 32–33. DOI: 10.24412/2520-6990-2022-12135-32-33.
13. Милославская Н. Г. Научные основы построения центров управления сетевой безопасностью в информационно-телекоммуникационных сетях / М.: Горячая линия – Телеком, 2021. – 432 с.
14. Кирсанов Д. Г., Айдинян А. Р. Эффективное обеспечение безопасности с помощью SIEM // Молодой исследователь Дона. 2024. № 9(3). С. 45–49.
15. Аникин И. В., Чепайкин Р. Н. Автоматизация процесса трансляции корреляционных правил для систем SIEM // Научные труды КубГТУ. 2023. № 4. С. 76–87.

COMPREHENSIVE SOLUTIONS TO MINIMISE INTERNAL INFORMATION SECURITY THREATS

Morozov V. E.[12], Miloslavskaya N. G.[13]

Purpose of work: *determination of the composition of modern solutions, which together allow creating a system of complex organization's information security management.*

Research methods: *analysis of relevant scientific publications, conceptual modelling, expert evaluation, synthesis of the system of complex information security managementf.*

Results obtained: *The article details the components of the information security (IS) management process and discusses the possible composition of a complex IS management system for an organisation focused on minimising internal threats. It is shown that such a system should include the following key elements: a subsystem of centralised monitoring of events and investigation of IS incidents, subsystem of data security control and identification of data access vulnerabilities, as well as a subsystem of control of data flows and counteraction to protected data breaches. These elements can be implemented by SIEM, DCAP and DLP systems, respectively. The main concepts and technologies on the basis of which these systems are developed, their architecture, features and analytical capabilities are considered using the example of software developed by the SearchInform company (SearchInform SIEM, SearchInform FileAuditor and SearchInform KIB). The analysis of all characteristics and experience in the use of these systems (provided they are integrated) shows that they can provide full-scale corporate protection at all levels.*

Practical significance *consists in substantiating the sufficiency of the specified composition of the IS management system to solve the problem of minimising internal threats.*

Keywords: *DLP, DCAP, SIEM, internal information security threats, information security incident, monitoring, information security event, information security management.*

References

1. Strakhov A. A., Dubinina N. M. Ob utechke dannykh i DLP-sistemakh // Kriminologicheskiy zhurnal. 2022. № 4. S. 226-232. DOI: 10.24412/2687-0185-2022-4-226-232.
2. Strakhov A. A., Dubinina N. M. O bezopasnosti personal'nykh dannykh // Kriminologicheskiy zhurnal. 2024. № 1. S. 255–263. DOI: 10.24412/2687-0185-2024-1-255-263.
3. Tokarev M. N., Vershinin A. N. Importozameshcheniye programmnogo obespecheniya // Mezhdunarodnyy zhurnal gumanitarnykh i yestestvennykh nauk. 2023. № 6-3 (81). S. 156–162. DOI: 10.24412/2500-1000-2023-6-3-156-162.
4. Fedorov A. V., Zhikharev A. G., Kal'chenko D. M. Obespecheniye informatsionnoy bezopasnosti v organakh ispolnitel'noy vlasti. Problemy i resheniya // Nauchnyy rezul'tat. Informatsionnyye tekhnologii. 2024. T. 9, №1. S. 19-28. DOI: 10.18413/2518-1092-2024-9-1-0-3.

12 Victor E. Morozov, Ph.D Associate Professor, Specialist of LLC «Librasoft», Minsk, Belarus. E-mail: v.morozov@searchinform.ru
13 Natalia G. Miloslavskaya, Dr.Sc., Ph.D in Cybersecurity, Associate Professor, Professor Dep. of Information Security of Banking Systems of National Research Nuclear University MEPhI, Moscow, Russia. E-mail: NGMiloslavskaya@mephi.ru

5. *Poltavtseva M. A. Model' aktivnogo monitoringa kak osnova upravleniya bezopasnost'yu promyshlennykh kiberfizicheskikh sistem // Voprosy kiberbezopasnosti. 2021. № 2(42). S. 51–60. DOI: 10.21681/2311-3456-2021-2-51-60.*
6. *Sizov V. A., Kirov A. D. Problemy vnedreniya SIEM-sistem v praktiku upravleniya informatsionnoy bezopasnost'yu sub"yektov ekonomicheskoy deyatel'nosti // Otkrytoye obrazovaniye. 2020. T. 24. № 1. S. 69–79. DOI: 10.21686/1818-4243-2020-1-69-79.*
7. *Sunayeva G. G., Petrova K. A. Vnedreniye komplayens-kontrolya V usloviyakh tsifrovizatsii ekonomiki // Vestnik UGNTU. Nauka, obrazovaniye, ekonomika. Seriya ekonomika. № 2 (40), 2022. S. 16–23. DOI: 10.17122/2541-8904-2022-2-40-16-23.*
8. *Alekseyev A. V., Kupriyanov D. O., Stefanovich I. D., Zavedeyev YU. M. Analiz intellektual'nykh tekhnologiy upravleniya IB morskikh integrirovannykh avtomatizirovannykh sistem // Trudy Krylovskogo gosudarstvennogo nauchnogo tsentra. 2021. № S1. S. 196–198. DOI: 10.24937/2542-2324-2021-1-S-I-196-198.*
9. *Morozov V., Miloslavskaya N. DLP Systems as a Modern Information Security Control. In: Samsonovich A., Klimov V. (eds) Biologically Inspired Cognitive Architectures (BICA) for Young Scientists. BICA 2017. Advances in Intelligent Systems and Computing, 2018 Vol. 636, Q4 pp. 296–301. DOI: 10.1007/978-3-319-63940-6_42*
10. *Zarubin A. V., Smirnov M. B., Kharitonov S. V., Denisov D.V. Osnovnyye drayvery i tendentsii razvitiya DLP-sistem v Rossiyskoy Federatsii // Prikladnaya informatika. 2020. T. 15. № 3. S. 75–90. DOI: 10.377 91/2687-0649-2020-15-3-75-90.*
11. *Ying, Z., Wu, B. DLP: towards active defense against backdoor attacks with decoupled learning process. Cybersecurity 6, 9 (2023). DOI: 10.1186/s42400-023-00141-4.*
12. *Popugayeva V. A., Sharypova T. N. Osobennosti rynka DLP-sistem // Colloquium-Journal. 2022. № 12-1 (135). S. 32–33. DOI: 10.24412/2520-6990-2022-12135-32-33.*
13. *Miloslavskaya N. G. Nauchnyye osnovy postroyeniya tsentrov upravleniya setevoy bezopasnost'yu v informatsionno-telekommunikatsionnykh setyakh / M.: Goryachaya liniya – Telekom, 2021. – 432 s.*
14. *Kirsanov D. G., Aydinyan A. R. Effektivnoye obespecheniye bezopasnosti s pomoshch'yu SIEM // Molodoy issledovatel' Dona. 2024. № 9(3). S. 45-49.*
15. *Anikin I. V., Chepaykin R. N. Avtomatizatsiya protsessa translyatsii korrelyatsionnykh pravil dlya sistem SIEM // Nauchnyye trudy KubGTU. 2023. № 4. C. 76–87.*

СРАВНИТЕЛЬНЫЙ АНАЛИЗ И ВЫБОР СТАТИЧЕСКИХ АНАЛИЗАТОРОВ БЕЗОПАСНОСТИ КОДА

Марков А. С.[1], Антипов И. С.[2], Арустамян С. С.[3], Магакелова Н. А.[4]

DOI: 10.21681/2311-3456-2024-5-79-88

Цель работы: *разработка методического подхода к проведению сравнительного анализа статических анализаторов безопасности исходного кода, применимых при сертификации средств защиты информации, по критериям результативности, применимости, функциональности и удобства, а также его демонстрация на примерах.*

Метод исследования: *анализ нормативных и методических документов по проведению статического анализа и по оценке статических анализаторов исходного кода программ с целью формирования методики их сравнения и выбора.*

Полученный результат: *приведены результаты анализа и синтеза системы показателей качества проприетарных анализаторов безопасности кода и анализаторов кода с открытым кодом, а также результаты их сравнения на реальных продуктах, что позволяет сформировать необходимую инструментальную базу сертификационных испытаний программных средств защиты информации по требованиям безопасности информации и сертификации процессов разработки безопасного программного обеспечения.*

Научная новизна: *проанализированы нормативные документы в области статического анализа кода применительно к решению задачи анализа и подбора нескольких статических анализаторов безопасности, приведены критерии выбора, выбраны тестовые продукты и проведен эксперимент, который продемонстрировал различную результативность анализаторов безопасности кода при сертификации.*

Вклад авторов: *Марков А. С. – разработка методического подхода, редактирование, Антипов И. С., Арустамян С. С., Магакелова Н. С. – проведение эксперимента.*

Ключевые слова: *программная безопасность, безопасные программные ресурсы, анализ безопасности программ, уязвимости, недекларированные возможности, программные закладки, инструментарий сертификационных испытаний.*

Введение

Статические анализаторы безопасности кода являются обязательным инструментарием выявления дефектов безопасности и неизвестных уязвимостей как в процессе испытаний программных средств защиты информации [1], так и при оценке соответствия процессов разработки безопасного программного обеспечения [2]. Применение статического анализа при испытаниях, как известно, обусловлено возможностью управления полнотой покрытия кода, принципиальным выявлением закладок (связанных с редко используемыми входными данными), независимостью от среды выполнения, прозрачностью расследований в случае преднамеренных инцидентов, контролем качества кодирования кода, возможностью выявления заимствованных компонент и подобных фрагментов (с целью оценки безопасности и выполнения распараллеливания и прочей оптимизации) и пр. В рамках разработки безопасного программного обеспечения внедрение статических анализаторов возможно на самых ранних стадиях разработки, что радикально снижает затраты на исправление ошибок и уязвимостей на последующих этапах жизненного цикла изделий.

Особенностью отечественного законодательства является замечание по использованию нескольких статических анализаторов кода, что обусловлено не просто борьбой с ошибками 1 и 2 рода, а повышением уровней достоверности и полноты испытаний. В то же время понятно, что различные статические анализаторы отличаются друг от друга множеством параметров, как-то: полнота поддержки базы дефектов (в частности, CWE), интеграция с динамическим анализом и всем жизненным циклом сертификации, удобством, поддержкой языков программирования и сред, возможностью абстрагирования от синтаксиса языка, стоимостью продукта и стоимостью поддержки, наконец, наличием сертификата и т.д. Вопросом комплексного сравнения статических анализаторов, применимых при сертификации средств защиты информации, посвящено данное исследование. Указанная статья родилась не на пустом месте, так как авторы участвовали в обсуждении

1 Марков Алексей Сергеевич, доктор технических наук, заведующий кафедрой 43 НИЯУ МИФИ, Москва, Россия. E-mail:asmarkov@mephi.ru
2 Антипов Илья Сергеевич, эксперт испытательной лаборатории АО «НПО «Эшелон», Москва, Россия. E-mail: mail@cnpo.ru
3 Арустамян Сас Сергеевич, заместитель руководителя испытательной лаборатории АО «НПО «Эшелон», Москва, Россия E-mail:s.arustamyan@npo-echelon.ru
4 Магакелова Нелли Александровна, эксперт испытательной лаборатории АО «НПО «Эшелон», Москва, Россия E-mail:mail@cnpo.ru

международного стандарта по статическим анализаторам – SATEC (Static Analysis Technologies Evaluation Criteria) [3] и проводили ранее подобные изыскания [4, 5], а также участвовали в обсуждении требований к статическим анализаторам по линии технического комитета ТК-362 («Защита информации»). В литературе можно встретить ряд весьма интересных тематических исследований для отдельных языков и приложений [6–12]. Авторы постарались учесть накопленный опыт и представить материал с точки зрения испытательной лаборатории.

Постановка задачи

В настоящее время известно множество способов и техник статического анализа безопасности программ, наиболее популярными из которых можно назвать следующие [1, 13]:

- тестирование по формальным моделям представления программного кода;
- сигнатурный метод выявления и анализа потенциально опасных фрагментов кода (по заранее выявленным шаблонам);
- эвристический метод выявления и анализа потенциально опасных фрагментов кода;
- межпроцедурный контекстно-чувствительный анализ;
- чувствительный к путям выполнения анализ;
- межмодульный анализ;
- анализа потока управления;
- анализ потока данных и др.[5]

Данная работа не имеет целью исследования глубины реализации указанных способов и техник, а ориентирована на повышение эффективности работы испытательной лаборатории, которая руководствуется необходимыми отечественными нормативно-правовыми актами. В этом плане были определены четыре задачи исследования:

1. Оценить результативность применения статических анализаторов;
2. Оценить применимость их в испытательных лабораториях, аккредитованных в различных системах сертификации;
3. Оценить функциональность анализаторов в плане необходимости и достаточности при выполнении сертификационных испытаний;
4. Оценить дополнительные показатели качества, которые бывают полезными и удобными.

В качестве стенда исследования использовался реальный полигон испытательной лаборатории НПО «Эшелон». В качестве объектов испытаний были выбраны пять доступных статических анализаторов безопасности кода, а именно:

- AK-BC 3.0 – коммерческий анализатор, поддерживающий C/C++, C#, Java, Python, PHP;
- Cppcheck – open-source анализатор, поддерживающий C/C++;
- Clang SA – open-source анализатор, поддерживающий C/C++, Objective-C;
- Horusec – open-source анализатор, поддерживающий C#, Java, Kotlin, Python, Ruby, Golang, Terraform, Javascript, Typescript, Kubernetes, PHP, C, HTML, JSON, Dart, Elixir, Shell, Nginx;
- Svace – коммерческий анализатор, поддерживающий C/C++, C#, Java, Kotlin и Go.

Оценка результативности статических анализаторов

С точки зрения программной безопасности базовым ее фактором представляются дефекты безопасности (weaknesses). Поэтому, казалось бы, логичным для оценки безопасности использовать программные тестовые средства с *известными* уязвимостями и сопоставить дефекты. Таким качеством обладают синтетические тесты [4, 5]. С другой стороны, испытательная лаборатория проводит, по сути, исследование кода с целью досконального изучения его уровня безопасности, а не тривиально сканирует программный продукт по базе известных уязвимостей. В данном исследовании из любопытства для тестирования был выбран ряд популярных продуктов с открытым кодом, а именно:

- FFmpeg – open-source коллекция библиотек и инструментов для обработки мультимедийного контента, такого как аудио, видео, субтитры и связанные с ними метаданные;
- Firebird – open-source реляционная база данных, предлагающая множество стандартных функций ANSI SQL, которая работает на Windows, MacOS, Linux и других различных платформах Unix;
- Httpd – open-source веб-сервер, совместимый с HTTP/1.1;
- Librdkafka – open-source реализация библиотеки C протокола Apache Kafka;
- Ruby – это интерпретируемый объектно-ориентированный язык программирования, часто используемый для веб-разработки;
- Unit – легкий и универсальный сервер с открытым исходным кодом;
- Vim – open-source редактор.

Исследование указанных продуктов показало наличие достаточно большого количества некорректностей кода и дефектов безопасности, которые, как известно, классифицируют по каталогу MITRE CWE (Common Weakness Enumeration). Как известно, дефекты потенциально способны привести к уязвимостям, наличие которых может составлять угрозу, что требует дополнительного тестирования продукта

5 ГОСТ Р 71207-2024 «Защита информации. Разработка безопасного программного обеспечения. Статический анализ программного обеспечения. Общие требования». М.: Российский институт стандартизации, 2024. – 20 с.

Таблица 1

Дефекты кода по классификации CWE, обнаруженные статическими анализаторами

Продукт	Статический анализатор кода				
	АК-ВС 3	**Cppcheck**	**Clang SA**	**Horusec**	**Svace**
FFmpeg	14, 114, 134, 259, 394, 398, 480, 511, 563, 569, 570, 571, 628, 665, 667, 672, 690, 758, 798	190, 398, 457, 476, 562, 682, 758, 775, 786, 788	-	2, 20, 12, 36, 37, 78, 119, 120, 126, 134, 190, 327, 352, 362, 367, 676, 798, 807, 82	-
firebird	378, 401, 465, 476, 563, 672	401, 415, 457, 562	-	312, 798	-
httpd	121, 188, 243, 259, 369, 416, 465, 467, 476, 561, 563, 587, 672, 676, 690, 704, 775, 788, 824, 1041	398, 457, 476, 758	-	489	-
librdkafka	14, 369, 398, 401, 416, 465, 476, 561, 563, 569, 570, 571, 670, 676, 761, 763, 770, 824	398, 401, 476, 628, 682, 685, 768	-	2, 12, 20, 36, 37, 78, 119, 120, 134, 190, 312, 327, 676, 704, 798, 807	-
ruby	14, 134, 401, 404, 480, 563, 570, 672, 676, 770	398, 401, 415, 457, 476, 562, 628, 682, 758	-	2, 12, 20, 22, 36, 37, 73, 78, 119, 120, 126, 134, 190, 250, 312, 352, 362, 327, 676, 785, 798, 807, 829	-
unit	401, 416, 465, 476, 561, 563, 570, 763, 824	398, 401, 457, 476, 562	-	2, 12, 20, 22, 36, 37, 73, 89, 119, 120, 134, 190, 209, 250, 327, 330, 362, 367, 539, 611, 676, 704, 785, 798, 807	-
vim	121, 134, 188, 369, 401, 416, 465, 466, 476, 502, 561, 563, 569, 587, 672, 676, 681, 704, 763, 775, 788, 824, 1041	398, 401, 457, 476, 672, 775, 788	-	352, 798	-
«-» – не поддерживает идентификаторы CWE					

в реальных условиях на реальном объекте информатизации.

Дефекты безопасности, которые экспертами испытательной лаборатории признаны достоверными, приведены в табл. 1, которая содержит идентификаторы по MITRE CWE.

Представленная таблица демонстрирует, что тезис экспертов ТК-362 по использованию пары анализаторов при проведении статического анализа, является допустимым подходом, поскольку каждый статический анализатор обладает своими особенностями и алгоритмами.

Легко показать, что продемонстрированный в таблице результат позволяет перейти к количественным (объективным) показателям оценки продукта и планирования испытаний, воспользовавшись *математическими моделями полноты испытаний* [1, 14]. Например, для простоты предположим, что в испытании

Таблица 2.

Соответствие методике ФСТЭК России

Критерий	Статический анализатор кода				
	АК-ВС 3.0	Cppcheck	Clang SA	Horusec	Svace
Основные требования по статическому анализу кода	+	+	+	+	+
Дополнительные требования по статическому анализу*	+	-	+	-	+
* – отдельные требования выполняется экспертным путем					

Таблица 3.

Соответствие руководящему документу Гостехкомиссии России

Критерий		Статический анализатор кода				
		АК-ВС 3.0	Cppcheck	Clang SA	Horusec	Svace
Статический анализ исходных текстов программ	Контроль полноты и отсутствия избыточности исходных текстов ПО (на уровне файлов)	+	-	-	-	-
	Контроль соответствия исходных текстов ПО его объектному (загрузочному) коду	-*	-*	-*	-*	-*
	Контроль связей функциональных объектов по управлению	+	-	-	-	-
	Контроль связей функциональных объектов по информации	+	-	-	-	-
	Контроль информационных объектов	+	-	-	-	-
	Контроль наличия заданных конструкций в исходных текстах	+	-	-	-	-
	Формирование перечня маршрутов выполнения функциональных объектов	+	-	-	-	-
	Анализ критических маршрутов выполнения функциональных объектов	+	-	-	-	-
	Анализ алгоритма работы функциональных объектов на основе блок-схем, диаграмм и т. п., построенных по исходным текстам контролируемого ПО	+	-	-	-	-
	Контроль связей функциональных объектов по управлению	+	-	-	-	-
«-*» – выполняется экспертным путем						

приложения vim участвует две группы экспертов: одна группа использует коммерческий сканер, а вторая – сканеры с открытым кодом. Тогда, опираясь на модель парной оценки, можно предположить, что в продукте еще присутствует 24 дефекта CWE:

$$\bar{N} = N - (N_1 + N_2 - N_{12}) = 23.4, \quad (1)$$

где: N_1 – число дефектов, обнаруженных АК-ВС, N_{12} – число совпавших дефектов, $N = N_1N_2/N_{12}$.

Оценка применимости статических анализаторов

Степень применимости статических анализаторов оценивалась, исходя из реализации ими требований регуляторов (Минобороны России, ФСБ России и ФСТЭК России). Как известно, системы сертификации средств защиты информации опираются на два документа, а именно:

- Методический документ. Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении (утв. ФСТЭК России 2021 г.);
- Руководящий документ. Защита от НСД к информации. Часть 1. ПО СЗИ. Классификация по уровню контроля отсутствия недекларированных возможностей (утв. Гостехкомиссией России 1999 г.).

Методический документ обязателен в сфере компетенции ФСТЭК России, а руководящий документ используется в остальных системах обязательной сертификации средств защиты информации, а также рядом отраслевых регуляторов.

Поэтому в следующих табл. 3 и 4 приведен сравнительный анализ статических анализаторов на предмет выполнения требований указанных документов.

Как видно из табл. 2, ряд статических анализаторов технически применим при испытаниях по требованиям методического документа ФСТЭК России (в части межмодульного анализа, символьного выполнения и анализа, чувствительного к путям выполнения и др.). Заметим, что методический документ ФСТЭК России перекликается с ГОСТ Р 71207-2024 «Защита информации. Разработка безопасного программного обеспечения. Статический анализ программного обеспечения. Общие требования».

Заметим, что в данном исследовании мы ограничились требованиями именно по статическому анализу, в то время как комплексный продукт (в данном случае АК-ВС) может поддерживать весь цикл сертификационных испытаний.

Оценка функциональности и удобства статических анализаторов

Хорошие практики информационной безопасности утверждают, что вопросы безопасности должны быть в гармонии еще с двумя свойствами, как-то: функциональностью и удобством [15]. Исходя из этого, авторы воспользовались популярными зарубежными стандартами, касающимися качества статических анализаторов, а именно:

1. NIST 500-268. Source Code Security Analysis Tool Function Specification [16];
2. Static Analysis Technologies Evaluation Criteria [17].

Стандарт NIST SP 500-268 определяет требования к работе анализаторов исходных текстов, что позволяет выявить минимальный набор возможностей анализатора.

SATEC является метастандартом и содержит подробный список «общих» критериев оценки, которые могут быть основой для формирования гибких частных требований!

Сравнительный анализ по критериям функциональности и удобства включал следующие пункты оценки:

- наличие минимально необходимых возможностей (согласно NIST);
- наличие дополнительных возможностей (согласно SATEC);

Результаты указанных оценок представлены соответственно в табл. 4 и 5.

Следует отметить, что существует три способа управления результатами (отчетами) статического анализа: группировка и сортировка, удаление ненужных результатов, комментарии к результатам работ статического анализатора. Группировка и сортировка позволяет, среди прочего, пометить группу триггерных событий как «ложноположительные» (false positive), таким образом, нет необходимости отмечать каждое триггерное событие отдельно.

Сравнив данные табл. 4 и 5, можно сделать вывод, что коммерческие анализаторы справляются с задачей предоставления результатов анализа кода в удобной для экспертов форме. Большинство анализаторов кода позволяют группировать и сортировать результаты, переопределять ложноположительные триггерные события, в частности, АК-ВС 3, по мнению авторов, имеет возможность получать удобные отчеты с разным уровнем детализации [17, п. 6.1].

Надо понимать, что доверие к сертификации основано на объяснении результатов. В этом плане АК-ВС 3.0, Cppcheck и Horusec соответствуют ожиданиям, так как поддерживают международный каталог дефектов CWE. Указанное позволяет подстроиться под систематику ФСТЭК России (угрозы по БДУ – уязвимости по БДУ – дефекты CWE).

Следует отметить важность возможности настройки набора правил проверки статических анализаторов, что позволяет рационально использовать временные и материальные ресурсы испытательной лаборатории. В данном случае мы можем говорить не только о результативности испытаний, но и об эффективности.

Таблица 4.

Соответствие руководящему документу Гостехкомиссии России

Критерий	Статический анализатор кода				
	АК-ВС 3.0	**Cppcheck**	**Clang SA**	**Horusec**	**Svace**
Формирование высокоуровневого отчета [16, п. 2.1]					
Определение выбранного класса дефектов	+	+	+ (CWE не пишется в явном виде)	+	+ (CWE не пишется в явном виде)
Сообщение о типе и месте дефекта	+	+	+	+	+
Создание отчета, совместимого с другими инструментами	+ (csv)	+ (.txt, xml)	-	+ (Sonarqube)	+ (Sarif, csv)
Возможность отключения сообщений о выбранных дефектах	+ (через комментарии в исходном коде)	+ (поштучно или по классам)	+ (по файлам)	+ (сложная настройка)	-
Использование общепринятых имен для классов дефектов	+	+	-	+	-
Обязательные требования [16, п. 2.2]					
SCSA-RM-1: Определение классов дефектов по NIST	+	+	-	+	-
SCSA-RM-2: Текстовый отчет о любых дефектах	+	+	+	+	+
SCSA-RM-4: Возможность указания каталога, файла и номера строки для дефекта	+	+	+	+	+
Дополнительные требования [16, п. 2.3]					
SCSA-RO-1: Возможность создания отчета в формате XML	-	+	-	-	-
SCSA-RO-3: Указание номера и класса CWE	+	+	-	+	-

Таблица 5.

Расширенные возможности статических анализаторов

Критерий	Статический анализатор кода				
	АК-ВС 3.0	**Cppcheck**	**Clang SA**	**Horusec**	**Svace**
Поддержка командной строки [17, п. 3.1]					
Поддержка командной строки	+	+	+	+	+
Поддержка интеграции с IDE [17, п. 3.2]					
Указание, какие IDE (и версии) поддерживаются, и что включает в себя проверка кода с помощью IDE	+	+	+	+	+
Системная поддержка [17, п. 3.3]					
Перечисление поддерживаемых систем сборки и их версии	+	+	-	+	+

Индивидуальная настройка [17, п. 3.4]					
Возможность добавить, удалить, изменить основные сигнатуры	-	+	-	+	-
Возможность создания авторских сигнатур	-	+	-	+	-
Возможности конфигурирования анализом [17, п. 3.5]					
Возможность планирования проверки	-	-	-	-	-
Возможность просмотра статуса выполняемых проверок в режиме РВ	+	+	+	+	+
Возможность сохранять конфигурации и повторно использовать их в качестве шаблонов конфигурации	-	+	+	-	-
Возможность одновременного выполнения нескольких проверок	+	-	+	+	+
Возможность поддержки нескольких пользователей	+	-	+	+	+
Возможность выполнения инкрементальных проверок	-	+	+	-	+
Возможности тестирования по безопасности [17, п. 3.6]					
Возможность точно идентифицировать и сообщать о возможных атаках и уязвимостях безопасности	+	+	+	+	+
Поддержка отчетов по ролям [17, п. 6.1]					
Представление краткого изложения результатов проверки на высоком уровне (для руководства)	+	+	+	+	+
Предоставление технического детального отчета: ■ с кратким описанием проблемы, включая категорию дефектов	+	-	-	+	-
■ с указанием местонахождения проблемы, включая имя файла и номер строки кода	+	+	+	+	+
■ с рекомендациями по устранению, которые должны быть настроены для каждой проблемы и включают примеры кода на выбранном языке	-	+	-	-	-
■ с подробной информацией о потоке, которая показывает поток помеченных (tainted) данных от источника к получателю	+	+	+	-	+
Персонализация отчетов [17, п. 6.2]					
Возможность включить в отчет комментарии экспертов	+	-	-	+	-
Возможность отмечать результаты как ложные срабатывания и удалять их из отчета	-	-	-	+	-
Форматы отчетов [17, п. 6.3]					
Поддерживаемые форматы отчетов (PDF, XML, HTML и т. д.)	+ (html, csv)	+ (xml, html)	+ (html)	+ (html, json)	+ (pdf, csv, json)
Поддержка корпоративного уровня [17, п. 7]					
Интеграция в системы отслеживания ошибок	+	+	+	+	+
Наличие платной лицензии (поддержка)	+	+	-	-	+

Выводы по эксперименту

Для визуализации результатов сравнений статических анализаторов использована лепестковая диаграмма (рис. 1), где ее параметрами являются экспертная оценка показателей *применимости* (полнота соответствия документам регуляторов), *функциональности* (выполнимости необходимых и достаточных требований) и *удобства* (реализации дополнительных удобных функций). Материалы первой таблицы (*результативность*) решили не выносить на рисунок, так как два статических анализатора в принципе не поддерживают CWE (оценку об обязательности этого критерия оставим на решение экспертов органов по сертификации), ну и выбор тестовых продуктов выполнен экспертным путем, то есть обладает известной степенью субъективизма.

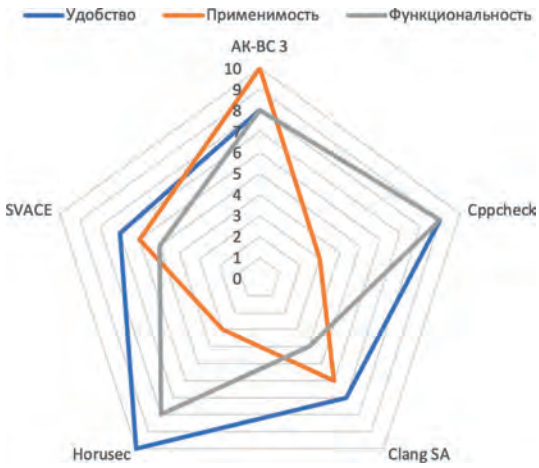


Рис. 1. Диаграмма выбора статического анализатора

Заключение

Использование статических анализаторов безопасности программного кода является необходимой процедурой оценки соответствия программного обеспечения по требованиям безопасности информации. Востребованность в таком инструментарии растет в связи с внедрением процедур разработки безопасного программного обеспечения и сертификации соответствующих процессов [2].

Приведенное исследование показало, что на сегодня оправдано указание по использованию нескольких статических анализаторов в процессе сертификации. Такой подход может быть легко обоснован математически [14].

Авторы полагают, что, с точки зрения испытательной лаборатории, предпочтителен унифицированный подход, как в плане формирования единой интегрированной среды всех сертификационных проверок и отчетов, так и поддержки концепции БДУ ФСТЭК России (BDU-CWE). В статье отмечен большой пул параметров, которые можно использовать при детальном сравнении (например, поддержка языков, наличие сертификата и поддержки). Интересен и подход SATEC к созданию метастандарта.

Проведенный эксперимент не претендует на абсолютную полноту, однако демонстрирует допустимость предложенного методического подхода. Исследование было сфокусировано именно на сертификационных испытаниях, то есть обсуждение ряда анализаторов кода, используемых при аудите отдельных программных приложений, вышло за рамки исследования.

В заключение следует сказать, что нормативно-методическое направление анализа безопасности программ находится в активном развитии и, благодаря деятельности ТК-362, обсуждаются российские требования к оценке анализаторов кода. Авторы надеются, что данный методический подход и эксперимент будут любопытны всем лицам, увлекающимся разработкой и оценкой безопасных продуктов.

Литература

1. *Марков А. С., Цирлов В. Л., Барабанов А. В. Методы оценки несоответствия средств защиты информации. М.: Радио и связь, 2012. 192 с.*
2. *Арустамян С. С., Варенница В. В., Марков А. С. Методические и реализационные аспекты внедрения процессов разработки безопасного программного обеспечения // Безопасность информационных технологий. 2023. Т. 30. № 2. С. 23–37.*
3. *Static Analysis Technologies Evaluation Criteria v1.0./Ed. by Sherif Koussa; Russian translation by Alec Shcherbakov and Alexey Markov, Web Application Security Consortium, 2013. Режим доступа: http://projects.webappsec.org/w/page/71979863/Static%20Analysis%20Technologies%20Evaluation %20Criteria %20-%20Russian/.*
4. *Марков А. С., Фадин А. А., Швец В. В. Сравнение статических анализаторов безопасности программного кода // Защита информации. Инсайд. 2015. № 6 (66). С. 38–47.*
5. *Markov A., Fadin A., Shvets V., Tsirlov V. The Experience of Comparison of Static Security Code Analyzers // International Journal of Advanced Studies. 2015. V. 5. N 3. С. 55–63.*
6. *Галатенко В. А., Костюхин К. А., Шмырев Н. В., Аристов М. С. Использование свободно распространяемых средств статического анализа исходных текстов программ в процессе разработки приложений для операционных систем реального времени // Программная инженерия. 2012. № 5. С. 2–5.*
7. *Пономарев Н. С., Таланов К. Е. Исследование особенностей анализаторов кода на выявление уязвимостей с использованием метода анализа иерархий Т. Л. Саати. В сборнике: XXXVI Международные Плехановские чтения. Сборник статей участников конференции. В 4-х томах. Москва, 2023. С. 232–238.*

8. Федоров А. Ю., Портнов Е. М., Кокин В. В. Исследование возможностей статических анализаторов кода по поиску ошибок памяти в языках C/C++ // Информатизация и связь. 2017. № 4. С. 45–49.
9. Fatima A. and etc. Comparative study on static code analysis tools for C/C++, In: 2018 15th International Bhurban Conference on Applied Sciences and Technology (IBCAST), Islamabad, Pakistan, 2018, pp. 465–469, DOI: 10.1109/IBCAST.2018.8312265.
10. Kuszczyński K., Walkowski M. Comparative Analysis of Open-Source Tools for Conducting Static Code Analysis // Sensors. 2023. V. 23. № 18. P. 79–78.
11. Shaukat R. and etc. Probing into code analysis tools: A comparison of C# supporting static code analyzers. In: 2018 15th International Bhurban Conference on Applied Sciences and Technology (IBCAST), Islamabad, Pakistan, 2018, pp. 455–464, DOI: 10.1109/IBCAST.2018.8312264.
12. Stefanović D., Nikolić D., Dakić D., Spasojević I., Ristić S. Static Code Analysis Tools: A Systematic Literature Review // In: Annals of DAAAM and Proceedings of the International DAAAM Symposium. 31. 2020. P. 565–573.
13. Бударный Г. С., Пестов И. Е., Штеренберг И. Г. Сравнение методов статического анализа исходного кода программы // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2024. № 1. С. 5–12.
14. Марков А. С. Модели оценки и планирования испытаний программных средств по требованиям безопасности информации. Вестник МГТУ им. Н. Э. Баумана. Сер. «Приборостроение». 2011. Спецвыпуск «Технические средства и системы защиты информации». С. 90–103.
15. Барабанов А. В., Дорофеев А. В., Марков А. С., Цирлов В. Л. Семь безопасных информационных технологий / Под. ред. А. С .Маркова. М.: ДМК Пресс, 2017. 224 с.
16. NIST 500-268. Source Code Security Analysis Tool Function Specification / Black P. E, Kass M., Koo M. Fong E. SSD ITL NIST, 2011. v.1.1. 14 p.
17. Static Analysis Technologies Evaluation Criteria / Ed. by Sherif Koussa – Web Application Security Consortium, 2013. v.1.0. 19 p.

COMPARATIVE ANALYSIS OF STATIC CODE SAFETY ANALYSERS

Markov A. S.[6], Antipov I. S.[7], Arustamyan S. S.[8], Magakelova N. A.[9]

Purpose of work: *development of a methodical approach to comparative analysis of static source code security analysers applicable to the certification of information protection tools by the criteria of performance, applicability, functionality and convenience, as well as its demonstration on examples.*

Research method: *analysis of normative and methodical documents on conducting static analysis and on evaluating static analysers of software source code in order to form a method of their comparison and selection.*

Obtained result: *the results of analysis and synthesis of the system of quality indicators of proprietary code safety analyzers and opensource code analyzers are given, as well as the results of their comparison on real products, which allows to form the necessary tool base for certification tests of software information protection means on information safety requirements and certification of safe software development processes.*

Scientific novelty: *normative documents in the field of static code analysis are analysed in relation to the solution of the task of analysis and selection of several static security analysers, selection criteria are given, test products are chosen and an experiment is carried out which demonstrated different efficiency of code security analysers during certification.*

Authors' contribution: *Markov A. S. – development of methodical approach, editing, Varenitsa V. V. – development of test bench architecture, Antipov I. S., Arustamyan S. S., Magakelova N. S. – conducting the experiment.*

Keywords: *software security, secure software resources, software security analysis, vulnerabilities, undeclared capabilities, backdoors, certification testing toolkit.*

References

1. Markov A. S., Cirlov V. L., Barabanov A. V. Metody ocenki nesootvetstviya sredstv zashchity informacii. M.: Radio i svyaz', 2012. 192 s.
2. Arustamjan S. S., Varenica V. V., Markov A. S. Metodicheskie i realizacionnye aspekty vnedrenija processov razrabotki bezopasnogo programmnogo obespechenija // Bezopasnost' informacionnyh tehnologij. 2023. T. 30. № 2. S. 23–37.
3. Static Analysis Technologies Evaluation Criteria v1.0./Ed. by Sherif Koussa; Russian translation by Alec Shcherbakov and Alexey Markov, Web Application Security Consortium, 2013. – Rezhim dostupa: http://projects.webappsec.org/w/page/71979863/Static%20Analysis%20Technologies%20Evaluation%20Criteria%20-%20Russian/.
4. Markov A. S., Fadin A. A., Shvec V. V. Sravnenie staticheskih analizatorov bezopasnosti programmnogo koda // Zashhita informacii. Insajd. 2015. № 6 (66). S. 38–47.

6 Aleksey S. Markov, Dr.Sc., Head of Department 43, Moscow, Russsia. E-mail: asmarkov@mephi.ru
7 Ilya S. Antipov, Expert of testing laboratory of Echelon, Moscow, Russia. E-mail: mail@cnpo.ru
8 Sas S. Arustamyan, Deputy head of testing laboratory of Echelon, Moscow, Russia. E-mail: s.arustamyan@npo-echelon.ru
9 Nelly A Magakelova, Expert of testing laboratory of Echelon, Moscow, Russia. E-mail: mail@cnpo.ru

5. *Markov A., Fadin A., Shvets V., Tsirlov V. The Experience of Comparison of Static Security Code Analyzers // International Journal of Advanced Studies. 2015. V. 5. N 3. S. 55–63.*
6. *Galatenko V. A., Kostjuhin K. A., Shmyrev N. V., Aristov M. S. Ispol'zovanie svobodno rasprostranjaemyh sredstv staticheskogo analiza ishodnyh tekstov programm v processe razrabotki prilozhenij dlja operacionnyh sistem real'nogo vremeni // Programmnaja inzhenerija. 2012. № 5. S. 2–5.*
7. *Ponomarev N. S., Talanov K. E. Issledovanie osobennostej analizatorov koda na vyjavlenie ujazvimostej s ispol'zovaniem metoda analiza ierarhij T. L. Saati. V sbornike: XXXVI Mezhdunarodnye Plehanovskie chtenija. Sbornik statej uchastnikov konferencii. V 4-h tomah. Moskva, 2023. S. 232–238.*
8. *Fedorov A. Ju., Portnov E. M., Kokin V. V. Issledovanie vozmozhnostej staticheskih analizatorov koda po poisku oshibok pamjati v jazykah S/S++ // Informatizacija i svjaz'. 2017. № 4. S. 45–49.*
9. *Fatima A. and etc. Comparative study on static code analysis tools for C/C++, In: 2018 15th International Bhurban Conference on Applied Sciences and Technology (IBCAST), Islamabad, Pakistan, 2018, pp. 465–469, DOI: 10.1109/IBCAST.2018.8312265.*
10. *Kuszczyński K., Walkowski M. Comparative Analysis of Open-Source Tools for Conducting Static Code Analysis // Sensors. 2023. V. 23. № 18. P. 7978.*
11. *Shaukat R. and etc. Probing into code analysis tools: A comparison of C# supporting static code analyzers. In: 2018 15th International Bhurban Conference on Applied Sciences and Technology (IBCAST), Islamabad, Pakistan, 2018, pp. 455–464, DOI: 10.1109/IBCAST. 2018.8312264.*
12. *Stefanović D., Nikolić D., Dakić D., Spasojević I., Ristić S. Static Code Analysis Tools: A Systematic Literature Review // In: Annals of DAAAM and Proceedings of the International DAAAM Symposium. 31. 2020. P. 565–573.*
13. *Budarnyj G. S., Pestov I. E., Shterenberg I. G. Sravnenie metodov staticheskogo analiza ishodnogo koda programmy // Vestnik Sankt-Peterburgskogo gosudarstvennogo universiteta tehnologii i dizajna. Serija 1: Estestvennye i tehnicheskie nauki. 2024. № 1. S. 5–12.*
14. *Markov A. S. Modeli ocenki i planirovanija ispytanij programmnyh sredstv po trebovanijam bezopasnosti informacii. Vestnik MGTU im.N. Je. Baumana. Ser. «Priborostroenie». 2011. Specvypusk «Tehnicheskie sredstva i sistemy zashhity informacii». S.90–103.*
15. *Barabanov A. V., Dorofeev A. V., Markov A. S., Cirlov V. L. Sem' bezopasnyh informacionnyh tehnologij/Pod. red. A.S .Markova. M.: DMK Press, 2017. 224 s.*
16. *NIST 500-268. Source Code Security Analysis Tool Function Specification / Black P. E, Kass M., Koo M. Fong E. – SSD ITL NIST, 2011. – v.1.1. – 14 p.*
17. *Static Analysis Technologies Evaluation Criteria / Ed. by Sherif Koussa - Web Application Security Consortium, 2013. – v.1.0. – 19 p.*

ЗАЩИТА UNIX-ПОДОБНЫХ СИСТЕМНЫХ ОКРУЖЕНИЙ ОТ ЭКСПЛУАТАЦИИ НЕДОСТАТКОВ БЕЗОПАСНОСТИ ПАМЯТИ

Марченко И. В.[1]

DOI: 10.21681/2311-3456-2024-5-89-94

В настоящее время одним из самых распространенных недостатков программного обеспечения, написанного на языках программирования C и C++, является некорректная работа с памятью. Она может приводить к несанкционированному получению информации, исполнению произвольного кода и другим негативным последствиям.

***Целью данной работы** является повышение защищенности программ от атак, использующих недостатки работы с памятью, посредством создания системного окружения, реализующего аппаратно-программную технологию контроля целостности состояния памяти.*

***Методы.** Проведен сравнительный анализ и выбор аппаратных технологий контроля корректности состояния памяти, а также программных технологий, поддерживающих выбранную аппаратную платформу. Предложена методика создания системных окружений для Режима безопасных вычислений аппаратно-программной платформы «Эльбрус», учитывающая особенности данной технологии. Методика учитывает необходимость компиляции исходного кода программ для поддержки Режима безопасных вычислений, а также возможное наличие несовместимых с ним конструкций.*

***Полученные результаты.** На основе предложенной методики разработано базовое системное окружение, функционирующее в Режиме безопасных вычислений. В рамках разработки системного окружения в пакетах с открытым исходным кодом на языке C были выявлены и исправлены конструкции, соответствующие угрозам безопасности памяти.*

***Практическая значимость.** Предложенная методика может применяться для дальнейшей разработки безопасных системных окружений на основе Режима безопасных вычислений платформы «Эльбрус», использующих программные технологии, отличные от представленных в статье. Разработанное системное окружение позволяет предотвратить эксплуатацию недостатков безопасности памяти в программах, входящих в его состав, без потери их функциональности.*

***Ключевые слова:** аппаратно-программная платформа «Эльбрус», Режим безопасных вычислений, ARM MTE, CHERI, язык C, тегирование памяти.*

Введение

В настоящее время одним из актуальных вопросов безопасности информационных систем является обеспечение безопасности памяти. Согласно отчетам, предоставленным MITRE за 2021–2023 гг.[2,3,4], ведущее место в рейтинге 25 самых опасных недостатков программного обеспечения (CWE – Common Weakness Enumeration) занимает запись за границами буфера (CWE-787 – Out-of-bounds Write). Кроме того, в данные рейтинги входят чтение за границами выделенной памяти (CWE-125 – Out-of-bounds Read), использование указателя после освобождения памяти (CWE-416 – Use After Free), разыменование нулевого указателя (CWE-476 – NULL Pointer Dereference). Данные недостатки программного обеспечения относятся к угрозам безопасности памяти и могут приводить к отказу в обслуживании, получению злоумышленником конфиденциальной информации, исполнению произвольного кода, а также эскалации привилегий[5].

В то же время около 70 % обнаруживаемых ежегодно уязвимостей, которые Microsoft признает общеизвестными уязвимостями (CVE – Common Vulnerabilities and Exposures), связаны с проблемами безопасности памяти. Проблемы безопасности памяти несут значительную угрозу безопасности системы.

В первую очередь это касается программ, написанных на языках программирования, небезопасных при работе с памятью, таких как C и C++ [1].

Изначально распространение языка C связано с развитием Unix-подобных операционных систем. Одним из ключевых принципов операционной системы Unix и в дальнейшем Unix-подобных операционных систем стала переносимость на другие платформы. Вместо ассемблера, как стандартного языка разработки программного обеспечения, в операционной системе Unix впервые начал использоваться язык программирования C для машинно-независимого

1 Марченко Ирина Викторовна, аспирант кафедры компьютерных систем и технологий (№12) НИЯУ МИФИ, Москва, Россия. E-mail: Irina.V.Marchenko@mcst.ru

2 CWE VIEW: Weaknesses in the 2023 CWE Top 25 Most Dangerous Software Weaknesses. URL: https://cwe.mitre.org/data/definitions/1425.html (дата обращения: 14.04.2024).

3 2022 CWE Top 25 Most Dangerous Software Weaknesses. URL: https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html (дата обращения: 14.04.2024).

4 2021 CWE Top 25 Most Dangerous Software Weaknesses. URL: https://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html (дата обращения: 14.04.2024).

5 CWE-787: Out-of-bounds Write. URL: https://cwe.mitre.org/data/definitions/787.html (дата обращения: 22.07.2024).

кода, позволив расширить круг доступных аппаратных платформ [2].

В настоящее время язык С является основным при написании ядер многих Unix-подобных операционных систем и их базового общего программного обеспечения [3]. Таким образом, ключевые компоненты операционных систем являются подверженными угрозам безопасности памяти.

Существует два подхода к решению проблемы безопасности памяти:

1. Использование безопасных при работе с памятью языков программирования, ближайшим по характеристикам к языку С из которых является Rust;
2. Использование технологий аппаратного контроля корректности состояния памяти, наиболее развитыми из которых являются ARM Memory Tagging Extension (ARM MTE), Capability Hardware Enhanced RISC Instructions (CHERI) и Режим безопасных вычислений аппаратно-программной платформы «Эльбрус».

Использование безопасных языков программирования делает невозможным появление угроз безопасности памяти в программах, однако требует полного переписывания исходных кодов используемых программ с языка С на безопасный язык программирования. Данная задача является крайне трудоемкой. В то же время использование аппаратных технологий контроля корректности состояния памяти позволяет предотвращать эксплуатацию уязвимостей программного обеспечения, связанных с угрозами безопасности памяти, для любой программы на небезопасном языке программирования, запущенной для такой платформы[6].

Для использования технологии аппаратного контроля корректности состояния памяти требуется поддержка со стороны программного обеспечения [4]. Для функционирования безопасного системного окружения необходимо обеспечить безопасность работы всех его компонентов — библиотек и исполняемых файлов.

По этой причине необходимо разработать безопасное системное окружение, реализующее аппаратно-программный комплекс защиты от угроз безопасности памяти, при помощи технологии аппаратного контроля корректности состояния памяти.

1. Аппаратная платформа

Безопасное системное окружение реализует аппаратно-программный комплекс контроля корректного состояния памяти. Для создания безопасного системного окружения требуется определить аппаратную и программную платформы.

На данный момент существует три основных аппаратных технологии контроля безопасности памяти, реализованных в процессорах существующих архитектур: ARM MTE (архитектура ARM [5]), CHERI (архитектура ARM, существуют разработки для архитектур MIPS, RISC-V [6]) и Режим безопасных вычислений «Эльбрус» (архитектура E2K [7]).

Технология ARM MTE осуществляет вероятностный контроль над соответствием указателя выделенной памяти по принципу «ключ-замок»: теги указателя («ключа») и области памяти («замка») должны совпасть при обращении. Размер тега составляет 4 бита, следовательно, количество возможных вариантов тегов равно 16. При однократном запуске вероятность обнаружения ошибки составляет 93% [8].

Технология CHERI не является вероятностной и осуществляет контроль над соответствием указателя и выделенной памяти при помощи дескрипторов (ориг. Capability), представляющих собой указатели с метаданными. Дескрипторы позволяют обратиться по указателю к заданному объекту с учетом верхней и нижней границы выделенной для него области памяти, что позволяет предотвратить выходы за границы объекта [9].

Режим безопасных вычислений не является вероятностной технологией и использует дескрипторы вместо указателей, позволяющие контролировать границы объекта, к которому происходит обращение. Также в Режиме безопасных вычислений предусмотрена технология внешних тегов, не входящих непосредственно в состав дескриптора и позволяющих контролировать тип содержимого каждого 32-битного слова, находящегося в оперативной памяти [10].

Возможности обнаружения типов недостатков программного обеспечения при помощи рассмотренных технологий [11] представлены в табл. 1.

Для дальнейшей работы выбран Режим безопасных вычислений платформы Эльбрус, как реализующий гарантированную невероятностную защиту от эксплуатации большего числа типов недостатков программного обеспечения.

2. Программная платформа

Для выбора программной платформы следует учитывать наличие компонентов, реализующих поддержку Режима безопасных вычислений со стороны операционной системы, компилятора и его компонентов [12].

В качестве первичного критерия отбора операционной системы выступает поддержка архитектуры E2K. Поддержка операционной системой выбранной архитектуры, предоставляющей технологию контроля корректности состояния памяти, необходима для функционирования безопасного системного окружения.

Еще одним немаловажным критерием при выборе операционной системы является наличие доступа

6 Back To The Building Blocks: A Path Toward Secure And Measurable Software // The White House. Washington. 2024. URL: https://www.whitehouse.gov/wp-content/uploads/2024/02/Final-ONCDTechnical-Report.pdf (дата обращения: 21.07.2024).

Таблица 1.

Возможность обнаружения типов уязвимостей технологиями тегирования памяти

Наименование технологии	Обнаруживаемые недостатки				
	CWE-787	CWE-125	CWE-587	CWE-416	CWE-457
ARM MTE	+	+	+	+	-
CHERI	+	+	+	-	-
Режим безопасных вычислений	+	+	+	+	+

Таблица 2.

Дистрибутивы, поддерживающие архитектуру E2K

Дистрибутив	Поддержка E2K	Доступ к исходному коду	Доступ к системе сборки ОС
ОС Эльбрус	+	+	+
ALT Linux	+	+	-
Astra Linux	+	-	-

к исходному коду пакетов, входящих в состав операционной системы, так как исполнение программы в Режиме безопасных вычислений требует перекомпиляции ее исходного кода.

В качестве возможной операционной системы рассматривались дистрибутивы GNU/Linux, поддерживающие архитектуру E2K: ОС Эльбрус[7], ALT Linux[8] и Astra Linux[9]. Сравнительная таблица данных операционных систем представлена в табл. 2.

Операционной системой для создания безопасного системного окружения выбрана ОС Эльбрус производства АО «МЦСТ».

В качестве разрабатываемого системного окружения выбран LXC-контейнер. Этот вид окружения обеспечивает работу программ в изолированном пространстве процессов, ускоряя отладку контейнера при помощи основной операционной системы и общего ядра Linux.

3. Методика создания безопасного системного окружения

Разработана методика создания безопасного системного окружения. Ее общий алгоритм включает в себя четыре основных этапа:

1. Определение базового списка пакетов;
2. Сборка пакетов;
3. Разработка правил создания и настройки системного окружения;
4. Функциональное тестирование программ.

На этапе определения базового списка пакетов безопасного системного окружения необходимо учитывать наличие пакетов поддержки режима безопасных вычислений, в особенности библиотеки языка C с поддержкой Режима безопасных вычислений. На этапе сборки пакетов из составленного списка возможно обнаружение конструкций, несовместимых с Режимом безопасных вычислений при помощи ошибок и предупреждений компилятора. Разработка правил создания и настройки осуществляется индивидуально для каждого набора выбранных

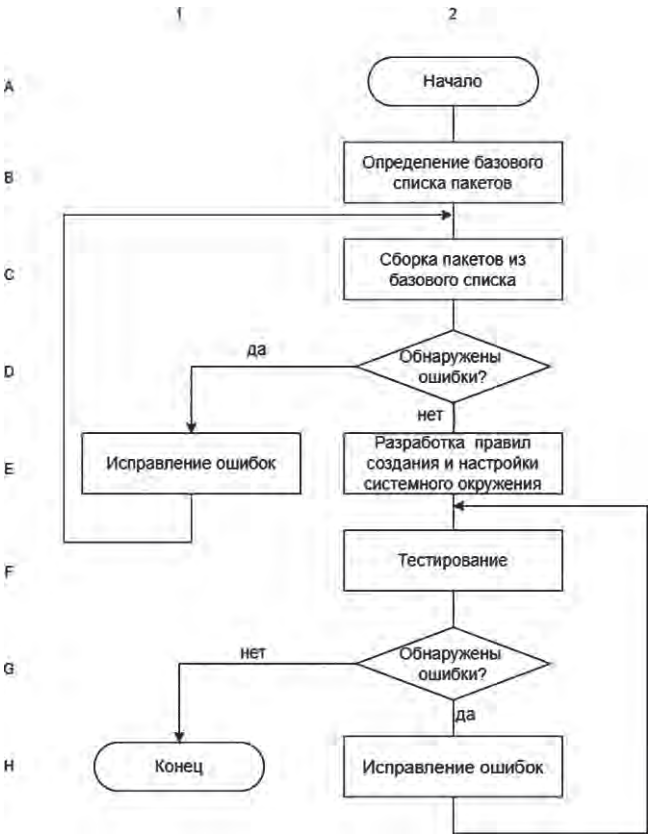


Рис. 1. Блок-схема алгоритма создания безопасного системного окружения

7 Операционные системы «Эльбрус». URL: http://www.mcst.ru/elbrus_os (дата обращения: 27.07.2024).

8 Дистрибутивы ОС Альт для Эльбрус. URL: https://www.altlinux.org/Эльбрус/дистрибутивы (дата обращения: 27.07.2024).

9 Совместимость Astra Linux с процессорами Эльбрус. URL: https://wiki.astralinux.ru/kb/sovmestimost-astra-linux-s-protsessorami-el-brus-187795264.html (дата обращения: 27.07.2024).

программных технологий с учетом их особенностей. Тестирование проводится в первую очередь с целью выявления в утилитах и библиотеках, входящих в состав безопасного системного окружения, конструкций, несовместимых с Режимом безопасных вычислений. Блок-схема алгоритма создания безопасного системного окружения представлена на рис. 1.

Предложенная методика универсальна и не зависит от выбранной технологии создания системного окружения.

4. Реализация

В базовый список пакетов безопасного системного окружения вошли пакеты минимальной базовой системы ОС Эльбрус, а также их сборочные зависимости – 70 пакетов.

Произведена компиляция пакетов из базового списка в режиме безопасных вычислений. Разработаны правила создания и настройки безопасного системного окружения. Проведено функциональное тестирование – программы в Режиме безопасных вычислений при возникновении конструкции с ошибкой завершают свою работу с выдачей диагностики.

Из 70 пакетов, вошедших в состав базового системного окружения, в рамках тестирования интерес представляют пакеты с открытым исходным кодом, написанные на языке С, к таким относятся 53. Распределение пакетов из состава безопасного системного окружения по принадлежности к проприетарному программному обеспечению, пакетам с отрытым исходным кодом на языке С и не на языке С представлено в табл. 3.

Таблица 3.

Разделение пакетов базового списка по категориям

<table>
<tr><th colspan="3"></th><th>Количество пакетов, шт.</th></tr>
<tr><td rowspan="3">Базовый список</td><td colspan="2">Проприетарное ПО</td><td>4</td></tr>
<tr><td rowspan="2">Открытый исходный код</td><td>Исходный код не на языке С</td><td>13</td></tr>
<tr><td>Исходный код на языке С</td><td>53</td></tr>
<tr><td colspan="3">Итого</td><td>70</td></tr>
</table>

По итогам тестирования 28 из 53 исследуемых пакетов содержали конструкции, несовместимые с Режимом безопасных вычислений, что составляет 53%. Некорректные конструкции разделены на 5 категорий, наиболее часто встречающейся из которых стало использование неинициализированных данных. В данные категории включают ранее рассмотренные классы недостатков программного обеспечения, кроме использования указателей после освобождения памяти, примеров такой уязвимости в рассматриваемых пакетах обнаружено не было. Обнаруженные в ходе тестирования некорректные конструкции исправлены. Распределение конструкций представлено в табл. 4.

Таблица 4.

Классы конструкций, несовместимых с режимом безопасных вычислений в пакетах базового списка

Класс конструкции	Количество конструкций, шт.	Процент от общего числа конструкций, %
Использование неинициализированных данных	70	51.9
Запись за границами выделенной памяти	2	1.5
Чтение за границами выделенной памяти	5	3.7
Преобразование переменной целочисленного типа в указатель	38	28.1
Использование фиксированных выравниваний	20	14.8

Реализованное безопасное системное окружение по функциональности полностью соответствует системному окружению в обычном режиме. Таким образом, пользователь безопасного системного окружения получает преимущества использования технологии контроля корректного состояния памяти в виде защиты от эксплуатации ряда недостатков программного обеспечения, в том числе и от еще не выявленных уязвимостей, при этом не будучи ограниченным в своих действиях.

Заключение

Технологии аппаратного контроля корректности состояния памяти предоставляют защиту от эксплуатации угроз безопасности памяти, однако не предназначены для функционирования обособленно, без программной поддержки. В рамках данной работы проведено сравнительное исследование аппаратных технологий и для наиболее оптимальной из них, Режима безопасных вычислений, предложены программные технологии реализации безопасного системного окружения.

Разработана методика создания безопасного системного окружения, учитывающая особенности выбранных технологий. В соответствии с методикой реализовано безопасное системное окружение.

В рамках разработки и отладки безопасного системного окружения в 53 % пакетов с открытым исходным кодом на языке C обнаружены конструкции, несовместимые с Режимом безопасных вычислений, а также найдены 77 потенциально опасных конструкций при работе с памятью. Это подтверждает эффективность использования безопасного системного окружения: оно реализует возможность выявления недостатков программного обеспечения, соответствующих проблемам безопасности памяти. Обнаруженные недостатки исправлены. Безопасное системное окружение предоставляет функциональность, аналогичную функциональности в обычном режиме, в рамках пакетов, входящих в его состав.

Литература

1. *Gavin, T. A proactive approach to more secure code. URL: https://msrc.microsoft.com/blog/2019/07/a-proactive-approach-to-more-secure-code/ (дата обращения: 22.07.2024).*
2. *Цейтин Г. С. UNIX и постановка вопроса о переносимости программного обеспечения // SORUCOM-2011. – 2011. – С. 320–322. URL: https://sorucom.iis.nsk.su/files/page/sorucom-2011_0.pdf (дата обращения: 27.07.2024).*
3. *Tanenbaum A. Modern Operating Systems. Fourth Edition. // Vrije Universiteit, 2014. – 1106 с.*
4. *Jero S. TAG: Tagged Architecture Guide / S. Jero, N. Burow, B. Ward, R. Skowyra // ACM Computing Surveys. 2022. – Vol. 55. – № 6. – Article 124. DOI: https://doi.org/10.1145/3533704.*
5. *Serebryany K. ARM Memory Tagging Extension and How It Improves C/C++ Memory Safety // ;login:. – Summer 2019. – Vol. 44. – № 2. URL: https://www.usenix.org/system/files/login/articles/ login_summer19_03_serebryany.pdf (дата обращения: 26.07.2024).*
6. *Watson R. An Introduction to CHERI. // University of Cambridge, 2019. https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-941.pdf (дата обращения: 28.07.2024).*
7. *Нейман-заде М. И., Королёв С. Д. Руководство по эффективному программированию на платформе «Эльбрус». АО «МЦСТ». 2024. URL: http://mcst.ru/doc/elbrus_prog/elbrus-prog-1.2_2024-02-28.pdf (дата обращения: 26.07.2024).*
8. *Partap A. Memory Tagging: A Memory Efficient Design / A. Partap, D. Boneh // arXiv. Cryptography and Security. – 2022. DOI: https://doi.org/10.48550/arXiv.2209.00307.*
9. *Watson R. Capability Hardware Enhanced RISC Instructions: CHERI Instruction-Set Architecture (Version 9). // University of Cambridge, 2023. URL: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-987.pdf (дата обращения: 28.07.2024).*
10. *Мустафин Т. Р. Безопасная среда исполнения критических приложений во встраиваемых системах на базе вычислительных средств семейства «Эльбрус» / Т.Р. Мустафин, А.И. Алехин, Е.М. Кравцунов, Б.О. Макаев // Радиопромышленность. – 2019. – № 1 – С. 16–22. – EDN YXUUPJ.*
11. *Артемьев И. А. Сравнительный анализ технологий безопасного использования памяти с учетом аппаратно-программных особенностей вычислительных комплексов / И. А. Артемьев, И. В. Марченко, Д. В. Ярапов, Н. А. Шаменков // Цифровые технологии и решения в сфере транспорта и образования. 2023. С. 11–20. – EDN BVFFDD.*
12. *Волконский В. Ю. Безопасная реализация языков программирования на базе аппаратной и системной поддержки // Вопросы радиоэлектроники. – 2008. – Т. 4. – № 2. – С. 98–141. – EDN JTNBAR.*

PROTECTING UNIX-LIKE SYSTEM ENVIRONMENTS FROM EXPLOITATION OF MEMORY SECURITY WEAKNESSES

Marchenko I. V.[10]

Nowadays one of the most common weaknesses of software written in the C and C++ programming languages is incorrect memory handling. It can lead to unauthorized access to information, executing arbitrary code, and other negative consequences.

***The purpose of this work** is increasing the protection of programs from attacks using memory safety weaknesses by implementing a protected system environment using hardware memory integrity monitoring technology.*

***Methods.** A comparative analysis and selection of hardware and software memory integrity monitoring technology, as well as software technologies supporting the selected hardware platform, are performed. A methodology for creating system environments for Secure computing mode is proposed, taking into account the features of this technology. The methodology takes into account the need to compile the source code of the program to support Secure computing mode compilation option, as well as the possible existence of incompatible constructions.*

***Results.** Based on the proposed methodology, a basic Secure computing mode protected system environment has been developed. During the development of the system environment in C language open source packages, constructions corresponding to memory security threats were identified and corrected.*

***Practical significance.** The proposed methodology can be used for further development of protected system environments based on the Secure computing mode while using software technologies other than those presented in the article.*

10 Irina V. Marchenko, Postgraduate Student, Department of Computer Systems and Technologies (No12), National Research Nuclear University MEPhI, Moscow, Russia. E-mail: Irina.V.Marchenko@mcst.ru

The developed system environment allows preventing the exploitation of memory safety weaknesses in the software included in it, without reducing functionality for the user.

Keywords: *Elbrus hardware and software platform, Secure computing mode, ARM MTE, CHERI, C language, memory tagging.*

References

1. *Gavin, T. A proactive approach to more secure code. URL: https://msrc.microsoft.com/blog/2019/07/a-proactive-approach-to-more-secure-code/ (accessed: 22.07.2024).*
2. *Tseytin G. S. UNIX and the Statement of Software Portability Problem // SORUCOM-2011. – 2011. – P. 320–322. (in Russian). URL: https://sorucom.iis.nsk.su/files/page/sorucom-2011_0.pdf (accessed: 27.07.2024).*
3. *Tanenbaum A. Modern Operating Systems. Fourth Edition. // Vrije Universiteit, 2014. – 1106 p.*
4. *Jero S. TAG: Tagged Architecture Guide / S. Jero, N. Burow, B. Ward, R. Skowyra // ACM Computing Surveys. 2022. – Vol. 55. – № 6. – Article 124. DOI: https://doi.org/10.1145/3533704.*
5. *Serebryany K. ARM Memory Tagging Extension and How It Improves C/C++ Memory Safety // ;login:. – Summer 2019. – Vol. 44. – № 2. URL: https://www.usenix.org/system/files/login/articles/ login_summer19_03_serebryany.pdf (accessed: 26.07.2024).*
6. *Watson R. An Introduction to CHERI. // University of Cambridge, 2019. https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-941.pdf (accessed: 28.07.2024).*
7. *Neiman-Zade M. I., Korolev S. D. Guide to Effective Programming on the Elbrus Platform. MCST. 2024. (in Russian). URL: http://www.mcst.ru/doc/elbrus_prog/elbrus-prog-1.2_2024-02-28.pdf (accessed: 26.07.2024).*
8. *Partap A. Memory Tagging: A Memory Efficient Design / A. Partap, D. Boneh // arXiv. Cryptography and Security. – 2022. DOI: https://doi.org/10.48550/arXiv.2209.00307.*
9. *Watson R. Capability Hardware Enhanced RISC Instructions: CHERI Instruction-Set Architecture (Version 9). // University of Cambridge, 2023. URL: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-987.pdf (accessed: 28.07.2024).*
10. *Mustafin T. R. Secure execution environment for critical applications in embedded systems based on Elbrus family computing facilities / T. R. Mustafin, A. I. Alekhin, E. M. Kravtsunov, B. O. Makaev // Radio Inustry. – 2019. – № 1 – P. 16–22. (in Russian). – EDN YXUUPJ.*
11. *Artemiev I. A. Comparative analysis of technologies for the safe use of memory, taking into account the hardware and software features of computing complexes / I. A. Artemiev, I. V. Marchenko, D. V. Yarapov, N. A. Shamenkov // Digital technologies and solutions in the field of transport and education. 2023. P. 11–20. (in Russian). – EDN BVFFDD.*
12. *Volkonskii V. Y. Secure implementation of programming languages based on hardware and system support // Issues of radio electronics. – 2008. – T. 4. – № 2. – P. 98–141. (in Russian). – EDN JTNBAR.*

КИБЕРПАРАДИГМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

Горбатов В. С.[1], Эрдниев А. С.[2]

DOI: 10.21681/2311-3456-2024-5-95-104

Цель исследования: *изучить возможность и необходимость использования терминологического описания безопасности информационных технологий и систем.*

Методы исследования: *диалектический и полипарадигмальный подходы, системный анализ, синтез решений.*

Полученные результаты: *могут быть полезны специалистам по защите информации при создании и совершенствовании внутренней (локальной) нормативной базы, а также при создании учебно-методических материалов в сфере образовательных услуг в области информационной безопасности. Полученные результаты также можно рекомендовать потенциальным авторам научных публикаций в аспекте диалектического изложения своих научных достижений.*

Научная новизна: *уделено внимание обсуждению кибернетической сущности рассматриваемого феномена, имеющей с прагматической точки зрения относительно общий характер и определяющей более общее толкование различных понятий с приставкой кибер-..., в частности, взаимосвязь терминов информационная безопасность и кибербезопасность.*

Практическая ценность: *с практической точки зрения данное исследование рассматривается, как решение частной задачи в рамках общей проблемы совершенствования подготовки кадров для органов внутренних дел.*

Ключевые слова: *законы диалектики, информационная безопасность, кибернетика, кибербезопасность, критическая информационная инфраструктура, метапредметность, парадигма, понятийный аппарат, терминология.*

Введение

Всеобщая цифровизация жизнедеятельности российского общества не обходит стороной и органы внутренних дел (ОВД) как особой разновидности государственной службы. Преобразования в области ИТ-технологий последних лет позволили автоматизировать многие процессы оказания государственных услуг, обеспечить оцифровку реестров значимой информации, в том числе касающихся персональных данных граждан Российской Федерации. Происходит активное внедрение телекоммуникационных систем для обеспечения охраны общественного порядка и безопасности граждан.

Вместе с тем, очевидно, что активная цифровизация государственного управления требует наличия у представителей органов госвласти дополнительного набора профессиональных компетенций, что, в свою очередь, актуализирует проблему совершенствования процесса подготовки кадров, в том числе в интересах системы ОВД.

С целью определения возможных подходов разрешения этой проблемы было поставлено исследование этого актуального аспекта системы ведомственного образования[3], в частности, в рамках задачи, поставленной в [1].

Актуальность указанного исследования также поддерживается перспективой реформирования в ближайшие годы общей системы высшего образования, в том числе утверждения новых образовательных стандартов. В рамках проводимой реформы перед профессиональным научно-образовательным сообществом поставлена задача более основательного подхода к разработке новых квалификационных требований и компетенций на основе современных тенденций развития цифровых технологий.

Несмотря на уже существующую детальную формализацию образовательного процесса в интересах системы ОВД, в ней существует ряд позиций, изменение которых, на наш взгляд, позволит повысить уровень подготовки необходимых специалистов по вопросам безопасности используемых цифровых технологий. Например, изменение структуры и содержания требований к специальной профессиональной подготовке сотрудников ОВД с учетом современных тенденций позволит расширить рамки применяемых образовательных программ, а их содержательное наполнение под задачи профессиональной деятельности обеспечит впоследствии детальную проработку вариативной части соответствующего учебно-методического обеспечения.

1 Горбатов Виктор Сергеевич, кандидат технических наук, доцент, Национальный исследовательский ядерный университет «МИФИ», г. Москва, Россия, e-mail: VSGorbatov@mephi.ru, https://orcid.org/0000-0001-9998-9733

2 Эрдниев Александр Сергеевич, кандидат педагогических наук, Московский университет МВД России имени В. Я. Кикотя, г. Москва, Россия, e-mail: konfuci@inbox.ru, https://orcid.org/0009-0007-5363-8365

3 Научно-исследовательская работа проводится в рамках выполнения договора о взаимном сотрудничестве между НИЯУ МИФИ и Московским университетом МВД России имени В. Я. Кикотя от 12 июля 2023 г. № 394.

Выше уже упоминалась возможность решения одной из частных задач такого исследования применительно к вопросам обеспечения безопасности информационной инфраструктуры ОВД [1]. В настоящей работе в качестве логического продолжения рассмотрена еще одна частная задача, связанная с уточнением и конкретизацией используемого в будущем терминологического аппарата для дальнейшего общего анализа вопросов совершенствования подготовки кадров в исследуемой области в интересах ОВД.

Актуальность поставленной задачи определяется тем, что такое многомерное явление как информационная безопасность (ИБ) находит свое отражение применительно к различным областям научного познания и, следовательно, современный феномен цифровой информации с прагматической точки зрения требует внимания к вопросам унификации соответствующего понятийного аппарата научной и/или образовательной деятельности, в том числе в области обеспечения безопасности информационных систем. При этом, как правило, предполагается возможность решения указанной проблемы по однозначному пониманию и описанию сложно формализуемых задач данной области с последующей единообразной их технологической реализации в различных приложениях. Прагматичная мотивация подобного подхода сводится к очевидной необходимости создания общепринятой понятийной основы для повышения эффективности коммуникативного взаимодействия специалистов различного профиля в условиях «взрывного» характера развития информационных технологий. Не умаляя научной и практической значимости такой методологии, отметим, однако, что в соответствии с законами диалектики указанный подход имеет и серьезные ограничения в аспекте его применения к анализу фундаментальных проблем образовательной деятельности. Попытки «жесткой» унификации (стандартизации) определений (дефиниций) основных понятий сложной предметной области, в частности, обеспечения информационной безопасности, только на основе «хороших практик», без учета диалектики развития содержания и сущности таких понятий, может привести к их «омертвлению» в аспекте совершенствования образовательных программ, что является характерным следствием метафизической методологии познания.

В настоящей работе показаны возможность и необходимость использования для терминологического описания такой предметной области исследования, как безопасность информационных технологий и систем, полипарадигмального подхода, учитывающего диалектику развития языковых и речевых явлений, терминов и понятий [2].

При этом обеспечивается «взрывной» характер развития указанных технологий даже при наличии относительной неопределенности терминологического базиса.

Трудно не согласиться с авторами указанной выше работы [2, с. 1], которые утверждают, что «... сущность языкового явления раскрывается только путем обнаружения его связей и отношений с другими явлениями на основе выделения единичного, особенного и всеобщего». При этом важнейшим условием является применение основных законов диалектики. Далее утверждается, что «...современная функциональная лингвистика провозглашает новый подход к изучению языковых явлений: не от формы к значению и функции...», а в точности до наоборот. Постулирование необходимости полипарадигмального подхода к изучению языковых и речевых явлений позволяет изучать их со всех сторон: системно-структурной, функциональной, коммуникативной и прагматической.

Как показано ниже такая лингвистическая методология хорошо подтверждается контент-анализом различных исследований искомого понятия ИБ, которое рассматривается в качестве объекта или предмета научного познания не только в естественных и технических отраслях наук [1, 3, 7 и др.]., но и гуманитарного профиля: философии, правоведения, социологии, политологии, педагогики и т.д. [4, 5, 6 и др.].

И, естественно, с точки зрения методологического преломления понятие ИБ приобретает неоднозначные сущностные парадигмы. Так в базовом законе[4] правовое содержание ИБ раскрывается через понятия «защита информации» (ст. 16), «ограничение доступа к информации и распространения сведений, имеющих свойство конфиденциальности» (ст. 5 ч. 3; ст. 6). В ГОСТ[5] приводится наиболее распространенное в сфере оказания дополнительных образовательных услуг определение ИБ (п. 3.28) как безопасность информации, определяемое по трем основным критериям: доступности (ст. 3.7), целостности (п. 3.36) и конфиденциальности (п. 3.10). И далее дополняется критериями подлинности (п.3.6), неотказуемости (п. 3.48) и достоверности (п. 3.55).

В кредитно-финансовой сфере принята своя формулировка парадигмы ИБ[6], целью которой является необходимость обеспечения непрерывности бизнеса.

4 Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

5 Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27000-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология» (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 19 мая 2021 г. N 392-ст).

6 Стандарт ЦБР СТО БР ИББС-1.0-2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (принят и введен в действие распоряжением ЦБР от 21 июня 2010 г. № Р-705).

Таким образом, без необходимого уточнения понятия ИБ применительно к сфере профессиональной деятельности ОВД дальнейший анализ образовательных аспектов в интересах данной структуры государственной службы будет содержать существенные недостатки системного характера.

Одной из существенных новаций терминологического характера последних лет в исследуемой области, связанной с научно-образовательной деятельностью, является нормативная легализация применения понятия «кибербезопасность» [3]. Введена новая научная специальность – кибербезопасность – наряду с традиционной – информационная безопасность, методы и средства защиты информации, в Российской академии наук создано новое подразделение.

Эта легализация сопровождается активной разработкой различных проектов соответствующих организационно-распорядительных и методических документов в сфере высшего образования[7]. В Российской академии наук создана организационная структура государственного характера с данным наименованием.

Поэтому в соответствии с обсужденной выше методологией научного познания необходим анализ введения и такой новации применительно к сфере деятельности ОВД и на этой основе выявление характерных ее особенностей для соответствующей подготовки необходимых специалистов.

Таким образом, задается цель данной работы – определение терминологической сущности и содержания основных понятий: ИБ и кибербезопасности, применительно к системе ОВД. Результаты решения этой задачи будут использованы для дальнейшей проработки предложений по совершенствованию учебно-методической базы подготовки кадров в интересах ОВД, хотя в методологическом плане могут быть полезны специалистам и других сфер общественной деятельности.

1. Метапредметное свойство ИБ

На нынешнем этапе подготовка специалистов в исследуемой области в интересах ОВД осуществляется в рамках обучения по укрупненной группе специальностей и направлений подготовки (УГСНП) – информационная безопасность – в соответствии с нормативными требованиями, заданными федеральными образовательными стандартами высшего образования (ФГОС ВО), в частности по специальности 10.05.05[8] с ведомственными процедурными уточнениями[9]. Терминологическую основу данных ФГОС составляет уже устоявшаяся, хотя и не без дискуссионных моментов, обширная понятийная база естественных и технических наук. В то же время практически отсутствуют компетенции, связанные с гуманитарными аспектами ИБ. Поэтому в рамках задачи, поставленной в настоящей работе целесообразно провести анализ различных полипарадигмальных подходов, исходя из понятийной базы наук гуманитарного профиля, как необходимого этапа достижения сформулированной выше цели исследования метапредметного свойства (сущности) феномена ИБ.

1.1. Философский подход

Осмысление проблемы на уровне философской методологии предполагает применение диалектического подхода [4], по которому термин ИБ тесно связано с понятиями «информационная свобода» и «информационное насилие». В этом случае феномен ИБ может определяться с одной стороны метафизическим состоянием свободы, как противоположностью детерминированности, с другой в социально-политическом смысле, как отсутствием ограничений. Генезис безопасности в информационной пространстве связывается не только с наиболее традиционным представлением как защита информации ограниченного доступа, но и с «защитой от нежелательной информации». Отсюда следует что, любое вмешательство третьих лиц в добровольное и свободное информационное взаимодействие, приводящее к нарушению данного фактора, является «информационным насилием». В этом случае допустимо применить так называемый либертарианский подход к осмыслению феномена ИБ, по которому свобода рассматривается с точки зрения отсутствия инициированного насилия. Таким образом, ИБ можно рассматривать в качестве некоторого состояния защищенности информационного пространства от нежелательных воздействий. Эта конструкция используется в первой и второй версиях Доктрины информационной безопасности Российской Федерации[10].

В то же время развитие толкования понятия ИБ тесно связывается с четвертой промышленной революцией и одной из рамочных характеристик выступает понятия «информационная цивилизация» в контексте информационной реальности [5]. Рассмотрение информационной реальности на основе метафизического и диалектического подходов предполагает выделение ряда свойств ИБ:

7 Портал федеральных государственных образовательных стандартов высшего образования // URL: https://fgosvo.ru/ (дата обращения: 24.05.2024).

8 Приказ Минобрнауки РФ от 26.11.2020 № 1461 «Об утверждении федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере» (Зарегистрировано в Минюсте РФ 22.12.2020 № 61703).

9 Приказ МВД России от 2 февраля 2024 г. № 44 «Об утверждении Порядка организации подготовки кадров для замещения должностей в органах внутренних дел Российской Федерации» (Зарегистрировано в Минюсте РФ 12.03.2024 № 77488).

10 Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

- развитие потенциала социальной коммуникации за счет внедрения информационных технологий;
- угроза информационной защищенности благодаря выделению таких институтов, как информационная война, информационный терроризм, нейролингвистическое программирование, отчуждение личности в виртуальной компьютерной реальности (метавселенная);
- отрицательная энтропия, основанная на системности, организованности, упорядоченности информации, отсюда информационная реальность выступает в качестве силы, противодействующей хаосу и дезорганизации.

С позиции метафизического подхода ИБ выступает в качестве произвольно конструируемой системы, в основе которой лежит технологический прогресс. В этом случае ИБ обладает определенными динамическими свойствами, своего рода энергетическим потенциалом, для которых выступают потребности информационного общества. Диалектический подход к толкованию ИБ возлагает на это понятие свойство противодействия деструктивным информационным проявлениям.

Динамика социально-политических явлений как внутреннего, так и международного характера последних нескольких лет предполагает рассмотрение понятия ИБ через призму прокси-войн и военной безопасности российской цивилизации [6]. Именно через призму такого противоборства в так называемом киберпространстве как части сферы военного противостояния и часто рассматривается легализируемый ныне термин кибербезопасность [7].

Применение междисциплинарной методологии и системного подхода к осмыслению ИБ как составляющей военной безопасности Российской Федерации также определяет актуальность ее учета во всех сферах общественных отношений. Причем деструктивному воздействию подвергаются как социальные общности, так и отдельные индивиды. С точки зрения состояния защищенности ИБ не разделяет обеспеченность защитой отдельного индивида или социума в целом, а лишь расширяет или сужает объекты информационного воздействия. ИБ выступает в качестве «состояния репрезентативной практики социума, регистрирующей ее качественную способность реагировать на предотвращение различного вида опасностей материальным и духовным ценностям».

Таким образом, философское осмысление понятия ИБ позволяет определить этот феномен и как статичное состояние материального и духовного объекта, так и представить в качестве динамического процесса, направленного на обеспечение интересов общества и индивида, в том числе в рамках охраны общественного порядка.

1.2. Социологический подход

Социологический подход к определению понятия информационной безопасности предполагает выделение трех ключевых элементов в структуре информационной безопасности [8]. Среди них:

1) Информационно-правовое или нормативное правовое регулирование, обеспечивающее защиту интересов различных субъектов в сфере информационной безопасности.
2) Информационно-техническое или обеспечение защищенности информации путем технических и программных средств защиты.
3) Информационно-психологического защита личности от деструктивного информационного контента.

При этом ключевой проблемой [8, с. 12] в вопросе трактовки понятия ИБ автор видит в «смешении подходов естественнонаучных и гуманитарных дисциплин». При этом отмечено, что гуманитарный подход обладает избыточной абстракцией в конкретизации терминологии. Такой социологический подход позволяет позиционировать ИБ в качестве составляющей социологии безопасности. Указанные условия определяют ИБ, как «сложное системное, многоуровневое явление современного социума, представляющее собой стабильное, равновесное существование информационно-коммуникационной подсистемы общества, выражающееся в отсутствии дезорганизационно-дисфункциональных индикаторов (маркеров) в ее функционировании».

Проще говоря, ИБ есть отрицание (и преодоление) информационной опасности, проявляющейся в любых масштабах. Опасности и угрозы ИБ определяют содержание деятельности по ее обеспечению. «Обеспечение ИБ представляет собой защиту от опасностей и угроз инфосферы общества, а также предполагает позитивное развитие информационной реальности, порождающее отсутствие негативных эффектов от процесса информатизации».

1.3. Политологический аспект ИБ

Глубина политологических исследований направлена на анализ технологий, средств и методов обеспечения ИБ. Современная геополитическая ситуация определяет интерес к исследованию феномена ИБ в контексте политических процессов и «мягкой» методологии их организации [9]. Политологическая ориентация определения понятия ИБ предлагает следующую трактовку: «состояние защищенности всех сфер общественной жизни, общественного сознания от негативного воздействия информацией, обеспечиваемое государством и гражданским обществом и являющееся ключевым условием модернизации и демократизации общества и государства и их готовности к защите национальных интересов страны на международной арене». Подобная трактовка

позволяет определить нетрадиционную форму понятия ИБ, как «состояние защищенности от информации», в качестве альтернативно предложенного ранее определению «защищенности информации и информационного пространства».

То есть ИБ, как социально-политический феномен, связывается с развитием гражданского общества, в этом случае объективно безрамочное информационное пространство ограничивается интересами отдельной социальной общности. Информация переходит из категории идеального в материальный объект, обеспечивающий артикулированность интересов отдельного индивида и социальных структур. В этом случае концепция информационной безопасности выделяет в качестве объекта охраны национальную идентичность. Векторами обеспечения национальной ИБ выступают: идеологическая целостность национального информационного пространства и защита от внешних деструктивных информационных акторов.

Ключевым акцентом политологического рассмотрения понятия ИБ является отношение к таким понятиям как целостность и доступность информации. Целостность обеспечивается свободой распространения взглядов любыми социальными субъектами, равенство доступа к информации. Доступность наделяет информационное пространство такой характеристикой, как защита от сокрытия информации от потребителя.

1.4. Право и ИБ

Связь ИБ с гражданским обществом определяет потребность изучения контекста данного понятия через призму юридических наук. Связь ИБ с правами человека обуславливает анализ теоретико-правовой значимости этого понятия [10]. В данном контексте справедливо применение аксиологического подхода в осмыслении понятия ИБ в связи с теорией государства и права. Определение ИБ в качестве правовой категории выделяет такие понятия, как информационный патернализм, цифровая идентичность и свобода информации в рамках национального права.

Формальный антагонизм между информационной свободой и информационной безопасностью преодолевается путем определения взаимозависимостей между двумя категориями как правовыми ценностями нового времени. Отсюда следует, что правовая природа ИБ определяется, как «состояние защищенности прав человека в информационной сфере». Обеспечение ИБ личности реализуется путем дополнения правовых средств защиты техническими нормами. При этом важнейшим композитом достижения баланса интересов личности и государства выступает принцип правовой соразмерности.

Систематизация нормативно-правовых оснований, определяющих сущность ИБ в национальном законодательстве, выделяет потребность в унификации терминологического аппарата [11, с. 165]. В качестве обоснования представлены дефиниции отдельных смысловых конструкций, не имеющих однозначной трактовки, например «информационные ресурсы» (ИР). Универсальная с точки зрения права и науки трактовка понятия ИР позволит преодолевать нарушения правовой логики при формализации общественных отношений.

2. Формализация метапредметности ИБ

Проведенный краткий и даже в некотором роде поверхностный анализ толкований понятия ИБ с позиций гуманитарных наук дает обоснование закрепить его метапредметное свойство как особенную характеристику, определяющую его полипарадигмальную (многоаспектную) сущность и не позволяющую в полной мере осуществить возможный таксонометрический подход.

На рис. 1 представлена сущностная характеристика ИБ с точки зрения совокупности научных гуманитарных знаний, ее определяющих. Так философский подход позволяет дать статичные и динамические свойства ИБ, социологический подход наделяет ИБ потенциалом отрицания и преодоления информационной опасности, политологический подход наделяет ИБ характеристиками целостности и доступности, аксиологическое основание через призму юридического подхода определяет ИБ, как состояние защищенности прав человека в информационной сфере.

Нормативная правовая регламентация ИБ применительно к органам внутренних дел обоснованно затрагивает и уголовно-правовые аспекты [12]. Уголовно-правовое содержание ИБ тесно связано с такими понятиями, как: конфиденциальность (тайны) информации, безопасность обращения с компьютерной информацией, права граждан на получение информации. В рассматриваемом контексте ИБ представляется в виде совокупности «общественных отношений, регулируемых системой правовых норм, направленных на обеспечение национальных интересов государства, интересов общества, на обеспечение законных интересов личности и субъектов хозяйствования в информационной сфере». Ключевой характеристикой в призме уголовно-правового регулирования является защита компьютерной информации от несанкционированного доступа, уничтожения, блокирования, модификации, копирования и неправомерного использования».

В этом смысле ассоциативное соотнесение системы ОВД с институтом принуждения приводит к однобокой трактовке понятия ИБ применительно возможной тематике соответствующих образовательных программ. Нормативный правовой контекст указанного понятия в искомом институте государственной

власти связывает ИБ только с защитой информации [13].

Сформулированная ранее сущность ИБ позволяет сделать вывод о том, что интерпретация искомого понятия в контексте ОВД исключает ряд значимых характеристик, к которым относится: обеспечение доступности информации, отрицание и преодоление информационной опасности, активное противодействие информационному насилию. Исключения приводят к нивелированию всех динамических свойств понятия ИБ, сводя его только в состояние защищенности ограниченного информационного пространства. При таком прочтении ИБ в контексте деятельности ОВД приобретает окрас как некий объект охраны без активного противоборства, что значительно сужает содержание образовательной подготовки в интересах ОВД по направлению ИБ.

Возможные решения противоречий основываются на конкретизации и системной структуризации образовательной подготовки в ведомственных ООВО. ИБ, как ключевое определение направлений подготовки не должно основываться на «таксономическом» представлении понятия, как обеспечения безопасности отдельных видовых объектов [14, с. 139]. А рассматриваться с точки зрения состояния защищенности собственного информационного пространства и защищенности от деструктивной информации. Подобная целевая установка позволяет расширить образовательный потенциал ведомственной подготовки кадров, увеличивая спектр возможных компетенций.

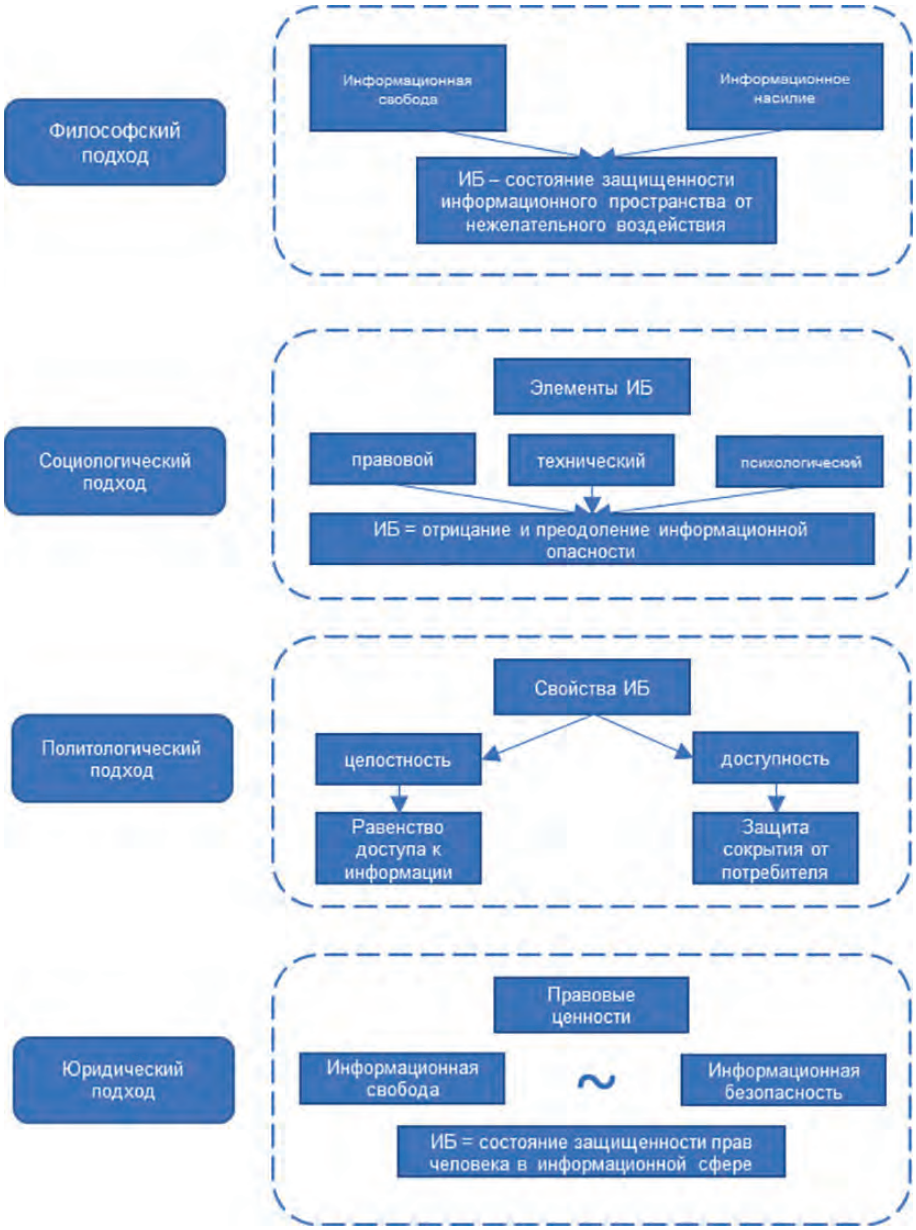


Рис. 1. Сущность понятия ИБ как метапредметной категории

3. Кибернетическая сущность ИБ

Описанное выше с позиций наук гуманитарного профиля метапредметное свойство (сущность) исследуемой области в рамках поставленной задачи на наш взгляд целесообразно дополнить практически не встречающимся в научных публикациях представлением, названным нами киберпарадигмой ИБ. Выбор этого термина сделан по примеру повального применения в последнее время понятий с приставкой кибер-... (киберпространство, киберугрозы, кибератаки и т.д.). В этом же аспекте лежит упомянутая выше нормативная легализация понятия «кибербезопасность» в виде наименования альтернативы научной специальности – информационная безопасность, методы и средства защиты информации.

Информационный поиск «на просторах Интернета» показал, что данный термин не является новацией авторов настоящей работы. Так в YouTube уже существует канал молодого пытливого исследователя PardigM[11], используемый для «романтического» описания государства будущего, «всеобщее процветание» на основе «правильной» цифровизации общественных отношений. То есть за счет технологических достижений можно добиться коренного изменения социальных отношений. Не вдаваясь в дальнейшую дискуссию, отметим только в качестве существенного замечания используемое определение понятия кибер (CYBER) как «приставка, использующаяся для того, чтобы присвоить слову значение чего-то относящегося к эпохе компьютеров, Интернета и цифровых технологий». Довольно распространенное представление, генезис которого будет обсужден ниже.

Применительно к сфере общественной безопасности данный термин по умолчанию, без определения, используется в публикации[12]. Но опять суть приставки понятен из контекста статьи и в целом совпадает с указанным выше представлением.

Недостаток таких представлений, несомненно, имеющих «право на жизнь», состоит в том, что они сильно сужают области возможного применения, так как авторы в своих рассуждениях используют критикуемый лингвистами подход от формы к значению и функции.

В отличие от этих публикаций в данной работе применительно к термину киберпарадигма будет обсуждаться его сущность, исходя из определения общего функционала систем обеспечения ИБ, то есть путем перехода от их функционала к форме понятия. Такой функционал определяется на основе кибернетического подхода, определяемого как «...наука об управлении, изучающая ... общие законы получения, хранения, передачи и преобразования информации в сложных управляющих системах»[13] независимо от формы их представления в материальном мире (см. рис. 2).

Рассматриваемая в данной работе взаимосвязь кибернетики и проблематики ИБ, правда по отношению к понятию «защита информации», была представлена еще в конце прошлого века профессором Герасименко В.А. в работе [15]. Суть такой взаимосвязи автор рассматривал через, введя очевидное, но практически, не используемое, понятие «качество информации», то есть условия, очевидно необходимое для эффективных управленческих процессов. В свою очередь, оно раскрывается через традиционное толкование информационной безопасности (защиты информации), в соответствии с упомянутым выше «гостовским» подходом: доступности, целостности и конфиденциальности.

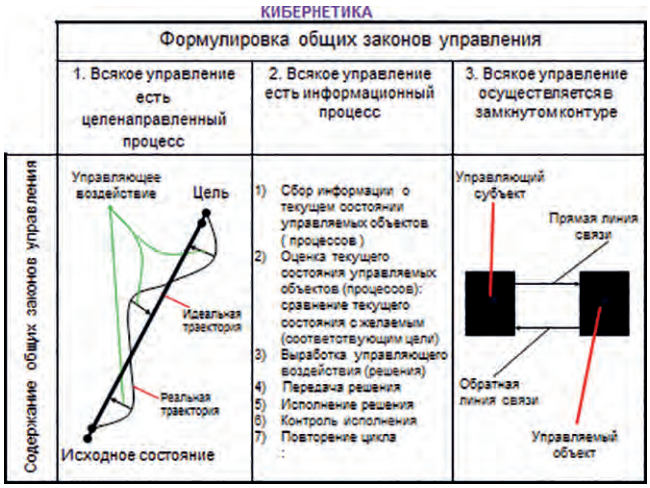


Рис. 2. Функционал кибернетического подхода [15]

Второй новацией рассматриваемой работы, связанной, в общем-то, с важной, но достаточно традиционной проблемой – повышением информационной грамотности, это представление уровня развития информации применительно к разным видам систем объектного (материального мира) (см. рис. 3).

Такое представление послужило толчком для дальнейшего расширения толкования киберпарадигмы ИБ с использованием сущности понятия «информационные ресурсы» (ИР). Оно имело легальное представление в недействующем с 2006 г. базовом законе «Об информации, информатизации и защите информации». Но, с методологической точки зрения, в рамках данной работы имеет смысл привести полностью определение функционала данного понятия:

11 [Философия] Основа киберпарадигмы. URL: https://www.youtube.com/watch?v=PjLbC_P-qoc (дата обращения: 24.05.2024).

12 Кибер-парадигма и общественная безопасность - действительно ли мы готовы. URL: https://safecity.by/index.php?route=revolution/revblog_blog&revblog_id=12 (дата обращения: 24.05.2024).

13 Кибернетика. Большая Советская энциклопедия. URL:https://bigenc.ru/c/kibernetika-979287 (дата обращения: 24.05.2024).

Рис. 3. Взаимосвязь видов информации и видов материального мира

«Глава 2., Статья 4. Основы правового режима ИР:

1. *Информационные ресурсы* являются объектами отношений физических, юридических лиц, государства, составляют ИР России и защищаются законом наряду с другими ресурсами.

Статья. 5 Документирование информации

1. *Документирование информации* является обязательным условием включения информации в ИР».

Не вдаваясь в обсуждение очевидной прагматической сущности понятия ИР как документированной информации, приведем возможную формулировку киберпарадигмы ИБ, определяющей известную риск-ориентированную или «бизнес»-процессную методологию обеспечения ИБ, применимую не только к предпринимательской деятельности, но и к государственной службе.

«Информационная безопасность – необходимое условие и цель деятельности в виде одного из показателей эффективности управления любой сложной системы управления. Управление невозможно без ИР (активов), защищаемых законом. Документирование – необходимое условие включения информации в ИР».

При таком киберпредставлении сложное описание сущности ИБ сводится к ее тривиальному прагматическому представлению как обеспечение безопасности делопроизводства и документооборота, в том числе в аналоговом (бумажном) виде с известными технологиями архивной деятельности. Недаром в указанном выше «гостовском» определении ИБ к трем основным критериям добавлены дополнительные: подлинности (п. 3.6), неотказуемости (п. 3.48) и достоверности (п. 3.55), что свидетельствует об интуитивном понимании прагматической сущности ИБ.

В то же время такое достаточно тривиальное представление не отменяет, а, скорее поясняет в современных условиях цифровизации общественной деятельности, многообразие системно-структурной сути («ниш») понятия ИБ. В частности, в отечественном законодательстве выделены: ограничение к государственной и профессиональным тайнам, ограничение распространения сведений, имеющих свойство конфиденциальности, защита персональных данных, в том числе общедоступного характера, безопасность электронного документооборота, обеспечение устойчивости критической информационной инфраструктуры, с разнообразными сложными механизмами и процедурами правового регулирования.

Очевидно разнообразие и прагматической сущности феномена ИБ. Любая система управления, рассматриваемая через призму технологий делопроизводства и документооборота, тем более в аспекте государственной службы, имеет свою специфику, исходя из назначения и функционала объекта управления. Это будет учитываться в дальнейшем уточнении профессиональных компетенций работников ОВД и вариативной части соответствующих образовательных программ.

Несмотря на указанную относительную общность предлагаемого толкования парадигмы ИБ на основе кибернетической сущности, необходимо в соответствии с законами диалектики также указать и на ограничение такого подхода.

Достаточно очевидно, что предлагаемая формулировка отражает лишь технологическую сущность феномена ИБ. Ее толкование, например, в рамках рассмотренного выше метапредметного свойства в аспекте гуманитарных наук достаточно затруднительно, хотя законы кибернетики по достаточно общепринятому представлению можно распространить и на процессы социального характера. Но такая пока неочевидная взаимосвязь кибернетики и ИБ требует дополнительного изучения представителями наук гуманитарного профиля.

Несколько слов о понятии «кибербезопасность» применительно к выводам данной работы. Его общее толкование, опирающееся на кибернетическую сущность феномена ИБ, по существу является его синонимом при указанном выше ограничении в аспекте гуманитарных подходов.

Но, исторически кибернетика наряду с другими научно-техническими достижениями давшая мощный импульс развитию компьютерных технологий, стала одной из фундаментальных основ так называемых «computer science» в развитых странах. Это и привело к более узкому толкованию приставки кибер-... как сущности, определяющей область своего применения только как в цифровом киберпространстве. С позиций полипарадигмального подхода это вполне допустимо, хотя в информационном противоборстве более важной и существенной частью является содержательный (контентный) подход, чем технологическая (инструментальная), составляющая.

Заключение

Представленные выше результаты анализа полипарадигмального подхода к толкованию сущности понятий ИБ и кибербезопасность, исходя из понятийной базы наук гуманитарного профиля и кибернетики, показывает, что в условиях, казалось бы, терминологического «хаоса» возможно достижение достаточно удовлетворительного уровня защищенности отечественной информационной инфраструктуры.

В то же время актуализируется необходимость дальнейшего совершенствования учебно-методической базы подготовки соответствующих специалистов в интересах ОВД, как совокупности структур отдельного вида государственной службы, обеспечивающего практически полную совокупность вопросов обеспечения ИБ Российской Федерации.

В частности, с позиций представленных подходов уже были проанализированы проекты новых ФГОС 4+ применительно к системе ОВД, подготовлены соответствующие предложения по их корректировке, которые в ближайшее время будут опубликованы в одном из научных изданий, входящих в перечень ВАК России.

Литература

1. *Горбатов, Виктор С.; Эрдниев, Александр С. Совершенствование подготовки кадров по обеспечению безопасности информационной инфраструктуры органов внутренних дел. Безопасность информационных технологий, [S.l.], т. 31, № 1, с. 100–119, 2024. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2024.1.06.*
2. *Девдариани Н. В., Рубцова Е. В. Законы диалектики в языке. Балтийский гуманитарный журнал. 2018, т. 7, № 2(23), с. 31–34. – EDN XULTMD.*
3. *Марков А. С. Кибербезопасность и Информационная Безопасность как Бифуркация Номенклатуры Научных Специальностей. Вопросы кибербезопасности. 2022, № 1(47), с. 2–9. DOI: 10.21681/2311-3456-2022-1-2-9. – EDN XMKFJH.*
4. *Столяров А. В. Информационная свобода и информационное насилие: специальность 09.00.11 «Социальная философия»: автореферат диссертации на соискание ученой степени кандидата философских наук. М. 2012 – 27 с.*
5. *Корягин В. В. Информационная реальность: сущность и особенности: специальность 09.00.11 «Социальная философия»: автореферат диссертации на соискание ученой степени кандидата философских наук. Улан-Удэ, 2018. – 25 с.*
6. *Медняк И. А. Военная безопасность современного общества в условиях новой информационной реальности: специальность 5.7.7. «Социальная и политическая философия»: диссертация на соискание ученой степени кандидата философских наук. Новочеркасск, 2022. – 160 с.*
7. *Добродеев А. Ю. Кибербезопасность в Российской Федерации. Модный термин или приоритетное технологическое направление обеспечения национальной и международной безопасности XXI века. Вопросы кибербезопасности. 2021, № 4(44), с. 61–72. DOI: 10.21681/2311-3456-2021-4-61-72. – EDN MXUVBS.*
8. *Жуйков А. Е. Информационная безопасность в условиях генезиса виртуального пространства трансформирующегося российского общества: специальность 22.00.04 «Социальная структура, социальные институты и процессы»: диссертация на соискание ученой степени кандидата социологических наук. Краснодар, 2016. – 155 с.*
9. *Артамонова Я. С. Информационная безопасность российского общества: теоретические основания и практика политического обеспечения: специальность 23.00.02 «Политические институты, процессы и технологии»: автореферат диссертации на соискание ученой степени доктора политических. М., 2014. – 56 с.*
10. *Туликов А. В. Информационная безопасность и права человека в условиях постиндустриального развития (теоретико-правовой анализ): специальность 12.00.01 «Теория и история права и государства; история учений о праве и государстве»: автореферат диссертации на соискание ученой степени кандидата юридических наук. М., 2017. – 24 с.*
11. *Мамедов Э. Ф. Терминология законодательства об информации, информационных технологиях и о защите информации как средство обеспечения информационной безопасности. Теория государства и права. 2023, № 1(30), с. 163–174. DOI: 10.25839/MATGIP_2023_1_163. – EDN NZVWLS.*
12. *Мнацаканян А. В. Информационная безопасность в Российской Федерации: уголовно-правовые аспекты: специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право»: автореферат на соискание ученой степени кандидата юридических наук. М., 2016. – 40 с.*
13. *Григорьев А. Н., Локтионов О. В., Подружкина Т. А. и др. Основы информационной безопасности в органах внутренних дел: Учебник. СПб: Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2019. – 312 с. – EDN SQGZCB.*
14. *Толстой Александр И. Систематика понятий в области информационной безопасности. Безопасность информационных технологий, [S.l.], т. 30, № 1, с. 130–148, 2023. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2023.1.10.*
15. *Герасименко В. А. Основы информационной грамоты. М.: Энергоатомиздат, 1996. – 320 с.*

CYBER PARADIGM OF INFORMATION SECURITY IN THE INTERNAL AFFAIRS BODIES

Gorbatov V. S.[14], Erdniev A. S.[15]

The purpose of the study *is to study the possibility and necessity of using a terminological description of the security of information technologies and systems.*

14 Viktor S. Gorbatov, Ph.D. in Engineering sciences, Associate Professor, National Research Nuclear University «MEPhI», (Moscow Engineering Physics Institute), Moscow, Russia. E-mail: VSGorbatov@mephi.ru, https://orcid.org/0000-0001-9998-9733

15 Aleksandr S. Erdniev, Ph.D. in Pedagogical sciences, Moscow University of the Ministry of Internal Affairs of the Russian Federation named after V. Y. Kikot, Moscow, Russia. E-mail: konfuci@inbox.ru, https://orcid.org/0009-0007-5363-8365

Research methods: *dialectical and polyparadigm approaches, system analysis, synthesis of solutions.*

The results obtained *can be useful to information security specialists in the creation and improvement of the internal (local) regulatory framework, as well as in the creation of educational and methodological materials in the field of educational services in the field of information security. The results obtained can also be recommended to potential authors of scientific publications in the aspect of dialectical presentation of their scientific achievements.*

Scientific novelty: *the author pays attention to the discussion of the cybernetic essence of the phenomenon under consideration, which from a pragmatic point of view has a relatively general nature and determines a more general interpretation of various concepts with the prefix cyber-..., in particular, the relationship between the terms information security and cybersecurity.*

Practical value: *from a practical point of view, this study is considered as a solution to a particular problem within the framework of the general problem of improving the training of personnel for internal affairs bodies.*

Keywords: *laws of dialectics, information security, cybernetics, cybersecurity, critical information infrastructure, meta-subjectivity, paradigm, conceptual apparatus, terminology*

References

1. *Gorbatov, Viktor S.; Erdniev, Aleksandr S. Sovershenstvovanie podgotovki kadrov po obespecheniju bezopasnosti informacionnoj infrastruktury organov vnutrennih del. IT Security, [S.l.], v. 31, no. 1, p. 100–119, 2024. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2024.1.06.*
2. *Devdariani N. V., Rubtsova E. V. Zakony dialektiki v jazyke. Baltic Humanitarian Journal. 2018, v. 7, no. 2(23), p. 31–34 – EDN XULTMD.*
3. *Markov A.S. Kiberbezopasnost' i Informacionnaja Bezopasnost' kak Bifurkacija Nomenklatury Nauchnyh Special'nostej. Issues of cybersecurity 2022, no. 1(47), p. 2–9 – EDN XMKFJH.*
4. *Stolyarov A. V. Informacionnaja svoboda i informacionnoe nasilie: special'nost' 09.00.11 «Social'naja filosofija»: avtoreferat dissertacii na soiskanie uchenoj stepeni kandidata filosofskih nauk, A. V. Stolyarov M. 2012 – 27 p.*
5. *Koryagin V. V. Informacionnaja real'nost': sushhnost' i osobennosti: special'nost' 09.00.11 «Social'naja filosofija»: avtoreferat dissertacii na soiskanie uchenoj stepeni kandidata filosofskih nauk. Ulan-Ude, 2018 – 25 p.*
6. *Mednyak I. A. Voennaja bezopasnost' sovremennogo obshhestva v uslovijah novoj informacionnoj real'nosti: special'nost' 5.7.7. «Social'naja i politicheskaja filosofija»: dissertacija na soiskanie uchenoj stepeni kandidata filosofskih nauk. Novocherkassk, 2022. – 160 p.*
7. *Dobrodeev A. Y. Kiberbezopasnost' v Rossijskoj Federacii. Modnyj termin ili prioritetnoe tehnologicheskoe napravlenie obespechenija nacional'noj i mezhdunarodnoj bezopasnosti XXI veka. Issues of cybersecurity. 2021, no. 4(44), p. 61–72. DOI: 10.21681/2311-3456-2021-4-61-72 – EDN MXUVBS.*
8. *Zhuikov A. E. Informacionnaja bezopasnost' v uslovijah genezisa virtual'nogo prostranstva transformirujushhegosja rossijskogo obshhestva: special'nost' 22.00.04 «Social'naja struktura, social'nye instituty i processy»: dissertacija na soiskanie uchenoj stepeni kandidata sociologicheskih nauk. Krasnodar, 2016. – 155 p.*
9. *Artamonova Ya. S. Informacionnaja bezopasnost' rossijskogo obshhestva: teoreticheskie osnovanija i praktika politicheskogo obespechenija: special'nost' 23.00.02 «Politicheskie instituty, processy i tehnologii»: avtoreferat dissertacii na soiskanie uchenoj stepeni doktora politicheskih. M., 2014. – 56 p.*
10. *Tulikov A. V. Informacionnaja bezopasnost' i prava cheloveka v uslovijah postindustrial'nogo razvitija (teoretiko-pravovoj analiz): special'nost' 12.00.01 «Teorija i istorija prava i gosudarstva; istorija uchenij o prave i gosudarstve»: avtoreferat dissertacii na soiskanie uchenoj stepeni kandidata juridicheskih nauk. M., 2017. – 24 p.*
11. *Mammadov E. F. Terminologija zakonodatel'stva ob informacii, informacionnyh tehnologijah i o zashhite informacii kak sredstvo obespechenija informacionnoj bezopasnosti. 2023, no. 1(30), p. 163–174. DOI: 10.25839/MATGIP_2023_1_163 – EDN NZVWLS.*
12. *Mnatsakanyan A. V. Informacionnaja bezopasnost' v Rossijskoj Federacii: ugolovno-pravovye aspekty: special'nost' 12.00.08 «Ugolovnoe pravo i kriminologija; ugolovno-ispolnitel'noe pravo»: avtoreferat na soiskanie uchenoj stepeni kandidata juridicheskih nauk. M., 2016. – 40 p.*
13. *Grigoriev A. N., Loktionov O. V., Druzhkina T. A. et al. Osnovy informacionnoj bezopasnosti v organah vnutrennih del: Uchebnik. SPb: Sankt-Peterburgskij universitet Ministerstva vnutrennih del Rossijskoj Federacii, 2019. – 312 p. – EDN SQGZCB.*
14. *Tolstoy Alexandr I. Sistematika ponjatij v oblasti informacionnoj bezopasnosti. IT Security (Russia), [S.l.], v. 30, no. 1, p. 130–148, 2023. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2023.1.10.*
15. *Gerasimenko V. A. Osnovy informacionnoj gramoty. M.: Energoatomizdat, 1996. – 320 p.*

ИНФОРМАЦИОННАЯ ВОЙНА И СОВРЕМЕННЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Малюк А. А.[1]

DOI: 10.21681/2311-3456-2024-5-105-114

Аннотация. *Появление данной статьи является следствием бурного развития в последнее время средств и технологий ведения информационной войны, практического превращения ее в основную форму военно-силового противоборства в XXI веке. В связи с этим особую остроту приобретает задача разработки концептуальных и методологических подходов к формированию комплексной системы обеспечения информационной безопасности, учитывающей принципиально междисциплинарный характер этого вида деятельности и необходимость принятия решений в условиях неполноты и недостоверности исходной информации. Под этим углом в статье предлагается рассматривать обеспечение информационной безопасности как совокупность процессов защиты информации и защиты от информации, что приводит к новым подходам к разработке соответствующих нормативно-методических документов и рационализации схем и структур управления комплексной защитой на объектовом, региональном и государственном уровнях.*

Ключевые слова: *информационная война, информационная безопасность, защита информации, защита от информации, комплексное обеспечение информационной безопасности, культура информационной безопасности.*

Введение

Постоянно расширяющееся использование новых информационных технологий привело мировую цивилизацию к формированию нового информационного общества. Сегодня все мы являемся свидетелями серьезнейших качественных изменений в экономической, социально-политической и духовной сферах общественной жизни. При этом необходимо констатировать, что развитие информационного общества, помимо расширения созидательных возможностей, приводит и к росту угроз национальной безопасности, связанных с нарушением установленных режимов использования информационных и коммуникационных систем, ущемлением конституционных прав граждан, распространением вредоносных программ, а также с использованием возможностей современных информационных технологий для осуществления враждебных, террористических и других преступных действий, причем и на межгосударственном уровне [1,2].

В связи с этим важнейшее значение в настоящее время приобретает задача обеспечения информационной безопасности (ИБ) как органической совокупности решения задач защиты информации и защиты от информации. Все это говорит о необходимости формирования научно-методологического базиса такой комплексной защиты как краеугольного камня интенсификации процессов обеспечения информационной безопасности. В подтверждение такой постановки проблемы можно сослаться на Доктрину информационной безопасности Российской Федерации, утвержденную Президентом страны в декабре 2016 года (Указ от 05.12.2016, № 646), которая констатирует, что «информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности России». В Доктрине прямо указывается, что «обеспечение информационной безопасности играет ключевую роль в обеспечении национальной безопасности страны».

И отечественные, и зарубежные специалисты единодушны в оценке чрезвычайной важности проблемы обеспечения ИБ, история которой насчитывает уже практически полвека. Естественно, что за истекшее после возникновения проблемы время коренным образом изменилось как представление о ее сущности, так и методологические подходы к решению. Как уже отмечалось, характерный для настоящего времени этап с полным правом может быть назван этапом комплексной защиты. Его особенность заключается в попытках обобщения всего имеющегося опыта теоретических исследований и практического решения задач обеспечения ИБ. Основная задача переживаемого этапа – перевод всего дела обеспечения ИБ на интенсивные способы, базирующиеся на строгой научной основе.

1 Малюк Анатолий Александрович, кандидат технических наук, профессор, Заслуженный работник высшей школы РФ, профессор кафедры криптологии и кибербезопасности (№42) НИЯУ МИФИ, Москва, Россия. E-mail: AAMalyuk@mephi.ru

Углубленное изучение проблемы формирования научно-методологического базиса теории защиты информации привело к выводу, что эффективное решение задач защиты возможно только с учетом органической взаимосвязи всего комплекса проблем развития информационного общества (научно-технических, организационно-правовых, гуманитарных). При этом в силу указанной специфики методологической основой теории должны являться неформально-эвристические подходы, учитывающие все многообразие дестабилизирующих факторов, в том числе, связанных с особенностями поведения человека – члена информационного общества.

Таким образом, представляется, что основная цель и направленность научных исследований в области обеспечения информационной безопасности заключается сегодня в разработке концептуальных и методологических подходов к интенсификации процессов защиты информации и защиты от информации, позволяющих усовершенствовать организацию систем защиты и управление их функционированием.

Информационная война как средство военно-силового противоборства

Исторический анализ тенденций в развитии военно-силового противоборства ясно показывает, что «информационные войны» практически превращаются в основное средство борьбы в XXI веке [3,4]. И этот процесс благодаря чрезвычайно высокой информационной зависимости всех сфер жизнедеятельности современного общества будет продолжаться со все возрастающей скоростью. Информационная война становится очень эффективным средством нанесения непоправимого ущерба «противнику», а «информационное оружие» начинает представлять все более серьезную военную угрозу.

В подтверждение этого можно привести оценку американских экспертов, утверждающих, что нарушение работы компьютерных сетей, используемых в системах управления государственными и банковскими структурами США, путем вывода из строя вычислительных и связных средств или уничтожения хранящейся в сетях информации способно нанести экономике страны настолько серьезный ущерб, что его можно сравнивать с ущербом от применения против США ядерного оружия[2].

Если говорить о негативном воздействии информации на личность и общество и необходимости применять в этом случае соответствующие меры защиты, то можно констатировать, что эта проблема имеет, вообще говоря, глубокие исторические корни. В качестве примера здесь можно привести Указ Императрицы Елизаветы Петровны[3], относящийся к XVIII веку. Дословно:

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

Сегодня можно выделить целый ряд основных объектов, как технического, так и социально-психологического характера, уязвимых с точки зрения вредного воздействия информации и нуждающихся в применении тех или иных средств защиты. К таким объектам относятся:

- военная информационная инфраструктура, решающая в интересах вооруженных сил задачи управления войсками и боевыми средствами, сбора и обработки информации;
- критическая информационная инфраструктура, объединяющая государственное управление, управленческие структуры кредитно-финансовой сферы, транспортных и промышленных предприятий;
- средства массовой информации, в первую очередь электронные (радио, телевидение, Интернет и т.д.);
- психологические ресурсы общества (система ценностей, индивидуальное и массовое сознание граждан, их психическое здоровье).

В последнее время значительно увеличилось число различных публикаций, посвященных таким вопросам как цели и последствия информационной войны, особенности и виды информационных войн, особенности применения информационно-технического оружия при ведении современных гибридных войн, информационные войны как результат социального управления и социального взаимодействия в эпоху глобализации, влияние информационных войн на стабильность государства, особенности ведения современных информационных войн в средствах массовой информации (СМИ) и в сети Интернет, социальные сети как инструмент ведения информационных войн, феномен так называемых «фейк-новостей» в современной информационной войне и др.

2 По материалам средств массовой информации.
3 Газета «С. Петербургские ведомости», 1750 г., № 46.

Основной вывод из анализа этих публикаций заключается в том, что сегодня проблема защиты от информационного оружия заслуживает самого пристального внимания. Дело в том, что, например, по данным ЦРУ США, число стран, разрабатывающих сегодня информационное оружие (в основном с использованием сети Интернет), превышает 120 (при 30, разрабатывающих оружие массового уничтожения), и рано или поздно они получат возможность вести информационные войны. Основными задачами в них, очевидно, будут дезорганизация функционирования критически важных военных, промышленных, административных объектов и систем «противника», а также информационно-психологическое воздействие на военно-политическое руководство, войска и население.

Каковы же основные цели информационной войны? Следуя тому, о чем уже говорилось, напрашивается заключение, что этими целями могут быть:

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

При этом объектом информационного противоборства может явиться любой объект, в отношении которого возможно осуществление информационного воздействия, результатом чего будет модификация его свойств как системы (информационной, экономической, политической и т.д.). Таким образом, ясно, что объектом информационного противоборства может стать любой сегмент информационно-психологического пространства, в том числе массовое и индивидуальное сознание граждан, социально-политические системы и процессы, информационная инфраструктура, информационные и психологические ресурсы.

Определив объекты информационного противоборства, необходимо определить и субъекты, которые могут применять информационное оружие. Сюда могут быть отнесены:

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

Все приведенные субъекты в этом случае должны обладать вполне определенными признаками, которые предполагают их заинтересованность и возможность осуществлять информационное противоборство. К этим признакам могут быть отнесены:

- наличие у субъекта в информационно-психологическом пространстве собственных интересов;
- наличие в составе субъекта специальных сил (структур), функционально предназначенных для ведения информационного противоборства или уполномоченных на его ведение;
- обладание информационным оружием или его разработка, а также разработка средств его доставки и маскировки;
- наличие под контролем субъекта определенного сегмента информационного пространства, в пределах которого он обладает преимущественным правом устанавливать нормы регулирования информационно-психологических отношений (на правах собственности, закрепленных нормами национального и международного законодательства) или государственным суверенитетом;
- существование в официальной идеологии положений, допускающих участие субъекта в информационном противоборстве.

Здесь целесообразно особо выделить роль в информационно-психологической борьбе транснациональных сетевых корпораций, которую можно охарактеризовать следующим образом.

Первое, транснациональные корпорации в глобальном информационном обществе практически обладают всеми признаками суверенного государства – территорией, определяемой ареалом распространения их сетевой инфраструктуры, стратегическими ресурсами (информационными потоками в их информационных и телекоммуникационных системах), «населением» (штатом сотрудников) и относительно полным суверенитетом.

DOI: 10.21681/2311-3456-2024-5-105-114

И второе, транснациональные корпорации, разрабатывая новые информационно-коммуникационные технологии, развивая свои информационные и телекоммуникационные системы и сети, контролируя циркулирующие по ним потоки, создают театр военных действий, на котором затем будут разворачиваться боевые действия между участниками информационно-психологического противоборства.

Итак, из проведенного нами краткого анализа военных и международных аспектов проблемы информационной войны можно сделать сегодня следующие основные выводы:

- ряд стран стремится получить преимущество в создании систем и средств ведения информационной войны, что представляло бы серьезную угрозу национальной безопасности России;
- создание целостного комплекса средств и методов ведения информационной войны будет осуществляться постепенно, по мере развития в мире базовых информационных технологий, что позволяет осуществлять мониторинг этого процесса;
- тема информационного оружия и информационной войны, в силу своей чрезвычайной важности для безопасности страны, требует комплексной проработки ее военно-стратегических, правовых, разведывательных и контрразведывательных аспектов, а также координации усилий всех заинтересованных ведомств России.

Общие аспекты проблемы безопасности как научной категории, подходы к обеспечению информационной безопасности

Прежде чем рассматривать проблемы, связанные с обеспечением информационной безопасности, целесообразно, наверное, определить содержание общего понятия «безопасность», тем более что среди специалистов в этой области единство в настоящее время практически отсутствует. Разработка общей теории безопасности (или, как принято называть ее сегодня, «секьюритологии») пока не нашла своего удовлетворительного разрешения, хотя, по мнению большинства ученых, формирование этого нового научного направления является важнейшим условием выживания и развития человечества. Пока по-прежнему многие базовые понятия и определения этого направления («безопасность», «опасность», «угроза безопасности», «виды безопасности» и др.) носят дискуссионный характер. При этом отметим, что если говорить о рассматриваемом нами предмете «информационная безопасность», то многие определения ИБ, которые хотя и могут быть приняты в плане практическом, не отражают специфики современного этапа формирования информационного общества.

Если рассматривать безопасность как общенаучную категорию, то представляется, что она может быть определена как некоторое качество той или иной системы, характеризующее, с одной стороны, ее способность противостоять дестабилизирующему воздействию внешних и внутренних угроз, а с другой – возможность возникновения и уровень угроз для элементов самой системы и внешней среды, связанных с ее функционированием.

При таком подходе мерой безопасности системы, очевидно, могут служить:

- с точки зрения способности противостоять дестабилизирующему воздействию внешних и внутренних угроз – степень (уровень) сохранения системой своей структуры, технологии и эффективности функционирования при воздействии дестабилизирующих факторов;
- с точки зрения отсутствия угроз для элементов самой системы и внешней среды – степень (уровень) возможности (или отсутствия возможности) появления таких дестабилизирующих факторов, которые могут представлять угрозу элементам системы или внешней среде.

Интерпретация данного подхода в области ИБ приводит нас к следующему возможному определению.

Информационная безопасность системы – это ее качество, характеризующее, с одной стороны, способность противостоять дестабилизирующему воздействию внешних и внутренних угроз информации, а с другой – уровень информационных угроз, которые создает ее функционирование для элементов самой системы и внешней среды.

Как видим, такое определение ИБ отличается от определения, положенного в основу Доктрины информационной безопасности Российской Федерации. Представляется, что использование термина «состояние защищенности» не учитывает происходящих в последнее время изменений в подходах к созданию новых информационных технологий (например, технологии облачных вычислений). При этом безопасность должна рассматриваться не как некоторая надстройка, обеспечивающая «состояние защищенности», а как изначальный базис технологии, т.е. ее непременное «качество». Таким образом, представление безопасности как качества более объективно характеризует способность системы противостоять тем или иным угрозам как внешнего, так и внутреннего характера.

Учитывая это, приведенное нами определение можно считать более полным и достаточно корректным. Вместе с тем, чтобы сделать его ориентиром при поиске решения проблемы обеспечения ИБ, необходимо уточнение и детализация его основополагающих понятий. В качестве отправной точки

такого уточнения используем тот факт, что информация как непременный компонент любой организованной системы, с одной стороны, легко уязвима, а с другой сама может быть источником угроз, как для элементов самой системы, так и для внешней среды. Отсюда естественным образом вытекает, что обеспечение ИБ в общей постановке проблемы может быть достигнуто лишь при взаимоувязанном решении двух задач (подтвердим это еще раз):

- ***защита информации***, под которой понимается защита находящейся в системе информации от дестабилизирующего воздействия внешних и внутренних угроз;
- ***защита от информации***, подразумевающая защиту элементов системы от дестабилизирующего воздействия внешних и внутренних информационных угроз, а также защиту внешней среды от информационных угроз со стороны рассматриваемой нами системы.

Еще одно важное, на наш взгляд, замечание. Проблема обеспечения ИБ является составляющей более общих проблем информатизации. Поэтому ее содержание должно формироваться в строгом соответствии с содержанием проблем информатизации, а концептуальные подходы к ее решению должны быть взаимоувязаны с концепциями информатизации.

Остановимся далее на современном состоянии теоретической и практической разработки проблемы обеспечения ИБ. Первая ее составляющая, т.е. проблема защиты информации, уже продолжительное время (свыше 40 лет) находится в центре внимания специалистов, и к настоящему времени на примере Российской Федерации можно говорить о следующих общепризнанных результатах:

- в настоящее время практически разработаны основы теории защиты информации;
- налажено широкомасштабное производство технических и программных средств защиты;
- создана целостная государственная система защиты информации;
- организована планомерная подготовка и повышение квалификации специалистов соответствующего уровня и профиля;
- накоплен значительный опыт практического решения задач защиты информации в системах различного масштаба и функционального назначения.

На основе перечисленных результатов можно констатировать, что защита информации сегодня имеет определенный базис для дальнейшего целенаправленного развития. При этом, основные задачи такого развития на ближайшую перспективу могут быть сформулированы следующим образом:

- организация регулярного сбора и обработки статистических данных о составе и результатах функционирования реальных систем защиты, которые необходимы для совершенствования методологии проектирования новых систем защиты, повышения эффективности их функционирования, дальнейшего развития теории защиты;
- создание организационных структур, обеспечивающих решение первой задачи, которые, как показывает накопленный на сегодня опыт, могут, например, формироваться в виде специализированных региональных и отраслевых центров защиты, способных обеспечить оказание широкого спектра услуг своим абонентам;
- дальнейшее развитие научно-методологического базиса как основы интенсификации процессов защиты.

Решение последней задачи, очевидно, включает следующие проблемы:

- формирование более общей (по сравнению с классической) теории систем, ориентированной не только на технические, но и на социальные системы;
- разработка строгой аксиоматической теории защиты информации, базисом которой должны служить общая теория систем и статистические данные о структуре и функционировании реальных систем защиты;
- разработка комплекса рабочих моделей, необходимых и достаточных для решения всей совокупности задач защиты информации.

Обратимся далее к состоянию дел с изучением и разработкой мер обеспечения второй составляющей ИБ – защиты от информации. При этом обратим внимание на то, что информация способна оказывать такое воздействие как на технические комплексы, так и на людей, результаты которого могут носить не просто негативный, а трагический и даже катастрофический характер. Все это свидетельствует о чрезвычайной важности проблемы защиты от информации в условиях формирования информационного общества. Причем, необходимо отметить, что проблема защиты от информации существенно сложнее проблемы защиты информации в силу того, что информационные угрозы чрезвычайно многообразны, а их воздействие далеко не всегда очевидно.

В постановочном плане задача защиты от информации естественным образом делится на две составляющие: защита от информации технических средств и систем и аналогичная защита людей. Если говорить о первой составляющей, т.е. защите от информации технических средств и систем, то можно констатировать, что основные положения развиваемой

в последнее время концепции комплексной защиты информации остаются здесь вполне адекватными (с точностью до нюансов терминов). Предотвращение же и нейтрализация информационных угроз, направленных на людей, требуют не столько технических решений, сколько организационно-правовых и политических, причем не только на внутригосударственном, но и на международном уровне.

Таким образом, отличительная особенность проблемы защиты людей от информации, создающая, кстати, немалые дополнительные трудности, состоит в том, что ее решение носит преимущественно гуманитарный характер, в то время как решения по защите от информации технических средств и систем имеют существенную техническую составляющую и, в основном, поддаются строгой структуризации.

Современная постановка задач защиты информации и защиты от информации

Для обеспечения информационной безопасности, как следует из предыдущего изложения, необходимо решение двух задач – защиты информации и защиты от информации.

Если говорить о первой из них, то необходимо отметить, что в современных условиях существуют и объективная необходимость, и объективные предпосылки для кардинального изменения взгляда на саму проблему защиты информации и подходы к ее решению. Заметим, что необходимость своевременного видоизменения постановки задачи является одним из важнейших общеметодологических принципов развития науки.

Основные факторы, обуславливающие объективную необходимость назревшего изменения постановки задачи защиты, заключаются в следующем.

1. ***Исключительное повышение значимости информации как общественного ресурса***. Отметим, что главным противоречием современного информационного общества является как бы «индустриальный» характер современных информационных технологий, с одной стороны, и сохраненный со времен индустриального общества характер управления им, существенно зависящий от искусства управленческого персонала. В целях преодоления названного противоречия управление должно быть основано на других принципах, как бы использующих методы поточно-индустриального производства. Осуществление такого перевода и составляет одну из главных задач развития информационного общества. А поскольку всякое управление в основе своей есть информационный процесс, то это еще раз подтверждает тот факт, что информация приобретает сегодня статус главного ресурса общества со всеми вытекающими из этого требованиями, предъявляемыми к обращению с ним.
2. ***Существенные изменения в организации информационных технологий***. Современные информационные технологии характеризуются массовым насыщением сверхбыстродействующими компьютерными средствами и объединением их в глобальные сети, что обеспечивает расширение обработки огромных объемов информации в очень короткие сроки, не достижимые на предыдущих этапах общественного развития.
3. ***Все возрастающие опасности злоумышленных действий по отношению к информации и злоумышленного ее использования***. Настоящее время характеризуется исключительным ростом преступности, использующей возможности информационно-коммуникационных технологий для нанесения ущерба интересам граждан, общества и государства. При этом возможности злоумышленного использования информации достигли такого уровня, что сегодня, как уже отмечалось выше, практически ведутся информационные войны.

Решить возникающие в этих условиях проблемы можно только видоизменив саму постановку задачи защиты информации. Успех в этом могут обеспечить следующие обстоятельства.

1. ***Наличие богатого опыта организации различных защитных процессов по отношению к информации как в традиционных («бумажных»), так и в автоматизированных технологиях ее обработки***. На сегодняшний день отработаны современные методологии обеспечения сохранности (целостности) информации, ее надежности, качества обработки и выдачи, регулирования использования (предупреждения несанкционированного доступа).
2. ***Значительные достижения в научном обеспечении названных выше процессов***. В последние два десятилетия XX века большое развитие получили теория надежности [5–7] и теория обеспечения качества информации [8]. В настоящий момент можно также с уверенностью утверждать, что разработаны основы теории защиты информации (в первую очередь трудами отечественных ученых).
3. ***Возможности решения всех проблем организации защитных процессов по отношению к информации в рамках единой концепции***. Такой концепцией может стать разрабатываемая в теории защиты информации унифицированная концепция защиты [9,10].

Таким образом, видоизмененная постановка задачи защиты информации должна учитывать

совокупность следующих основных концептуальных положений:

- интегральное представление понятия комплексности защиты информации в целевом и инструментальном планах;
- расширение рамок защиты от обеспечения компьютерной безопасности до защиты информации на объекте и защиты информационных ресурсов региона и государства;
- комплексное организационное построение систем защиты информации;
- обеспечение условий наиболее эффективного использования информации;
- переход к так называемой упреждающей стратегии осуществления защитных процессов.

Фактически при таком подходе проблема защиты информации как бы перерастает в более общую проблему управления информационными ресурсами.

Помимо защиты информации важнейшей составляющей обеспечения информационной безопасности является защита от информации, т.е. защита автоматизированных систем и людей (отдельно взятого человека, коллектива людей, населения региона или государства в целом) от разрушающего воздействия информации. Однако, разработка системно-концептуальных подходов к решению этой проблемы находится сегодня на начальной стадии. Объективная причина такого положения заключается в необычности проблемы, чрезвычайной ее сложности, многоаспектности и высоком уровне неопределенности. Существует и субъективная причина, заключающаяся в отсутствии до последнего времени общегосударственной востребованности серьезного решения этой проблемы. В средствах массовой информации время от времени появляются публикации по отдельным вопросам и конкретным фактам злоумышленного использования информации как средства противоборства при силовом решении политических, социальных и экономических проблем. Однако системные теоретико-концептуальные исследования проблемы защиты от информации еще ждут своего осуществления. Представляется, что положение здесь должно существенно улучшиться в связи с реализацией Стратегии развития информационного общества и Доктрины информационной безопасности Российской Федерации.

Выше мы уже упоминали о возможности трансформации в этих целях основных положений УКЗИ и использования их для решения задачи защиты от вредной информации различного рода автоматизированных систем. Действительно, основанием такого вывода служат сравнительно тесная родственная связь обеих задач и высокий уровень проработки и научной обоснованности УКЗИ. Как показывает практика использования основных положений УКЗИ при создании реальных систем защиты информации, она применима для обеспечения эффективной защиты в любых автоматизированных системах, в том числе организационно-технологического типа, на всех трех уровнях защиты: компьютерном, объектовом, региональном (государственном). На этой основе может быть сделан фундаментальный вывод о том, что полномасштабная реализация УКЗИ является основной частью задачи защиты от информации автоматизированных систем.

Если говорить о второй части информационной войны – негативном воздействии на человека (общество или отдельную личность), то при формулировании задачи защиты от информации в этом случае, естественно, возникает вопрос: каковы же возможности противостоять такому информационному воздействию?

Помимо технологических средств защиты информации и обеспечения информационной безопасности (противодействия так называемым киберугрозам), которые, конечно, и в этом случае имеют существенное значение, важнейшая роль должна отводиться здесь готовности общества к информационному противоборству и способности его противостоять различного рода манипуляциям общественным и личным сознанием граждан. Речь идет о своего рода психологических ресурсах общества, под которыми следует понимать систему ценностей общества и ее устойчивость по отношению к внешним или внутренним деструктивным воздействиям, индивидуальное и массовое сознание граждан и его устойчивость к манипулятивному воздействию и вовлечению в противоправную деятельность различными методами тайного принуждения личности. Наконец, к психологическим ресурсам должно быть отнесено также психическое здоровье граждан и его устойчивость по отношению к внешним или внутренним деструктивным воздействиям. Все это может быть представлено как развитие психологических ресурсов общества. Таким образом, в содержательном плане задача защиты от информации должна в современных условиях включать такие элементы как повышение уровня образования членов информационного общества и формирование культуры информационной безопасности.

Необходимость, пути и условия перехода к интенсивным способам обеспечения информационной безопасности

Под интенсификацией обычно понимается увеличение интенсивности и повышение производительности каких-либо действий, опирающееся, прежде всего, на достижения научно-технического прогресса. С уверенностью можно констатировать, что это довольно характерно для процессов, происходящих

в последнее время в области обеспечения информационной безопасности. При этом, если говорить о первой составляющей – защите информации, то преобладавший здесь до недавнего прошлого подход с полным основанием может быть назван экстенсивным, опирающимся на независимую организацию защиты на каждом объекте информатизации. В противоположность ему, интенсивный подход, являющийся предметом нашего рассмотрения, предполагает организацию защиты информации в соответствии с некоторой единой, научно обоснованной концепцией в масштабах региона и государства в целом.

Таким образом, переход к интенсивным способам защиты означает целенаправленную реализацию всех достижений теории и практики, которые, как мы это уже отмечали, в концентрированном виде отражены в унифицированной концепции защиты информации. С сегодняшних позиций можно выделить ряд основных положений УКЗИ, практическая реализация которых и будет означать переход к интенсивным способам защиты, причем как информации, так и от информации. К этим положениям могут быть отнесены следующие.

1. ***Структурированное описание среды защиты***. Такое описание позволяет четко представить структуру защищаемого объекта или системы и применяемую технологию обработки информации. При этом удобно в целях унификации методов такого описания ввести понятия типового структурного компонента и его типового состояния.
2. ***Количественный анализ степени уязвимости информации***. Такой анализ необходим для объективной оценки реальных угроз информации, принимаемых усилий и расходов на ее защиту. Отметим, что в основах теории защиты информации разработана довольно развитая методология оценки уязвимости информации, состоящая из трех элементов: системы показателей уязвимости, системы угроз информации и системы моделей определения текущих и прогнозирования ожидаемых значений показателей уязвимости.
3. ***Научно обоснованное определение требуемого уровня защиты***. Объективные трудности решения этой задачи связаны с тем, что на уровень защиты как информации, так и от информации в рамках конкретных объектов и условий их функционирования оказывает влияние большое количество разноплановых факторов. При этом, количественное определение требуемого уровня защиты должно быть основано на структуризации всех влияющих на него факторов и их количественных оценках.

Таким образом, интенсификация процессов защиты на основе единой методологии должна, в конечном счете, обеспечить построение оптимальных систем защиты с количественными оценками получаемых решений. При этом оптимизация систем защиты возможна в двух постановках, либо как обеспечение максимально возможного уровня защиты при имеющихся ресурсах, либо как обеспечение требуемого уровня защиты при минимальном расходовании ресурсов. Следует отметить, что для достижения указанных целей может быть использован как бы кортеж концептуальных решений, представляющий собой следующую последовательность: функции защиты – задачи защиты – средства защиты – система защиты. Дадим определения этих элементов кортежа:

- ***функция защиты*** – совокупность однородных в функциональном отношении мероприятий, регулярно осуществляемых в защищаемой системе различными способами и методами, с целью создания, поддержания и обеспечения условий, объективно необходимых для ее надежной защиты (причем, как информации, обрабатываемой в системе, так и от вредной информации, нарушающей ее работу);
- ***задача защиты*** – организованные возможности средств, методов и мероприятий, осуществляемых в защищаемой системе с целью полной или частичной реализации одной или нескольких функций защиты;
- ***система зашиты*** – организованная совокупность всех средств, методов и мероприятий, выделяемых (предусматриваемых) в защищаемой системе для решения в ней выбранных задач защиты.

Кортеж концептуальных решений создает основу для синтеза оптимальных систем защиты информации с количественными оценками достигаемого уровня защиты. Однако, необходимо отметить ряд трудностей, возникающих при их практической реализации. Наиболее серьезной проблемой здесь является формирование баз исходных данных, необходимых для реализации моделей систем и процессов защиты. Задача эта весьма трудоемкая, да к тому же не может быть решена на основе формальных методов. О трудоемкости задачи можно судить хотя бы по количеству данных, которые надо определять. Это количество оценивается даже для несложных систем числом в несколько тысяч.

Трудности формирования указанных баз исходных данных помимо большого их объема усугубляются еще и весьма высоким уровнем неопределенности, связанной с непредсказуемостью поведения злоумышленников. Исследования данного аспекта проблемы в процессе формирования теории защиты

информации на сегодняшний день привели к выводу, что единственным возможным способом формирования исходных данных является использование неформально-эвристических методов (или другими словами различных видов экспертных оценок). Кроме того, непрерывное изменение условий защиты, постоянный рост возможностей злоумышленного доступа к защищаемой информации, а также совершенствование методов ее защиты требуют того, чтобы экспертные оценки были не просто перманентными, а практически непрерывными. Этого можно достичь лишь при наличии стройной и целенаправленной организации сопровождения работ по защите. Наиболее полным и наиболее адекватным решением этой проблемы было бы создание сети специализированных центров защиты информации (ЦЗИ), аккумулирующих все новейшие достижения в области защиты и специализирующихся на формировании научно-методологического и инструментального базиса решения соответствующих задач на интенсивной основе (включая и базы необходимых исходных данных). Концепция создания и организации работы ЦЗИ к настоящему времени разработана достаточно полно [11,12]. Отметим, что в соответствии с этой концепцией на сегодняшний день в системе высшей школы, например, на базе ряда ведущих вузов уже созданы 29 региональных учебно-научных центров.

В заключение обратим внимание еще на одно весьма важное обстоятельство. Нетрудно видеть, что перевод процессов защиты информации и защиты от информации на интенсивные способы нуждается также в организации эффективной системы кадрового обеспечения информационной безопасности.

Литература

1. *Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы / Под ред. В. А.Садовничего и В. П.Шерстюка. – М.: МЦНМО, 2002;*
2. *Манойло А. В., Петренко А. И., Фролов Д. Б. Государственная информационная политика в условиях информационно-психологической войны. – М.: Горячая линия – Телеком, 2003.*
3. *Расторгуев С. П. Философия информационной войны. – М.: Вузовская книга, МПСИ, 2003.*
4. *Ламинина О. Г. Информационные войны: миф или реальность? // Гуманитарные ведомости Тульского государственного педагогического университета им. Л. Н. Толстого (сетевое издание), 2018, №1 (25).*
5. *Дружинин Г. В. Надежность автоматизированных систем. – М.: Энергия, 1997.*
6. *Самойленко С. И., Давыдов Д. А., Золотарев В. В., Третьякова В. Н. Вычислительные сети (адаптивность, помехоустойчивость, надежность). – М.: Наука, 1981.*
7. *Пивоваров А. Н. Методы обеспечения достоверности информации в АСУ. – М.: Радио и связь, 1982.*
8. *Герасименко В. А. Основы управления качеством информации. – М.: Московский историко-архивный институт, 1989, деп. В ВИНИТИ 26.06 89, №5392В89.*
9. *Герасименко В. А., Малюк А. А. Основы защиты информации: Учебник. – М.: МИФИ, 1997.*
10. *Малюк А. А. Теория защиты информации. – М.: Горячая линия–Телеком, 2012.*
11. *Проблемы создания и организации работы центров защиты информации /под ред. А. А.Малюка. // Безопасность информационных технологий, № 4, 1997.*
12. *Малюк А. А., Поляков А. А. Региональные учебно-научные центры по проблемам информационной безопасности – организационная основа реализации положений Доктрины информационной безопасности Российской Федерации в системе высшей школы. // Материалы VIII Всероссийской научно-практической конференции «Проблемы информационной безопасности в системе высшей школы», Москва, 2001.*

INFORMATION WARFARE AND MODERN PROBLEMS OF INFORMATION SECURITY

Malyuk A. A.[4]

Abstract. *The appearance of this article is a consequence of the rapid development of means and technologies of information warfare in recent years, its practical transformation into the main form of military-force confrontation in the 21st century. In this regard, the task of developing conceptual and methodological approaches to the formation of an integrated information security system that takes into account the fundamentally interdisciplinary nature of this type of activity and the need to make decisions in conditions of incompleteness and unreliability of initial information is becoming particularly acute. From this point of view, the article proposes to consider information security as a set of processes of information protection and protection against information, which leads to new approaches to the development of relevant regulatory and methodological documents and rationalization of schemes and structures for managing integrated protection at the object, regional and state levels.*

Keywords: *information war, information security, information protection, protection from information, integrated information security, culture of information security.*

4 Anatoly A. Malyuk, Ph.D. (in Tech.), , Professor, Honored Worker of Higher Education of the Russian Federation, Professor of the Department of Cryptology and Cybersecurity (No42) of the National Research Nuclear University MEPhI, Moscow, Russia. E-mail: AAMalyuk@mephi.ru

References

1. *Strel'cov A. A. Obespechenie informacionnoj bezopasnosti Rossii. Teoreticheskie i metodologicheskie osnovy / Pod red. V. A. Sadovnichego i V. P. Sherstjuka. – M.: MCNMO, 2002;*
2. *Manojlo A. V., Petrenko A. I., Frolov D. B. Gosudarstvennaja informacionnaja politika v uslovijah informacionno-psihologicheskoj vojny. – M.: Gorjachaja linija – Telekom, 2003.*
3. *Rastorguev S. P. Filosofija informacionnoj vojny. – M.: Vuzovskaja kniga, MPSI, 2003.*
4. *Laminina O. G. Informacionnye vojny: mif ili real'nost'? // Gumanitarnye vedomosti Tul'skogo gosudarstvennogo pedagogicheskogo universiteta im. L. N. Tolstogo (setevoe izdanie), 2018, №1 (25).*
5. *Druzhinin G. V. Nadezhnost' avtomatizirovannyh sistem. – M.: Jenergija, 1997.*
6. *Samojlenko S. I., Davydov D. A., Zolotarev V. V., Tret'jakova V. N. Vychislitel'nye seti (adaptivnost', pomehoustojchivost', nadezhnost'). – M.: Nauka, 1981.*
7. *Pivovarov A. N. Metody obespechenija dostovernosti informacii v ASU. – M.: Radio i svjaz', 1982.*
8. *Gerasimenko V. A. Osnovy upravlenija kachestvom informacii. – M.: Moskovskij istoriko-arhivnyj institut, 1989, dep. V VINITI 26.06 89, №5392B89.*
9. *Gerasimenko V. A., Maljuk A. A. Osnovy zashhity informacii: Uchebnik. – M.: MIFI, 1997.*
10. *Maljuk A. A. Teorija zashhity informacii. – M.: Gorjachaja linija–Telekom, 2012.*
11. *Problemy sozdanija i organizacii raboty centrov zashhity informacii /pod red. A. A.Maljuka // Bezopasnost' informacionnyh tehnologij, № 4,1997.*
12. *Maljuk A. A., Poljakov A. A. Regional'nye uchebno-nauchnye centry po problemam informacionnoj bezopasnosti – organizacionnaja osnova realizacii polozhenij Doktriny informacionnoj bezopasnosti Rossijskoj Federacii v sisteme vysshej shkoly. // Materialy VIII Vserossijskoj nauchno-prakticheskoj konferencii «Problemy informacionnoj bezopasnosti v sisteme vysshej shkoly», Moskva, 2001.*

ДОВЕРЕННАЯ ЭЛЕКТРОНИКА НА ФОРУМЕ «МИКРОЭЛЕКТРОНИКА 2024»

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ

Кессаринский Л. Н.[1]

DOI: 10.21681/2311-3456-2024-5-115-119

Премьер-министр Правительства РФ М. В. Мишустин и Президент РАН Г. Я. Красников на выставке Форума «Микроэлектроника 2024»

23–27 сентября в Федеральной территории (ФТ) Сириус состоялся юбилейный Десятый Российский форум «Микроэлектроника 2024», пожалуй, крупнейшее отраслевое событие года. Научная программа состояла из более 300 докладов, структурированных в виде пленарных заседаний, трека тематических обзорно-аналитических заседаний и 13 тематических секций. Деловая программа включала более 38 круглых столов, на которых обсуждались вопросы взаимодействия регуляторов, бизнеса, научной и образовательной среды. Экспозиционная площадка Форума включала около 200 стендов. До основной программы в ФТ Сириус, в Москве на базе Консорциума НИЯУ МИФИ и АО «ЭНПО СПЭЛС» прошла Предконференция №1 «Доверенная и экстремальная электроника» (9–12 сентября), в Зеленограде на базе НИУ МИЭТ состоялась Предконференция №2.

Основная программа Форума открылась 23 сентября выступлением председателя программного комитета Форума, президента РАН, академика Г. Я. Красникова, который огласил приветствие участникам Форума Президента РФ В. В. Путина и представил слово для выступления премьер-министру Правительства РФ М. В. Мишустину. В первом пленарном заседании также приняли участие Первый

1 Кессаринский Леонид Николаевич, кандидат технических наук, заместитель директора АИЦ ИБСЗИ НИЯУ МИФИ, руководитель РГ «ДИС» и ЭАГ. Москва, Россия. E-mail: LNKessarinskiy@mephi.ru

вице-премьер Правительства РФ Д. В. Мантуров, Министр промышленности и торговли РФ А. А. Алиханов, Министр цифрового развития, связи и массовых коммуникаций РФ М. И. Шаддаев, Министр образования и науки РФ В. Н. Фальков, Председатель правления ПАО «Сбербанк России» Г. О. Греф. Пленарное заседание завершилось награждением специалистов электронной отрасли государственными и отраслевыми наградами.

Важнейшей тематикой Форума, определившей скоординированную программу Предконференции №1, одного из пленарных заседаний и тематического трека обзорно-дискуссионных заседаний, стало обеспечение объектов гражданской критической (в том числе информационной) инфраструктуры доверенной электроникой (электронными компонентами, программно-аппаратными комплексами, системами). Актуальность данного направления, число заявляемых докладов, количество участников на Форуме каждый год растет в среднем на 25–30%.

Оговоримся, что под доверенным изделием активной электронной компонентной базы (АЭКБ) понимается изделие АЭКБ с подтвержденным соответствием заданным требованиям по качеству (работоспособности, надежности и стойкости к режимам и условиям эксплуатации) и безопасности (информационной, функциональной и технологической) [ПНСТ 911-2024 «Критическая информационная

инфраструктура. Доверенные интегральные микросхемы и электронные модули. Общие положения»].

До 2022 года субъекты критической информационной инфраструктуры (КИИ) закупали системы управления своими объектами «под ключ», опираясь прежде всего на узнаваемость и репутацию брендов (в подавляющем большинстве – иностранных), и не анализировали их состав даже на уровне ПАКов или, тем более, отдельных ЭКБ. С уходом авторитетных иностранных производителей и введения санкций, выходит Указ Президента РФ № 166 от 30.03.2022 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации», а затем развивающие его Постановления Правительства № 1280 от 22.08.2022 (об ограничении применения иностранного ПО на объектах КИИ) и № 1912 от 14.09.2023 (о порядке перехода субъектов КИИ на доверенные ПАКи). В рамках поручений Указа № 166 создается Научно-производственное объединение «Критические информационные системы» (АО «НПО «КИС»), специализирующегося на разработке, производстве, технической поддержке и сервисном обслуживании доверенных ПАК для КИИ. На базе АО «НПО «КИС» создается Технический комитет по стандартизации «ПАК для КИИ и ПО для них» № 167, в составе которого уже на базе НИЯУ МИФИ собрана Рабочая группа «Доверенные интегральные

DOI: 10.21681/2311-3456-2024-5-115-119

схемы» (РГ «ДИС») из числа представителей организаций комитета, дополняемая Экспертно-аналитической группой по вопросам обеспечения доверенности (ЭАГ), состоящая из числа экспертов отрасли (физических лиц).

Пленарное заседание «Доверенные программно-аппаратные комплексы и ЭКБ для объектов критической информационной инфраструктуры» собрало более 1 тысячи очных участников (не считая онлайн). В ходе пленарного заседания модератором (А. Ю. Никифоровым, НИЯУ МИФИ) был сделан обзор проблемной ситуации с доверенными ПАК и ЭКБ. Далее были представлены основные результаты деятельности ГК «Росатом» в сфере КИИ (А. Б. Шевченко, ГК «Росатом»), меры поддержки и направления нормативного регулирования (А. А. Заренин, Минцифры РФ и А. А. Гапонов, Минпромторг РФ). Рассмотрены научные вопросы квантовой сети (А. В. Глейм, ОАО «РЖД») и исследования киберустойчивости (Д. П. Зегжда, СПб Политех), представлены практический взгляд на проблемную ситуацию с доверенными ЭКБ с точки зрения РГ «ДИС» и ЭАГ в вопросах и ответах (Л. Н. Кессаринский, НИЯУ МИФИ) и доверенные процессоры для ПАК объектов ИИ (К. А. Трушкин, АО «МЦСТ»), национальный проект беспилотных автономных средств как драйвер для доверенной электроники (И. Г. Анцев, АО «НПП «Радар ммс»).

Научная программа Форума по тематике доверенной электроники в четверг 26.09.24 и пятницу 27.09.24 продолжилась четырьмя обзорно-дискуссионными заседаниями, объединенными в единый Трек «Доверенные ПАК и ЭКБ для КИИ»:

- Заседание 1 «Сквозное внедрение доверенных электронных компонентов и систем в транспорте», модератор – Д. В. Корначев, Ассоциация «Консорциум предприятий в сфере автомобильных электронных приборов и телематики» («Автоэлектроника») – 8 докладов,
- Заседание 2 «Доверенные решения для коммуникаций и интернета вещей», модераторы – А. Ю. Никифоров (НИЯУ МИФИ), Е. В. Хасин (Минцифры РФ) – 5 докладов,
- Заседание 3 «Переход на доверенные ПАК в КИИ: возможности, вызовы и перспективы», модератор – К. А. Смазнов (ГК «Росатом») – 6 докладов,
- Заседание 4 «Обеспечение и оценка информационной безопасности доверенных ПАК и ЭКБ», модератор – А. А. Шелупанов (ТУСУР) – 7 докладов.

Таким образом, на Форуме были представлены и всесторонне проанализированы основные идеи по методам задания и оценки соответствия требованиям по доверенности в целом, а также по отдельным составляющим (качеству и безопасностям). Были представлены наработки РГ «ДИС» и ЭАГ по стандартизации вопросов доверенности, представлена концепция проектов ПНСТ на Общие технические условия для доверенных интегральных микросхем.

Команда Консорциума «Доверенные и экстремальные электронные системы» (НИЯУ МИФИ и АО «ЭНПО СПЭЛС») отлично отработала на Форуме.

Фотоцитаты докладчиков взяты из официального телеграм канала Форума «Микроэлектроника 2024»: t.me/forum_microelectronica

Команда Консорциума НИЯУ МИФИ и АО «ЭНПО СПЭЛС» на Форуме «Микроэлектроника 2024» (слева направо): Л. Н. Кессаринский, А. С. Марков, А. П. Дураковский, А. В. Уланова, Г. В. Чуков, А. О. Ширин, И. Б. Леухин, Ю. М. Московская, А. Ю. Никифоров, Н. А. Усачев, Д. И. Грицаенко, А. Р. Грицаенко, Д. С. Уваркин.

DOI: 10.21681/2311-3456-2024-5-115-119

CYBERSECURITY ISSUES

SCIENTIFIC PEER-REVIEWED JOURNAL

2024, № 5 (63)

Cybersecurity Issues is a research periodical scientific and practical publication specializing in information security.
Published six times a year

https://cyberrus.info

The journal is being published from 2013
(Registration Certificate PI No. FS 77-75239).
CrossRef number (DOI): 10.21681/2311-3456

The journal is included in the Russian list of peer-reviewed academic publications of the Higher Attestation Commission (VAK), it is registered in the Russian Science Citation Index (RSCI/RINTs) on the Web of Science (WoS) platform and holds the 1st place in its cyber security rating. The journal's articles are available in full text

Founder and publisher
JSC «NPO «Echelon»
Postal address: Elektrozavodskaya str., 24, bld. 1, 107023, Moscow, Russia
E-mail: editor@cyberrus.info

CONTENTS

ИИКС
70 лет НИЯУ МИФИ

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРЫ

12 кафедра
Компьютерные системы и технологии

22 кафедра
Кибернетика

41 кафедра
Криптография и безопасность компьютерных систем

42 кафедра
Криптология и кибербезопасность

43 кафедра
Стратегические информационные исследования

44 кафедра
Информационная безопасность банковских систем

CYBERSECURITY ISSUES
VOPROSY KIBERBEZOPASNOSTI

№5 2024

DOI: 10.21681/2311-3456

МИФИ
Национальный
исследовательский
ядерный университет

www.cyberrus.info
editor@cyberrus.info