ISSN 2225-5435

Вестник УрФО.

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 1(47) / 2023

УЧРЕДИТЕЛИ

ФГАОУ ВО «ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИУ)»

ООО «ЮЖНО-УРАЛЬСКИЙ ЮРИДИЧЕСКИЙ ВЕСТНИК»

Подписной индекс 73852 в каталоге «Почта России»

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

Свидетельство ПИ № ФС77-65765 от 20.05.2016

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

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

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

16+

Journal of the Ural Federal District. Information security

ISSN 2225-5435

№ 1(47) / 2023

FOUNDER

SOUTH URAL STATE UNIVERSITY (NIU)

SOUTH URAL LEGAL NEWSLETTER

Subscription index 73852

in the «Russian Post» catalog

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

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

Publisher: OOO « South Ural Legal Newsletter»

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

Electronic version of the magazine in the Internet:

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

16+

В НОМЕРЕ

РАДИОТЕХНИКА, В ТОМ ЧИСЛЕ СИСТЕМЫ И УСТРОЙСТВА ТЕЛЕВИДЕНИЯ

СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ И ОБРАБОТКА ИНФОРМАЦИИ

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

IN THIS ISSUE

RADIO ENGINEERING, INCLUDING TELEVISION SYSTEMS AND DEVICES

SYSTEM ANALYSIS, MANAGEMENT AND INFORMATION PROCESSING

METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

УДК 621.372.543.2

Вестник УрФО № 1(47) / 2023, с. 5–14

Фомин Д.Г., Даровских С.Н.

DOI: 10.14529/secur230101

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ МНОГОСЛОЙНОГО ПОЛОСКОВО-ЩЕЛЕВОГО ПЕРЕХОДА ЧАСТОТНО-СЕЛЕКТИВНЫХ СВЧ УСТРОЙСТВ СКРЫТНЫХ РАДИОТЕХНИЧЕСКИХ СИСТЕМ

В работе представлена математическая модель многослойного полосково-щелевого перехода. Он являющегося базовым конструктивным элементом сверхширокополосных полосно-пропускающих фильтров, предназначенных для использования в скрытных радиотехнических системах. Такие системы обеспечивают защиту передаваемой информации за счет использования сигналов с малой спектральной плотностью мощности. При этом особое внимание уделено исследованиям: 1) резонансных частот; 2) частот и амплитуд экстремумов функции коэффициента отражения; 3) частот и амплитуд экстремумов функции коэффициента передачи. В основу математической модели многослойного полосково-щелевого перехода положен матричный метод представления его эквивалентной схемы. Результаты ее математического моделирования показали высокую степень сходимости с результатами схемотехнического моделирования многослойного полосково-щелевого перехода. Все исследования выполнены при использовании программного продукта MATLAB. Предложенная математическая модель позволяет проводить предварительный анализ амплитудно-частотных характеристик многослойного полосково-щелевого перехода без применения специализированных программ электродинамического и схемотехнического моделирования.

Ключевые слова: *многослойный полосково-щелевой переход, математическая модель, S-параметры, скрытность радиотехнических систем.*

MATHEMATICAL MODEL OF A MULTILAYER STRIP-SLOT TRANSITION OF FREQUENCY-SELECTIVE MICROWAVE DEVICES OF SECRECY RADIO ENGINEERING SYSTEMS

The paper presents a mathematical model of a multilayer strip-slot transition. It is the basic structural element of ultra-wideband band-pass filters that designed for application in secrecy radio engineering systems. Such systems ensure the protection of transmitted information by using signals with a low power spectral density. At the same time, special attention is paid to studies of: 1) resonant frequencies; 2) frequencies and amplitudes of extremes of the reflection coefficient function; 3) frequencies and amplitudes of extremes of the transmission coefficient function. The mathematical model of the multilayer strip-slot transition is based on a matrix method for representing its equivalent circuit. The results of its mathematical simulation showed a high degree of convergence with the results of circuit simulation of the multilayer strip-slot transition. All studies were performed using MATLAB software product. The proposed mathematical model allows a preliminary analysis of the amplitude-frequency characteristics of the multilayer strip-slot transition without the use of specialized programs for electrodynamics and circuit simulation.

Keywords: *multilayer strip-slot transition, mathematical model, S-parameters, secrecy of radio engineering systems.*

Введение. Скрытность радиотехнических систем является одной из основных их характеристик и обеспечивает противодействие обнаружению излучаемых сигнальных параметров средствами радиомониторинга. Это лежит в основе защиты передаваемой информации потребителю. В настоящее время известно несколько способов повышения скрытности радиотехнических систем. Одним из них является энергетический способ. Он заключается в использовании сверхширокополосных сигналов со спектральной плотностью мощности, не превышающей 10^{-2} мВт/МГц. Их использование затрудняет их обнаружение и распознавание средствами радиомониторинга [1]. Таким образом, в рамках решения задачи обеспечения скрытности радиотехнических систем, актуальной является задача разработки радиотехнических средств, обеспечивающих генерирование, прием, обработку и фильтрацию сверхширокополосных (СШП) сигналов с шириной спектра более 500 МГц (или более 50 % от значения центральной частоты).

Одним из этапов разработки антенно-фидерного тракта современных радиотехнических систем, использующих СШП сигналы, является проектирование частотно-селективных СВЧ устройств, которые выполняют фильтрацию полезного сигнала и ограничивают прием/передачу внеполосного спектра радиоизлучения [2–6]. Перспективным направлением реализации СШП частотно-селективных СВЧ устройств является объемно-модульная технология [7–14] их построения базовым конструктивным элементом которой является многослойный полосково-щелевой переход, обеспечивающий электро-

магнитную связь между слоями. В настоящее время для исследования амплитудно-частотных характеристик многослойного полосково-щелевого перехода целесообразно использование матричной математической модели, основанной на применении схемотехнических аналогий элементов его конструкции. Целью настоящей работы является обоснование применимости матричной математической модели многослойного полосково-щелевого перехода и его исследование с целью определения: 1) резонансных частот; 2) частот и амплитуд экстремумов функции коэффициента отражения; 3) частот и амплитуд экстремумов функции коэффициента передачи.

1. Многослойный полосково-щелевой переход

Многослойный полосково-щелевой переход [9–14] представляет собой пассивное двухпортовое СВЧ устройство, реализованное на двух диэлектрических основаниях, разделенных металлическим экраном (рис. 1). При этом на каждом диэлектрическом основании расположена полосковая линия, заканчивающаяся обрывом. Конструктивным элементом, обеспечивающим частотно-селективную СВЧ связь между полосковыми линиями является щелевой резонатор, расположенный в металлическом экране. Проекция щелевого резонатора пересекается с полосковыми линиями. Участок каждой полосковой линии от её места пересечения с проекцией щелевого резонатора и до места обрыва образует собой полосковый резонатор. С целью обеспечения наилучшего согласования многослойного полосково-щелевого перехода с антенно-фидерным трактом (волновое сопротивление 50 Ом) электрическая длина полосковых резонаторов θ_1 составляет четверть длины волны на центральной частоте, электрическая длина щелевого резонатора – половину длины волны на центральной частоте ($2\theta_2$). Эквивалентная схема многослойного полосково-щелевого перехода представляет собой каскадное соединение четырехполюсников с заданными матрицами А-параметров (рис. 2). Результаты моделирования эквивалентной схемы при различных значениях волновых сопротивлений полоскового и щелевого резонаторов приведены на рис. 3. Они отражают широкополосные свойства многослойного полосково-щелевого перехода. Исследования выполнены с использованием суперкомпьютерных ресурсов НИУ ЮУрГУ [15].

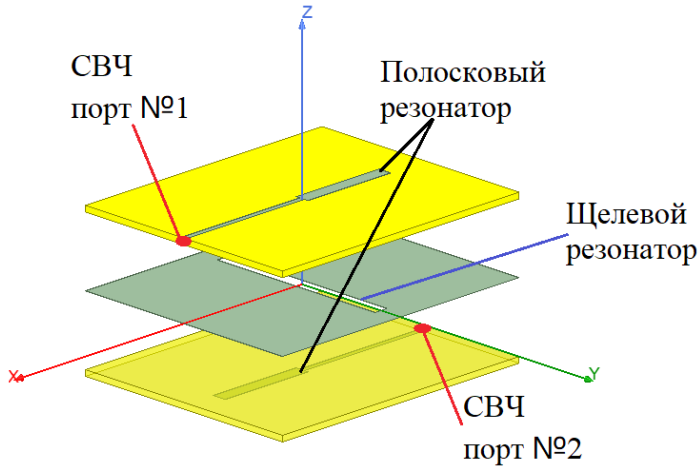


Рис. 1. Многослойный полосково-щелевой переход

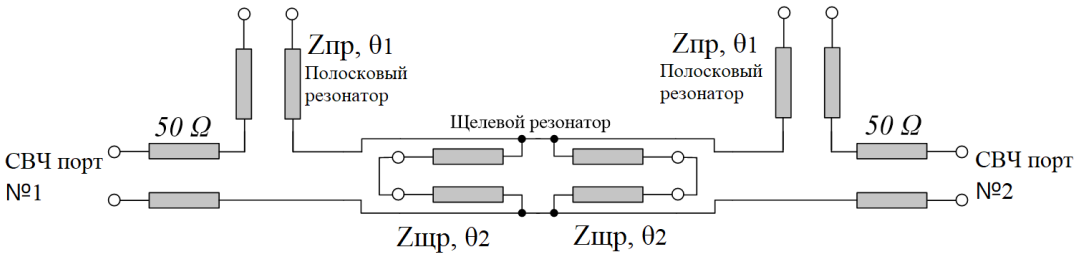
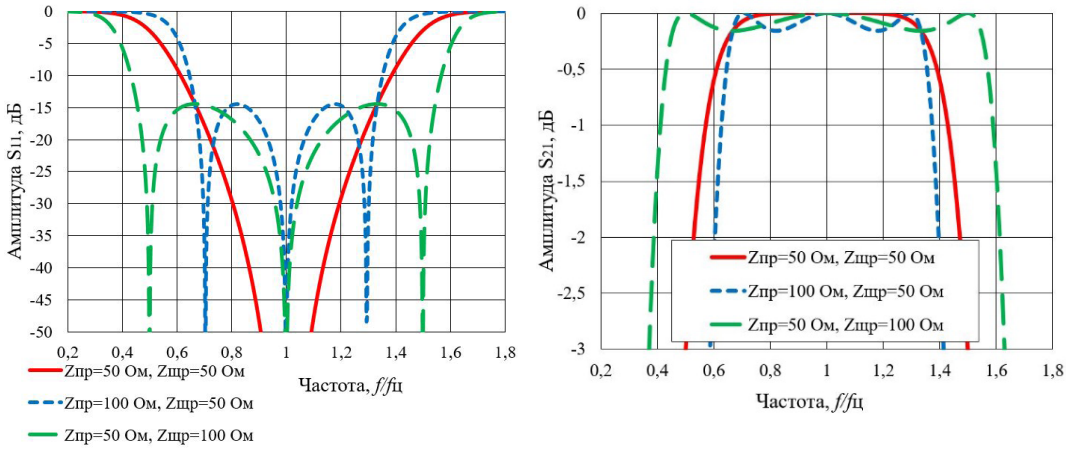


Рис. 2. Эквивалентная схема многослойного полосково-щелевого перехода



а) б)

Рис. 3. Зависимости: а) коэффициента отражения (S_{11}); б) коэффициента передачи (S_{21}) в диапазоне частот, полученные при моделировании эквивалентной схемы

2. Математическая модель многослойного полосково-щелевого перехода

2.1 Резонансные частоты

Рассмотрим матричную математическую модель многослойного полосково-щелевого перехода приняв во внимание, что электрическая длина полосковых (θ_1) и щелевого ($2\theta_2$) резонаторов пропорциональна четверти длины волны. Введем обозначение электрической длины θ, где $\theta = \theta_1 = \theta_2 = \pi/2$. Также выполним нормировку волновых сопротивлений полосковых $z_{НПР}$ и щелевого $z_{НЩР}$ резонаторов относительно волнового сопротивления 50 Ом. В таком случае результирующая матрица А-параметров многослойного полосково-щелевого перехода определяется согласно выражению (1):

$$[A_\Sigma]=\begin{bmatrix} 1-\frac{2z_{НПР}}{z_{НЩР}}ctg^2\theta & \frac{2z_{НПР}}{j}ctg\theta-\frac{2z_{НПР}{}^2}{jz_{НЩР}}ctg^3\theta \\ \frac{2}{jz_{НЩР}}ctg\theta & 1-\frac{2z_{НПР}}{z_{НЩР}}ctg^2\theta \end{bmatrix} \quad (1)$$

Выполним преобразование результирующей матрицы А-параметров в элементы матрицы рассеяния – коэффициенты отражения (S_{11}) и передачи (S_{21}) (2, 3).

$$S_{11}=\frac{A+B-C-D}{A+B+C+D}. \quad (2)$$

$$S_{21}=\frac{2}{A+B+C+D}. \quad (3)$$

Из анализа результирующей матрицы А-параметров (1) следует равенство коэффициентов A и D. Исходя из этого равенства выражение для коэффициента отражения (S_{11}) примет вид (4):

$$S_{11}=\frac{B-C}{A+B+C+D}. \quad (4)$$

Далее запишем закон сохранения энергии для пассивного двухпортового СВЧ устройства (5):

$$|S_{11}|^2+|S_{21}|^2=1. \quad (5)$$

Используя выражения (3, 4) выразим коэффициент отражения (S_{11}) через коэффициент передачи (S_{21}) (6) и подставим в закон сохранения энергии для пассивного двухпортового СВЧ устройства (7):

$$S_{11}=S_{21}\frac{B-C}{2}. \quad (6)$$

$$|S_{21}|^2\left|\frac{B-C}{2}\right|^2+|S_{21}|^2=1. \quad (7)$$

Из выражения (7) следует, что коэффициенты отражения (S_{11}) и передачи (S_{21}) могут быть выражены через коэффициенты B и C согласно выражениям (8, 9):

$$|S_{11}|^2=\frac{\left|\frac{B-C}{2}\right|^2}{1+\left|\frac{B-C}{2}\right|^2}. \quad (8)$$

$$|S_{21}|^2=\frac{1}{1+\left|\frac{B-C}{2}\right|^2}. \quad (9)$$

Из выражения (8) следует, что резонансные частоты функции коэффициента отражения (S_{11}) могут быть определены при условии:

$$\frac{B-C}{2}=0. \quad (10)$$

Подставим коэффициенты B и C результирующей матрицы А-параметров в выражение (10). Получаем выражение (11):

$$\frac{z_{НПР}}{j}ctg\theta-\frac{z_{НПР}{}^2}{jz_{НЩР}}ctg^3\theta-\frac{ctg\theta}{jz_{НЩР}}=0. \quad (11)$$

Из выражения (11) следует, что резонанс-

ные частоты функции коэффициента отражения (S_{11}) определяются согласно выражениям (12, 13):

$$ctg\theta = 0. \quad (12)$$

$$ctg\theta = \pm\frac{\sqrt{z_{НПР}z_{НЩР}-1}}{z_{НПР}}. \quad (13)$$

Из выражения (13) выразим θ (14, 15):

Для случая $ctg\theta \geq 0$ выражение для электрической длины θ примет вид:

$$\theta = arcctg\frac{\sqrt{z_{НПР}z_{НЩР}-1}}{z_{НПР}} + \pi k, \quad (14)$$

$k \in Z$, $k \geq 0$, $z_{НПР}z_{НЩР} \geq 1$, $z_{НПР} > 0$, $z_{НЩР} > 0$.

Для случая $ctg\theta < 0$:

$$\theta = \pi - arcctg\frac{\sqrt{z_{НПР}z_{НЩР}-1}}{z_{НПР}} + \pi k, \quad (15)$$

$k \in Z$, $k \geq 0$, $z_{НПР}z_{НЩР} \geq 1$, $z_{НПР} > 0$, $z_{НЩР} > 0$.

Из выражения (12) следует, что один резонанс функции коэффициента отражения (S_{11}) многослойного полосково-щелевого перехода будет на центральной частоте ($\theta = \pi/2$). Еще два резонанса функции коэффициента отражения (S_{11}) многослойного полосково-щелевого перехода определяются согласно выражениям (14, 15) и образуются при выполнении условий: $z_{НПР}z_{НЩР} \geq 1$, $z_{НПР} > 0$, $z_{НЩР} > 0$. Таким образом, в функции коэффициента отражения (S_{11}) многослойного полосково-щелевого перехода может наблюдаться до трех резонансов, положение которых определяется соотношением волновых сопротивлений полосковых и щелевого резонаторов. Аналогичные закономерности применимы к коэффициенту передачи (S_{21}), где резонансные частоты соответствуют значениям 0 дБ.

2.2 Экстремумы функций коэффициента отражения и коэффициента передачи

Дальнейшее исследование математической модели многослойного полосково-щелевого перехода связано с определением экстремумов функций коэффициента отражения (S_{11}) и коэффициента передачи (S_{21}). Введем функцию $\varphi(\theta) = (B-C)/2$. Тогда согласно выражению (1) функция $\varphi(\theta)$ может быть записана в следующем виде:

$$\varphi(\theta) = \frac{z_{НПР}}{j}ctg\theta - \frac{z_{НПР}^2}{jz_{НЩР}}ctg^3\theta - \frac{ctg\theta}{jz_{НЩР}}. \quad (16)$$

Аналогичным образом перезапишем выражение (8) для коэффициента отражения (S_{11}) (17):

$$|S_{11}|^2 = \frac{|\varphi(\theta)|^2}{1+|\varphi(\theta)|^2}. \quad (17)$$

Для определения экстремумов функции коэффициента отражения (S_{11}) приравняем его первую производную к нулю (18):

$$\frac{\partial|S_{11}(\theta)|}{\partial\theta} = \frac{\partial|\varphi(\theta)|}{\partial\theta}\cdot\frac{1}{(1+|\varphi(\theta)|^2)^{\frac{3}{2}}}. \quad (18)$$

Из выражения (18) следует, что $\partial S_{11}(\theta)/\partial\theta = 0$ при $\partial\varphi(\theta)/\partial\theta = 0$. Таким образом, для определения частот, соответствующих экстремумам функции коэффициента отражения (S_{11}) найдем нули первой производной функции $\varphi(\theta)$ (выражения 19-21):

$$\frac{\partial\varphi(\theta)}{\partial\theta} = -j\left(-\frac{z_{НПР}}{sin^2\theta} + 3\frac{z_{НПР}^2}{z_{НЩР}sin^2\theta}ctg^2\theta + \frac{1}{z_{НЩР}sin^2\theta}\right) = 0. \quad (19)$$

$$\left(-z_{НПР} + 3\frac{z_{НПР}^2}{z_{НЩР}}ctg^2\theta + \frac{1}{z_{НЩР}}\right) = 0. \quad (20)$$

$$ctg\theta = \pm\frac{1}{z_{НПР}}\sqrt{\frac{z_{НПР}z_{НЩР}-1}{3}}. \quad (21)$$

Из выражения (21) выразим θ (выражения 22, 23):

Для случая $ctg\theta \geq 0$:

$$\theta = arcctg\left(\frac{1}{z_{НПР}}\sqrt{\frac{z_{НПР}z_{НЩР}-1}{3}}\right) + \pi k, \quad (22)$$

$k \in Z$, $k \geq 0$, $z_{НПР}z_{НЩР} \geq 1$, $z_{НПР} > 0$, $z_{НЩР} > 0$.

Для случая $ctg\theta < 0$:

$$\theta = \pi - arcctg\left(\frac{1}{z_{НПР}}\sqrt{\frac{z_{НПР}z_{НЩР}-1}{3}}\right) + \pi k, \quad (23)$$

$k \in Z$, $k \geq 0$, $z_{НПР}z_{НЩР} > 1$, $z_{НПР} > 0$, $z_{НЩР} > 0$.

Таким образом, в функциях коэффициентов отражения (S_{11}) и передачи (S_{21}) многослойного полосково-щелевого перехода может наблюдаться до двух экстремумов, положение которых определяется соотношением волновых сопротивлений полосковых и щелевого резонаторов.

3. Результаты исследования математической модели

3.1 Расчет резонансных частот

Проведем расчет резонансных частот многослойного полосково-щелевого перехода (таблица 1). Полученные результаты сравним с результатами схемотехнического моделирования эквивалентной схемы (рис. 4, 5). При проведении расчетов будем использовать следующие комбинации значений волновых сопротивлений полосковых и щелевого резонаторов многослойного полосково-щелевого перехода: 1) $z_{ПР} = 25$ Ом, $z_{ЩР} = 25$ Ом; 2) $z_{ПР} = 50$ Ом, $z_{ЩР} = 50$ Ом; 3) $z_{ПР} = 100$ Ом, $z_{ЩР} = 50$ Ом; 4) $z_{ПР} = 50$ Ом, $z_{ЩР} = 100$ Ом; 5) $z_{ПР} = 75$ Ом, $z_{ЩР} = 75$ Ом.

Таблица 1

Резонансные частоты многослойного полосково-щелевого перехода

	$f_1/f_Ц$	$f_2/f_Ц$	$f_3/f_Ц$
$z_{ПР}$ = 25 Ом, $z_{ЩР}$ = 25 Ом	-	1	-
$z_{ПР}$ = 50 Ом, $z_{ЩР}$ = 50 Ом	-	1	-
$z_{ПР}$ = 100 Ом, $z_{ЩР}$ = 50 Ом	0,705	1	1,295
$z_{ПР}$ = 50 Ом, $z_{ЩР}$ = 100 Ом	0,50	1	1,50
$z_{ПР}$ = 75 Ом, $z_{ЩР}$ = 75 Ом	0,59	1	1,41

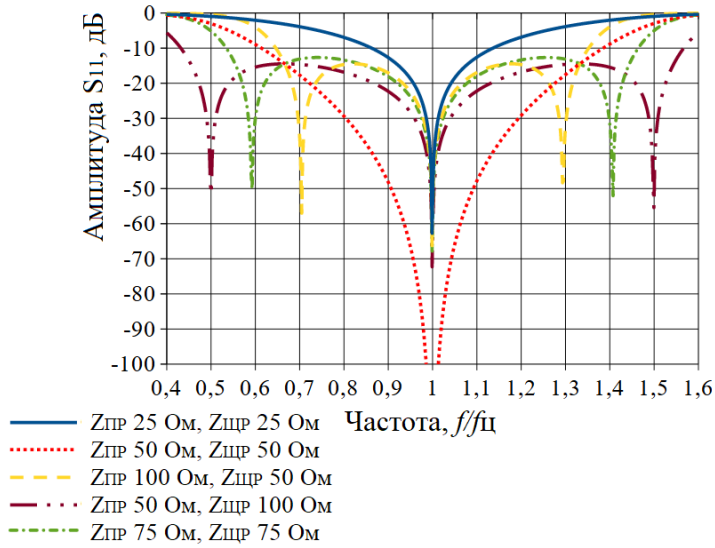


Рис. 4. Зависимости коэффициента отражения (S_{11}) от частоты, полученные по результатам схемотехнического моделирования

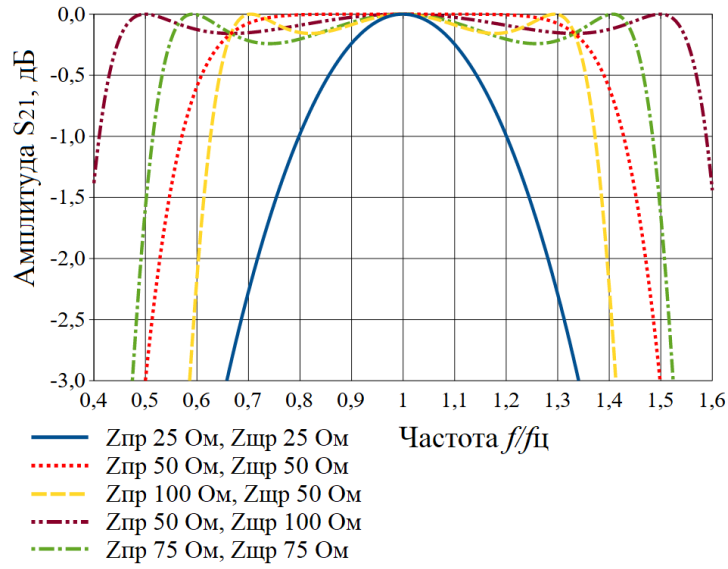


Рис. 5. Зависимости коэффициента передачи (S_{21}) от частоты, полученные по результатам схемотехнического моделирования

3.2 Расчет экстремумов функции коэффициента отражения

Аналогичным образом выполним расчет нормированных частот и амплитуд экстремумов функций коэффициентов отражения (S_{11}) и передачи (S_{21}). Результаты расчетов приведены в таблицах 2, 3. Полученные результаты сравним с результатами схемотехнического

моделирования эквивалентной схемы (Рис. 6, 7). При проведении расчетов будем использовать следующие комбинации значений волновых сопротивлений полосковых и щелевого резонаторов многослойного полосково-щелевого перехода: 1) $z_{ПР}$ = 100 Ом, $z_{ЩР}$ = = 50 Ом; 2) $z_{ПР}$ = 50 Ом, $z_{ЩР}$ = 100 Ом; 3) $z_{ПР}$ = 75 Ом, $z_{ЩР}$ = 75 Ом.

Таблица 2

Частоты и значения экстремумов функции коэффициента отражения (S_{11})

	$f_1/f_Ц$, $\|S_{11}\|$	$f_2/f_Ц$, $\|S_{11}\|$
$z_{ПР}$ = 100 Ом, $z_{ЩР}$ = 50 Ом	0,82; -14,47 дБ	1,18; -14,47 дБ
$z_{ПР}$ = 50 Ом, $z_{ЩР}$ = 100 Ом	0,67; -14,47 дБ	1,33; -14,47 дБ
$z_{ПР}$ = 75 Ом, $z_{ЩР}$ = 75 Ом	0,74; -12,67 дБ	1,25; -12,67 дБ

Таблица 3

Частоты и значения экстремумов функции коэффициента передачи (S_{21})

	f1/fЦ,|S21|	f2/fЦ,|S21|
$z_{ПР}$ = 100 Ом, $z_{ЩР}$ = 50 Ом	0,82; -0,157 дБ	1,18; -0,157 дБ
$z_{ПР}$ = 50 Ом, $z_{ЩР}$ = 100 Ом	0,67; -0,157 дБ	1,33; -0,157 дБ
$z_{ПР}$ = 75 Ом, $z_{ЩР}$ = 75 Ом	0,74; -0,24 дБ	1,25; -0,24 дБ

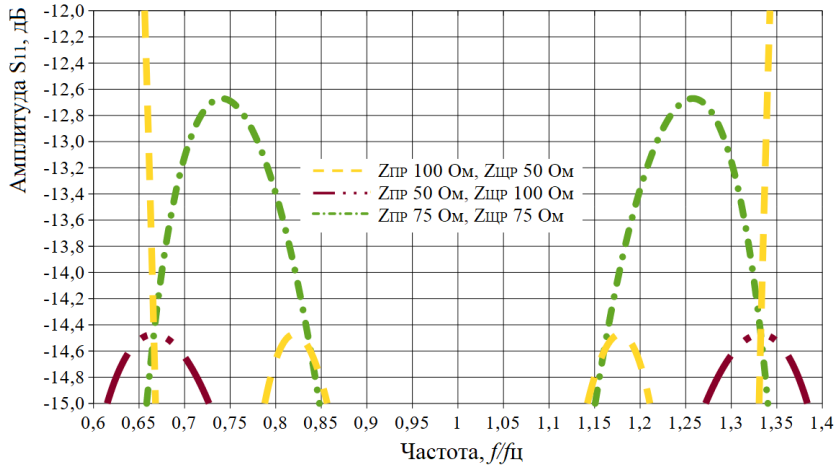


Рис. 6. Зависимости коэффициента отражения (S_{11}) от частоты, полученные по результатам схемотехнического моделирования

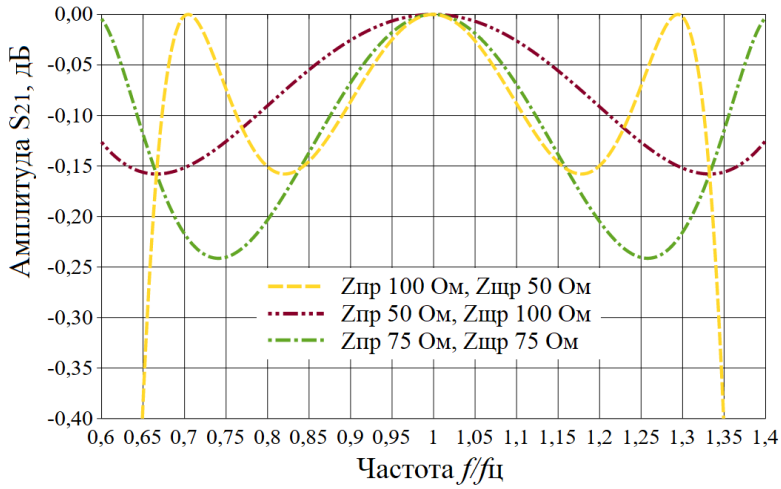


Рис. 7. Зависимости коэффициента передачи (S21) от частоты, полученные по результатам схемотехнического моделирования

4. Обсуждение результатов проведенных исследований

Из представленных табличных данных (Таблица 1) и графических зависимостей (Рис. 4, 5) следует, что резонансные частоты многослойного полосково-щелевого перехода, полученные по результатам схемотехнического моделирования совпадают с расчетными данными, полученными согласно выражениям (12-15). При этом установлено, положение резонансов определяется соотношением волновых сопротивлений полоскового и щелевого резонаторов. Из представленных табличных данных (Таблица 2, 3) и графических зависимостей (Рис. 6, 7) следует, что значения частот и амплитуд экстремумов функций коэффициентов отражения (S_{11}) и передачи (S_{21}), полученных по результатам схемотехнического моделирования совпадают с расчетными данными, полученными согласно выражениям (21-23). При этом установлено, что при постоянном соотношении $z_{ПР}z_{ЩР} = const$, величина экстремумов функций коэффициентов отражения (S_{11}) и передачи (S_{21}) остается постоянной. Таким образом, согласно полученным математическим выражениям (12-15, 21-23) можно проводить предварительный анализ следующих параметров амплитудно-частотной характеристики многослойного полосково-щелевого перехода: резонансных частот; частот и амплитуд экстремумов функции коэффициента отражения (S_{11}); частот и амплитуд экстремумов функции коэффициента передачи (S_{21}).

Заключение

В работе представлена математическая модель многослойного полосково-щелевого перехода и результаты ее исследования. Результатами исследования являются математические выражения, позволяющие проводить предварительный анализ амплитудно-частотной характеристики многослойного полосково-щелевого перехода. При этом анализу подлежат следующие параметры амплитудно-частотной характеристики: резонансные частоты; частоты и амплитуды экстремумов функции коэффициента отражения (S_{11}); частоты и амплитуды экстремумов функции коэффициента передачи (S_{21}). При проведении указанного анализа не требуется использование специализированных программных продуктов электродинамического и схемотехнического моделирований.

Литература

1. Разиньков С.Н. Основные направления развития и базовые технологии создания систем радиосвязи со сверхширокополосными сигналами. Воздушно-космические силы. Теория и практика, 2019, № 11, С. 38 – 44.

2. Таблица распределения полос радиочастот между радиослужбами Российской Федерации (статистические данные). URL: https://digital.gov.ru/opendata/7710474375-trpch/table/ (дата обращения: 26.12.2022).

3. Wang, Y. X. Dual-Band Bandpass Filter Design Using Stub-Loaded Hairpin Resonator and Meandering Uniform Impedance Resonator / Y.X. Wang, Y.L. Chen, W.H. Zhou, W.Ch. Yang, J. Zen // Progress In Electromagnetics Research Letters. – 2021. – Vol. 95. – P. 147–153.

4. Wang, Z. A compact negative-group-delay microstrip bandpass filter / Z. Wang, Z. Fu, C. Li, S. Fang, H. Liu // Progress In Electromagnetics Research Letters. – 2020. – Vol. 90. – P. 45–51.

5. Li-Tian Wang, Yang Xiong, Ming He. Review on UWB Bandpass Filters. In book: UWB Technology – Circuits and Systems. London, IntechOpen. 2019. URL: http://doi.org/10.5772/intechopen.87204 (дата обращения: 26.12.2022).

6. Pozar, D.M. Microwave Engineering. 4th ed. Hoboken, NJ:J. Wiley; 2011. – 736 p.

7. Dudarev, N.V. The Volume-Modular Technology in the Design of Passive Microwave Devices / N.V. Dudarev, D.G. Fomin, S.N. Darovskikh, D.S. Klygach, M.G. Vakhitov // Proceedings - 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology, USBEREIT 2021. – 2021. – P. 225–227.

8. Особенности применения объемно-модульной технологии в проектировании СВЧ электронных устройств / Д. Г. Фомин, Н. В. Дударев, С. Н. Даровских, Д.С. Клыгач, М. Г. Вахитов // Ural Radio Engineering Journal. 2021;5(2):91–103. — DOI: 10.15826/urej.2021.5.2.001.

9. Fomin, D.G. Scattering matrix simulation of the volumetric strip-slot transition and estimation of its frequency properties / D.G. Fomin, N.V. Dudarev, S.N. Darovskikh // Journal of Physics: Conference Series. – 2020 – Vol. 1679(2). – P. 1–6. DOI 10.1088/1742-6596/1679/2/022032

10. Tao, Z. Broadband microstrip-to-microstrip vertical transition design / Z. Tao, J. Zhu, T. Zuo, L. Pan, Y. Yu // IEEE Microwave and Wireless Components Letters. – 2016. – Vol. 26. – P. 660–662.

11. Yang, L. Analysis and design of wideband microstrip-to-microstrip equal ripple vertical transitions and their application to bandpass filters / L. Yang, L. Zhu, W.-W. Choi, K.-W. Tam // IEEE Transactions on Microwave Theory and Techniques. – 2017. – Vol. 65(8). – P. 2866–2877.

12. Abbosh, A.M. Ultra wideband vertical microstrip-microstrip transition. IET Microwaves, Antennas & Propagation. – 2007. – Vol. 1(5). – P. 968 – 972.

13. Фомин, Д.Г. Экспериментальное исследование полосно-пропускающих фильтров на основе многослойной технологии / С.Н. Даровских, Д.Г. Фомин, Н.В. Дударев, Д.С. Клыгач, М.Г. Вахитов // Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника. – 2022. – Т. 22. – № 4. – С. 48–55. DOI: http://dx.doi.org/10.14529/ctcr220405

14. Фомин, Д.Г. Моделирование полосно-пропускающих фильтров на основе многослойной технологии / Д.Г. Фомин, С.Н. Даровских, Н.В. Дударев, И.И. Прокопов, С.В. Дударев // Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника. – 2022. – Т. 22. – № 1. – С. 77–87. DOI: http://dx.doi.org/10.14529/ctcr220106

15. Биленко Р. В., Долганина Н.Ю., Иванова Е. В., Рекачинский А. И. Высокопроизводительные вычислительные ресурсы Южно-Уральского государственного университета // Вестник ЮУрГУ. Серия: Вычислительная математика и информатика. 2022. Т. 11, № 1. – С. 15–30. DOI: 10.14529/cmse220102.

References

1. Razin'kov S.N. Osnovnyye napravleniya razvitiya i bazovyye tekhnologii sozdaniya sistem radiosvyazi so sverkhshirokopolosnymi signalami. Vozdushno-kosmicheskiye sily. Teoriya i praktika, 2019, № 11, S. 38 – 44.

2. Tablitsa raspredeleniya polos radiochastot mezhdu radiosluzhbami Rossiyskoy Federatsii (statisticheskiye dannyye). URL: https://digital.gov.ru/opendata/7710474375-trpch/table/ (data obrashcheniya: 26.12.2022).

3. Wang, Y. X. Dual-Band Bandpass Filter Design Using Stub-Loaded Hairpin Resonator and Meandering Uniform Impedance Resonator / Y.X. Wang, Y.L. Chen, W.H. Zhou, W.Ch. Yang, J. Zen // Progress In Electromagnetics Research Letters. – 2021. – Vol. 95. – P. 147–153.

4. Wang, Z. A compact negative-group-delay microstrip bandpass filter / Z. Wang, Z. Fu, C. Li, S. Fang, H. Liu // Progress In Electromagnetics Research Letters. – 2020. – Vol. 90. – P. 45–51.

5. Li-Tian Wang, Yang Xiong, Ming He. Review on UWB Bandpass Filters. In book: UWB Technology – Circuits and Systems. London, IntechOpen. 2019. URL: http://doi.org/10.5772/intechopen.87204 (дата обращения: 26.12.2022).

6. Pozar, D.M. Microwave Engineering. 4th ed. Hoboken, NJ:J. Wiley; 2011. – 736 p.

7. Dudarev, N.V. The Volume-Modular Technology in the Design of Passive Microwave Devices / N.V. Dudarev, D.G. Fomin, S.N. Darovskikh, D.S. Klygach, M.G. Vakhitov // Proceedings - 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology, USBEREIT 2021. – 2021. – P. 225–227.

8. Osobennosti primeneniya ob"yemno-modul'noy tekhnologii v proyektirovanii SVCH elektronnykh ustroystv / D. G. Fomin, N. V. Dudarev, S. N. Darovskikh, D.S. Klygach, M. G. Vakhitov // Ural Radio Engineering Journal. 2021;5(2):91–103. — DOI: 10.15826/urej.2021.5.2.001.

9. Fomin, D.G. Scattering matrix simulation of the volumetric strip-slot transition and estimation of its frequency properties / D.G. Fomin, N.V. Dudarev, S.N. Darovskikh // Journal of Physics: Conference Series. – 2020 – Vol. 1679(2). – P. 1– 6. DOI 10.1088/1742-6596/1679/2/022032

10. Tao, Z. Broadband microstrip-to-microstrip vertical transition design / Z. Tao, J. Zhu, T. Zuo, L. Pan, Y. Yu // IEEE Microwave and Wireless Components Letters. – 2016. – Vol. 26. – P. 660–662.

11. Yang, L. Analysis and design of wideband microstrip-to-microstrip equal ripple vertical transitions and their application to bandpass filters / L. Yang, L. Zhu, W.-W. Choi, K.-W. Tam // IEEE Transactions on Microwave Theory and Techniques. – 2017. – Vol. 65(8). – P. 2866–2877.

12. Abbosh, A.M. Ultra wideband vertical microstrip-microstrip transition. IET Microwaves, Antennas & Propagation. – 2007. – Vol. 1(5). – P. 968 – 972.

13. Fomin, D.G. Eksperimental'noye issledovaniye polosno-propuskayushchikh fil'trov na osnove mnogosloynoy tekhnologii / S.N. Darovskikh, D.G. Fomin, N.V. Dudarev, D.S. Klygach, M.G. Vakhitov // Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta. Seriya: Komp'yuternyye tekhnologii, upravleniye, radioelektronika. – 2022. – T. 22. – № 4. – S. 48–55. DOI: http://dx.doi.org/10.14529/ctcr220405.

14. Fomin, D.G. Modelirovaniye polosno-propuskayushchikh fil'trov na osnove mnogosloynoy tekhnologii / D.G. Fomin, S.N. Darovskikh, N.V. Dudarev, I.I. Prokopov, S.V. Dudarev // Vestnik Yuzhno-

Ural'skogo gosudarstvennogo universiteta. Seriya: Komp'yuternyye tekhnologii, upravleniye, radioelektronika. – 2022. – T. 22. – № 1. – S. 77–87. DOI: http://dx.doi.org/10.14529/ctcr220106.

15. Bilenko R. V., Dolganina N.YU., Ivanova Ye. V., Rekachinskiy A. I. Vysokoproizvoditel'nyye vychislitel'nyye resursy Yuzhno-Ural'skogo gosudarstvennogo universiteta // Vestnik YUUrGU. Seriya: Vychislitel'naya matematika i informatika. 2022. T. 11, № 1. – S. 15–30. DOI: 10.14529/cmse220102.

ФОМИН Дмитрий Геннадьевич, аспирант кафедры инфокоммуникационных технологий, ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, пр. Ленина, д. 76. E-mail: Fomin95@ya.ru

ДАРОВСКИХ Станислав Никифорович, доктор технических наук, доцент, профессор кафедры инфокоммуникационных технологий, ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, пр. Ленина, д. 76. E-mail: darovskikhsn@susu.ru

FOMIN Dmitry Gennadievich, PhD student of Department of Information and Communication Technologies, South Ural State University (national research university). Russia, 454080, Chelyabinsk, Lenin Ave., 76. E-mail: Fomin95@ya.ru

DAROVSKIKH Stanislav Nikiforovich, Dr. Sci. (Eng.), Ass. Prof., Prof. of the Department of Information and Communication Technologies, South Ural State University (national research university). Russia, 454080, Chelyabinsk, Lenin Ave., 76. E-mail: darovskikhsn@susu.ru

УДК 004.771 + 004.75 Вестник УрФО № 1(47) / 2023, с. 15–26

Баринов А.Е., Морозов И.А., Мельников К.В., Руденко Е.А.

DOI: 10.14529/secur230102

БЕЗАГЕНТСКИЙ АННОТИРУЕМЫЙ СБОР ПОВЕДЕНЧЕСКОЙ ИНФОРМАЦИИ ПОЛЬЗОВАТЕЛЕЙ В КОНТЕЙНЕРНЫХ ИНФРАСТРУКТУРАХ [1]

Широкое внедрение технологий контейнеризации и приложений микросервисной архитектуры несет в себе новые специфичные риски при использовании и обслуживании. Технически и организационно обеспечение информационной безопасности в контейнерных средах сильно отличается от привычных подходов. В статье описывается специфика организации аудита действий системных администраторов при обслуживании контейнерных инфраструктур. Авторами предлагается технология безагентского аннотируемого сбора поведенческой информации на основе перехвата взаимодействия пользователей с псевдотерминалом и журналирования запуска приложений, описываются ее преимущества и связанные с ней ограничения.

Ключевые слова: *контейнеризация, аудит, ввод-вывод информации, системные вызовы, мультитенантность, облачная инфраструктура, технология BPF.*

Barinov A.E., Morozov I.A., Melnikov K. V., Rudenko E.A.

AGENTLESS ANNOTATED MONITORING OF USER BEHAVIORAL INFORMATION IN CONTAINER INFRASTRUCTURES

The widespread adoption of containerization technologies and microservice architecture applications brings new specific risks in use and maintenance. Technically and organizationally, ensuring information security in container environments is very different from the usual approaches. The paper describes specifics of organizing an audit of the actions of system administrators when servicing container infrastructures. The authors propose a technology for agent-

[1] Исследование поддержано грантом Российского научного фонда (проект № 22-71-10095).

less annotated collection of behavioral information based on intercepting user interaction with a pseudo-terminal and logging application launches, describe its advantages and limitations associated with it.

Keywords: *containers, auditing process, input and outputs, multi tenants, system calls, cloud infrastructure, Berkeley packet filters.*

Компании все чаще используют технологии контейнеризации для запуска приложений микросервисной архитектуры. Контейнерные приложения легче в обслуживании, их проще переносить, они запускаются в любой среде, где возможно развернуть контейнерезатор (например, платформа Docker портирована практически на все популярные операционные системы). Однако, технически и организационно обеспечение информационной безопасности в контейнерных средах сильно отличается от привычных подходов. Большое количество новых сущностей в микросервисных архитектурах и совершенно другой подход при доставке ПО создают свою специфику [1]. Одним из направлений информационной безопасности является мониторинг и аудит, и несмотря на кажущуюся простоту (прямой сбор информации, например, журналы событий, или вывод аварийных сообщений в некоторых случаях даже упрощаются по сравнению с традиционными или виртуальными инфраструктурами, например, сбор информации с консоли контейнера через dockerlogs), имеются определенные сложности со сбором информации о поведении пользователя в контейнере. В частности, в [2–3] отмечается, что зрелые средства анализа действий пользователя в контейнерных средах в настоящее время отсутствуют в открытом доступе. С одной стороны, если сервис является простым, и настраивается исключительно через консоль хостинг-провайдера и не предполагает интерактивной настройки, то для него нет необходимости в поведенческом мониторинге, однако если же внутри контейнера осуществляется сложное взаимодействие приложений тенанта, и его системный администратор имеет доступ к консольной настройке через SSH или WebSSH, то вопрос организаций мониторинга его действий должен лежать на стороне провайдера инфраструктуры (например, в целях расследования инцидентов, вызванных некорректной настройкой или злонамеренными действиями).

В настоящее время существующие на рынке IaaS провайдеры активно развивают решения по журналированию и аудиту действий пользователя в облачных инфраструктурах, в частности для централизованного журналирования применяются такие решения, как Yandex Cloud Logging [4], AWS CloudTrail [5], Google Cloud Logging [6], однако такие решения больше ориентированы на централизованный сбор событий об ошибках приложений (журналирование потоков stderr, stdout), обработку журналов операционных систем и приложений; AWS CloudTrail [5] кроме того обеспечивает журналирование доступа пользователей (системных администраторов) к API платформы; Google Cloud Logging [6] обладает широкими возможностями по телеметрии используемых ресурсов и журналированию запуска процессов. Некоторые IaaS провайдеры, такие как AWS и Yandex Cloud предоставляют также дополнительные сервисы по аудиту действий пользователей такие, как Yandex Audit Trails [7] и AWS Config [8]. При этом Yandex Audit Trails [7] в большей мере ориентирован на мониторинг действий пользователей (системных администраторов) к объектам инфраструктуры тенанта на основе обращений к API. AWS Config в свою очередь представляет собой сервис декларативного описания конфигурации требуемой виртуальной инфраструктуры и обеспечивает непрерывный мониторинг и журналирование потенциальных отклонений от требуемого состояния и связанные с этим действия. При этом вышеуказанные сервисы оперируют лишь со столь высокоуровневыми объектами, как API платформы, и в некоторых случаях журналы приложений и служб, лишь Google Cloud Logging [6] обеспечивает журналирование запуска процессов, при этом в случае использования виртуальных машин с несколькими контейнерами не обеспечивает аннотирование журнала запуска процессов к контейнерам. Отметим, что ни один из вышеупомянутых провайдеров не обеспечивает журналирование взаимодействия пользователей с ПО контейнера посредством командной строки.

Некоторый технологический задел по мониторингу действий пользователей в контейнерах создан в сфере виртуальных лабораторных работ для обучения студентов ИТ-

специальностей в том числе и по кибербезопасности. Виртуальные лаборатории для организации практических занятий по кибербезопасности в последнее время стали очень популярными во всем мире [9–10]. Более того их можно использовать, как при очном обучении (зачастую минуя приобретение дорогостоящего оборудования и обеспечивая масштабируемость на множество обучающихся), так и в обучении с применением дистанционных образовательных технологий. В большинстве случаев проверка корректности выполнения виртуальной лабораторной работы учащимся выполняется посредством тестовых заданий, реже исполняются специальные проверочные программы, скрипты, которые проверяют работоспособность реализованного учащимся задания. Но остается открытым вопрос как нашли студенты правильный ответ, применяя инструменты (под этим можно подразумевать и защиту от списывания). Решения, которые обеспечивают сбор поведенческой информации, также позволяют улучшить обратную связь со студентами. В частности, в виртуальных лабораторных работах по ИТ-дисциплинах может быть несколько путей к правильному решению, и то, как студенты решают эти задания может существенно обогатить их ответы, что, в конечном счете, может быть полезно при оценке [11].

Представленные в открытых источниках способы сбора в основном базируются на двух подходах [12]: сбор ввода и вывода информации на пользовательские виртуальные псевдотерминальные устройства и перехват команд в оболочке при их исполнении. Каждый из этих способов имеет существенные ограничения при сборе информации. Сбор ввода и вывода информации на псевдотерминальные устройства [13] используется в большинстве современных решений по сбору поведенческой информации пользователей. В этом решении предлагается использование давно развиваемого скрипта ttylog.pl, который, в конечном счете, перехватывает информацию с псевдотерминала, используя strace (вызовы read,write), и, таким образом, он успешно регистрирует все входные и выходные данные терминала. Однако существенным недостатком является то, что указанный перехватчик устанавливается внутрь каждого контейнера, что не всегда приемлемо по производительности. Кроме того, указанные инструменты запускаются в пространстве пользователя и всегда могут быть им злонамеренно остановлены. Кроме того, данное программное обеспечение написано на интерпретируемом языке Perl, что несет в себе необходимость также установки самого интерпретатора, а в некоторых решениях [14] производится дополнительная обработка (аннотирование) собранной информации также в контейнере, в том числе и с применением других интерпретируемых языков, в частности Python. В конечном счете, все обработчики помещаются в контейнер и там же исполняются. В итоге, объем установленных скриптов, интерпретаторов и модулей составляет порядка 60-100 Мб (для контейнеров, построенных на базе образов различных ОС), при том что контейнер, разработанный авторами статьи для изучения работы почтового сервера postfix на базе ОС alpine имеет размер всего 33 Мб. При том, что для некоторых инфраструктур требуется запуск более одного контейнера, а количество тенантов в системе может достигать сотен. В итоге для скачивания и дальнейшего анализа посредством инструментов среды контейнеризации скачивается файл, содержащий аннотированные команды.

В решении [15] представлен более легковесный подход, обеспечивающий перехват действий пользователя, основывающийся на переопределении параметра $PS0 действий пользователя (команда, исполняющаяся перед исполнением основной команды), однако он также определяется в пространстве пользователя и может быть злонамеренно отключен им. В дальнейшем информация помещается в системный журнал и отправляется для анализа с помощью демона rsyslogd. К недостаткам этого решения можно отнести то, что сбор информации таким образом можно производить лишь с ограниченного числа командных оболочек, например, bash и его модификации. Более легковесные решения, такие как ash не обладают таким функционалом. Отметим также, что интерпретация параметра $PS0 осуществляется перед исполнением команды, а, следовательно, перехват и анализ вывода команды в этом случае не возможен. Кроме того, при запуске пользователем в рамках сессии альтернативных оболочек, например, ipython и т.д., перехват сессии не осуществляется. При этом авторы решения [15] разработали альтернативные подходы (коннекторы) для специализированных оболочек, например, metasploit, PowerShell и

т.д. Однако на наш взгляд представляется затруднительным разработка таких модулей для всех существующих пользовательских оболочек.

К недостаткам обоих подходов можно отнести – модификацию образа при запуске контейнера, возможность остановки сбора поведенческой информации пользователем. Хотя возможно осуществить запуск и от стороннего пользователя, предоставив соответствующие права, однако для специфической настройки ПО в контейнере зачастую требуются права администратора (суперпользователя). Таким образом, любое из выше рассмотренных средств может быть нелегитимно остановлено. Кроме того, как указано выше, каждый из подходов предполагает избыточную установку стороннего ПО для каждого из контейнеров, что негативно сказывается как на использовании дискового пространства, так и ОЗУ. Кроме того, в [13] отмечается, что подобный сбор информации может пропускать значимые события такие, как запуск сторонних приложений, если они осуществляются пользователем косвенно, например, через сценарий, интерактивную оболочку (например, mc), или из стороннего приложения, для устранения этого недостатка авторы предлагают использовать стороннюю библиотеку [16], основанную на перехвате системного вызова exec на основе технологии LD_PRELOAD (перехват вызовов на основе специализированных библиотек, загружаемых в приоритетном порядке), однако этот подход также имеет ограниченное применение. Во-первых, не все ОС в контейнерах поддерживают эту технологию, например, используемый авторами статьи alpine без существенной дополнительной доработки не обеспечивает работу этой технологии, а кроме того даже в ОС общего назначения, например Ubuntu, если пользователь запустит статически скомпилированную программу этот метод также окажется неработоспособен.

Перед авторами статьи стояла задача обеспечить сбор поведенческой информации пользователей в контейнерной инфраструктуре с минимальным вмешательством в содержание контейнера (или без такового); обеспечить невозможность отключения сбора информации пользователем или изменение собранной информации. При этом помимо сбора информации с терминалов необходимо обеспечить сбор информации о запускаемых процессах.

Для построения исследовательской среды использовалась одна из наиболее популярных Linux-систем Ubuntu 22.04 и система контейнеризации Docker 20.10. Отметим что, двумя основными технологиями контейнеризации являются Docker и LXC. Docker — это легкие автономные исполняемые пакеты, включающие все необходимое для запуска приложений [17]. С одной стороны, LXC обладает большей гибкостью и меньшими накладными ресурсами, поскольку имеет возможность более гибкой настройки сетевых интерфейсов и более простым взаимодействием с ядром хоста, что повышает производительность [18]. Обе технологии обеспечивают изоляцию ресурсов контейнеров посредством механизма контрольных групп (cgroup), реализуемым в ядре Linux. В своей работе мы использовали стек на базе Docker исходя из требований масштабируемости, включая горизонтальную и функциональную. Кроме того, большинство хостинг-провайдеров – AWS, Yandex Cloud, и т.д. также используют технологию Docker в качестве основной. Также в пользу Docker говорит и ее широкое использование для построения комплексов виртуальных лабораторных работ [11].

Для решения рассматриваемой задачи нами было решено использовать технологию Berkley Packet Filter (BPF) [19]. Технология BPF позволяет осуществлять перехват событий ядра ОС, включая осуществление системных вызовов и т.д. В частности, программа strace, упомянутая выше в современных версиях ОС Linux использует эту технологию при отладке процессов и перехвате системных вызовов. Отметим, что для обеспечения работы технологии BPF она должна быть активирована в ядре. Однако для большинства серверных ОС это не является существенным ограничением. В рассматриваемой нами Ubuntu 22.04 все модули, обеспечивающие работу данной технологии активированы в ядре по умолчанию, кроме BPF_PRELOAD. Однако отсутствие этого модуля для рассматриваемой задачи не существенно влияет на функциональность, поскольку он отвечает лишь за предварительную загрузку BPF модулей в ядро ОС и обеспечивает безопасный доступ к ним из пользовательского режима (рис. 1).

Упомянем, что контейнер - это более слабая технология изоляция процессов, чем, например, виртуальные машины, и таким образом все процессы контейнера (в общем случае, без настройки специфичной изоляции со

```
andrey@andrey-virtual-machine:~$ cat /boot/config-5.15.0-46-generic | grep BPF
CONFIG_BPF=y
CONFIG_HAVE_EBPF_JIT=y
CONFIG_ARCH_WANT_DEFAULT_BPF_JIT=y
# BPF subsystem
CONFIG_BPF_SYSCALL=y
CONFIG_BPF_JIT=y
CONFIG_BPF_JIT_ALWAYS_ON=y
CONFIG_BPF_JIT_DEFAULT_ON=y
CONFIG_BPF_UNPRIV_DEFAULT_OFF=y
# CONFIG_BPF_PRELOAD is not set
CONFIG_BPF_LSM=y
# end of BPF subsystem
CONFIG_CGROUP_BPF=y
CONFIG_IPV6_SEG6_BPF=y
CONFIG_NETFILTER_XT_MATCH_BPF=m
CONFIG_BPFILTER=y
CONFIG_BPFILTER_UMH=m
CONFIG_NET_CLS_BPF=m
CONFIG_NET_ACT_BPF=m
CONFIG_BPF_STREAM_PARSER=y
CONFIG_LWTUNNEL_BPF=y
CONFIG_BPF_EVENTS=y
CONFIG_BPF_KPROBE_OVERRIDE=y
CONFIG_TEST_BPF=m
```

Рис. 1. Состав BPF модулей в ОС Ubuntu 22.04

стороны платформы контейнеризации) видны во внешней ОС и доступны для отладки. Таким образом, решение на базе скрипта ttylog.pl на первый взгляд кажется рабочим, однако при активации доступа пользователем к контейнеру через SSH (сетевой протокол прикладного уровня, позволяющий производить удаленное управление операционной системой посредством псевдотерминала) в каждом из контейнеров будет создаваться свой набор псевдотерминалов пользовательских сессий недоступных во внешней ОС, но при этом упоминающийся в аргументах запуска процессов.

Рассмотрим подробнее работу ttylog.pl. Во-первых, этот инструмент на основе регулярных выражений находит процесс sshd (один из популярных SSH серверов в таблице процессов на основе регулярных выражений), а затем при инициализации сессии пользователя определяет номер псевдотерминала используемого им (обычно в ОС Linux номера псевдотерминальных устройств присваиваются последовательно tty1, tty2 и т.д.; pts1, pts2 и т.д.; ttyS0, ttyS1 и т.д.). После чего подключает отладчик на базе strace к процессу (дочерний процесс sshd, создаваемый для каждой сессии) и на основе перехвата вызовов и выборке полезной нагрузки с помощью регулярных выражений осуществляет реконструкцию пользовательской сессии. Однако, в случае контейнерной инфраструктуры каждый из контейнеров будет создавать свой набор псевдотерминалов не видимый во внешней ОС, при этом каждый из этих псевдотерминалов будет, упомянут в аргументах запуска соответствующих процессов sshdв таблице процессов сервера. Таким образом, при запуске двух контейнеров и подключении к ним через sshd решение с помощью регулярного выражения выберет только один процесс (с меньшим PID) для подключения отладчика, поскольку активируются псевдотерминалы с одинаковым именем. Однако по ряду признаков (идентификаторы процессов, IP-адреса контейнеров в строке запуска) возможно, определить к какому контейнеру относится указанный процесс. С учетом этого сценарий ttylog.pl был доработан авторским коллективом (выборка по имени или адресу контейнера) и сбор пользовательского взаимодействия с псевдотерминалом стал возможен без вмешательства в пространство контейнера.

Рассмотрим вопрос сбора информации о запускаемых процессах. Как упомянуто выше, технологии на основе LD_PRELOAD не обеспечивают достоверный перехват системных вызовов exесв контейнерных инфраструктурах. Однако, напомним, что ядро операционной системы является общим для всех контейнеров, а технология BPF имеет возмож-

ность перехвата в том числе и системного вызова exec. Популярный программный пакет BCC [20] предоставляет набор инструментов для создания эффективных программ трассировки ядра и управления им, а также включает в себя несколько полезных инструментов и примеров. Среди включенных в состав пакета инструментов присутствует execsnoop.py, который обеспечивает перехват системных вызовов execв системе. Отметим, что указанный пакет легко устанавливается на Ubuntu 22.04 поскольку присутствует в стандартном репозитории пакетов под именем bpfcc-tools, при этом требуемый инструмент имеет имя execsnoop-bpfcc. При запуске по умолчанию решение выводит в консоль PID запускаемого процесса, родительского процесса и строку запуска. Однако нам для адекватного сопоставления с действиями в консоли, также требуется определять время запуска процесса. Кроме того, крайне затруднительно определить на основе одних лишь родительских процессов принадлежность процессов к тому или иному контейнеру.

Детальнее рассмотрим возможности инструмента execsnoop.py. Не представляет затруднений добавить в вывод команды время посредством соответствующего аргумента. Кроме того, инструмент имеет возможность выборки запускаемых процессов по контрольным группам (cgroup). Как упомянуто выше, Docker также использует механизм контрольных групп при своей работе. В общем случае новая контрольная группа создается при старте контейнера. При этом с помощью execsnoop.py возможно осуществить выборку процессов, относящихся к задаваемому множеству контрольных групп. Это может быть удобно, в частности в мультитенантных инфраструктурах, а также в виртуальных лабораторных работах, когда изучаемая инфраструктура представлена более чем в одном контейнере. В результате журнал активности (запуска процессов) в контейнерах одного тенанта формируется в едином месте. При этом подмножества контейнеров, над которыми выполняется мониторинг могут быть пересекающимися, это удобно в том случае, когда несколько тенантов разделяют некоторый разделяемый общий ресурс (файловое хранилище, сервис совместной работы и т.д.).

Множество контрольных групп для execsnoop.py задается посредством механизма разделяемой памяти BPF – карт BPF (BPFmaps). Карты BPF представляют собой динамическую, разделяемую ядром и пользовательским пространством структуру хранения данных, организуемую, как массив, хэш-таблицу, стэк, очередь и т.д. [21]. execsnoop.py использует библиотеку пакета BCC [20] containers.py для работы с контрольными группами. В качестве разделяемого ресурса используется хэш-таблица, в которой перечислены идентификаторы cgroupId контрольных групп, мониторинг которых требуется обеспечивать. Поскольку, карта BPF является динамическим ресурсом, то добавление контрольной группы, возможно, организовать без перерыва мониторинга других контейнеров. Таким образом, при запуске очередного контейнера тенантом соответствующий ему cgroupID должен быть помещен в карту BPF, соответствующую тенанту, для обеспечения мониторинга.

Обратим также внимание, что при длительной работе ОС возможно повторное назначение cgroupID, который уже присваивался ранее создаваемой и завершившей свою работу контрольной группе. Это, во-первых, может создать коллизии при мониторинге (в журнал мониторинга тенанта будут поступать записи с другого тенанта или системной контрольной группы), во-вторых, может вызвать переполнение записей в BPF карте (по умолчанию объем ограничен 1024 записями).

Авторами предлагается следующее решение (рис. 2). В данной диаграмме активностей представлен жизненный цикл аккаунта тенанта с точки зрения обеспечения мониторинга его ресурсов. Начнем с того, что администратор инфраструктуры тенанта создает аккаунт с функциями управления контейнерами посредством платформы доставки сервиса (интерфейса или прикладного API) IaaS платформы. На этом этапе нами предлагается создание BPF карты ассоциированной с данным тенантом. После того как администратор тенанта запускает контейнер для подключения к нему мониторинга необходимо добавить его в соответствующую BPF карту. Поскольку принадлежность процессов, определяется идентификатором cgroupID (8 байт), его необходимо определить после запуска контейнера. Этот идентификатор назначается подсистемой cgroup ядра операционной системы после запуска контейнера. Отметим, что все файловые объекты инфраструктуры cgroup во время исполнения контейнера (в случае среды контейнеризации docker) располагаются в специализированной файловой системе

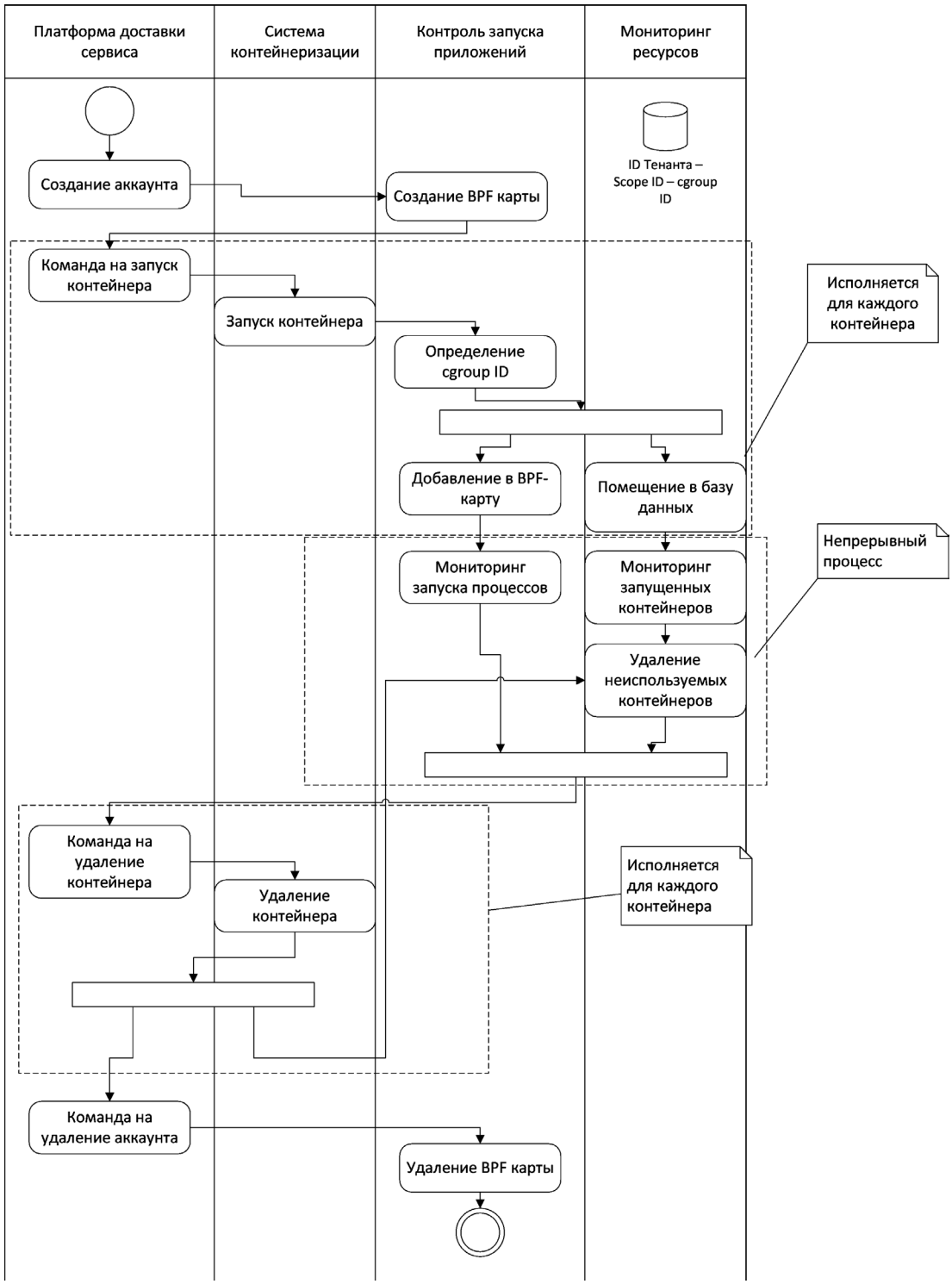


Рис. 2. Диаграмма активностей предложенного решения по запуску процессов

cgroupfs, которая поумолчанию монтируется в /sys/fs/cgroupпри этом пространство контейнера в ней определяется, как /sys/fs/cgroup/user-<uid пользователя, от которого запущен docker>.slice/docker-<ScopeID>.scope или sys/fs/cgroup/system.slice/docker-<ScopeID>.scope. Где ScopeID – это 32 байтный уникальный псевдослучайный идентификатор контейнера, назначаемый сервисом dockerпри создании контейнера. Очевидно, что уникальность идентификации контейнера по ScopeID выше, чем по cgroupID, поэтому

и возникают коллизии (повторные использования cgroupID контейнерами после использования, ранее освобожденного по завершению контейнера). С точки зрения ОС семейства Linux пространство контейнера в файловой системе – это директория, а cgroupID – это ее специализированный атрибут. Обработка специализированных атрибутов не всегда может быть выполнена стандартным ПО дистрибутива, включая ПО из репозиториев. В Ubuntu 22.04 также отсутствует подобное ПО. В [20] предлагается утилита в исходном коде cgroupid для чтения атрибута, и она была пакетирована авторским коллективом.

После определения cgroupID мы добавляем его в соответствующую тенанту BPF-карту, а также размещаем соответствующую запись в служебной базе данных, содержащую также ScopeID и ID тенанта из платформы доставки сервиса (в данном эксперименте мы использовали простой CSV-файл). При удалении контейнера или тенанта штатными средствами мы легко удаляем соответствующие записи из BPF карты или саму карту. Однако если по какой-то причине контейнер не был штатно завершен, и информация об этом не поступила в средство удаления записей мониторинга, то наше решение периодически опрашивает файловую систему на предмет активности пространств, отраженных в таблице. При обнаружении неактивных пространств соответствующие записи удаляются. При этом средству мониторинга запущенных контейнеров необходимо журналировать факт старта контейнера с фиксацией времени, а также PID, запущенных и родительского процесса (containerd-shim-runc-v"1|2"), обеспечивающего запуск контейнера. Также и факт удаления записи об запущенном контейнере должен журналироваться.

Рассмотрим пример работы мониторинга запуска процессов для небольшой системы из двух контейнеров и двух тенантов (для упрощения понимания). Один из ресурсов для них является общим, а один из тенантов (tenant1) также владеет и уникальным контейнером. На рис. 3 представлен вывод терминала содержащий, соответствующие идентификаторы и содержимое BPF карт. На рис. 4 представлен вывод мониторинга процессов с двух тенантов, как можно заметить, встает вопрос определения принадлежности того или иного процесса конкретному контейнеру при этом предлагается решение этой проблемы за счет определения принадлежности родительского процесса первой записи к конкретному контейнеру, а затем последовательной обработки записей. Используя журналы системы мониторинга ресурсов определяем, какой из процессов, к какому контейнеру относился.

```
andrey@andrey-virtual-machine:~$ sudo docker container list
[sudo] password for andrey:
CONTAINER ID   IMAGE                          COMMAND               CREATED          STATUS              PORTS                     NAMES
7861b4f3b686   postfix:latest                 "/usr/sbin/sshd -D"   2 minutes ago    Up About a minute   22/tcp, 25/tcp            nervous_chandrasekhar
f67c823d0c60   edurange2/ubuntu-sshd:16.04    "/usr/sbin/sshd -D"   7 days ago       Up 50 minutes       0.0.0.0:49155->22/tcp   gs_nat
andrey@andrey-virtual-machine:~$ cgroupid hex /sys/fs/cgroup/system.slice/docker-7861b4f3b686b0d5ad822f8fb042caf55fef07bd236be0cef774a6c2027e300c.scope/
4d 2b 00 00 00 00 00 00
andrey@andrey-virtual-machine:~$ cgroupid hex /sys/fs/cgroup/system.slice/docker-f67c823d0c60f1ad545965f2648e052b8e41e460d5217c6bca22486c5dc00daa.scope/
08 2a 00 00 00 00 00 00
andrey@andrey-virtual-machine:~$ sudo bpftool map create /sys/fs/bpf/tenant1 type hash key 8 value 8 entries 128 name cgroupset flags 0
andrey@andrey-virtual-machine:~$ sudo bpftool map create /sys/fs/bpf/tenant2 type hash key 8 value 8 entries 128 name cgroupset flags 0
andrey@andrey-virtual-machine:~$ sudo bpftool map update pinned /sys/fs/bpf/tenant1 key hex 4d 2b 00 00 00 00 00 00 value hex 00 00 00 00 00 00 00 00 any
andrey@andrey-virtual-machine:~$ sudo bpftool map update pinned /sys/fs/bpf/tenant1 key hex 08 2a 00 00 00 00 00 00 value hex 00 00 00 00 00 00 00 00 any
andrey@andrey-virtual-machine:~$ sudo bpftool map update pinned /sys/fs/bpf/tenant2 key hex 4d 2b 00 00 00 00 00 00 value hex 00 00 00 00 00 00 00 00 any
andrey@andrey-virtual-machine:~$ sudo bpftool map dump pinned /sys/fs/bpf/tenant1
key: 4d 2b 00 00 00 00 00 00  value: 00 00 00 00 00 00 00 00
key: 08 2a 00 00 00 00 00 00  value: 00 00 00 00 00 00 00 00
Found 2 elements
andrey@andrey-virtual-machine:~/cgroupid$ sudo bpftool map dump pinned /sys/fs/bpf/tenant2
key: 4d 2b 00 00 00 00 00 00  value: 00 00 00 00 00 00 00 00
Found 1 element
```

Рис. 3. Используемые идентификаторы контейнеров.

```
TIME     PCOMM            PID    PPID   RET ARGS
23:56:17 sshd             6115   5679     0 /usr/sbin/sshd -D -R
23:56:23 sshd             6119   5120     0 /usr/sbin/sshd -D -R
23:56:23 bash             6124   6123     0 /bin/bash -c /usr/local/src/ttylog/start_ttylog.sh
23:56:23 start_ttylog.sh  6124   6123     0 /usr/local/src/ttylog/start_ttylog.sh
23:56:23 grep             6127   6125     0 /bin/grep ^sftp
23:56:23 grep             6130   6128     0 /bin/grep ^scp
23:56:23 tty              6132   6124     0 /usr/bin/tty
23:56:23 hostname         6133   6124     0 /bin/hostname
23:56:23 sudo             6134   6124     0 /usr/bin/sudo cat /usr/local/src/logs/count.NAT
23:56:23 cat              6135   6134     0 /bin/cat /usr/local/src/logs/count.NAT
23:56:23 sudo             6137   6124     0 /usr/bin/sudo tee /usr/local/src/logs/count.NAT
23:56:23 tee              6138   6137     0 /usr/bin/tee /usr/local/src/logs/count.NAT

TIME     PCOMM            PID    PPID   RET ARGS
23:56:17 sshd             6115   5679     0 /usr/sbin/sshd -D -R
23:56:46 bash             6202   6201     0 /bin/bash
23:57:03 date             6204   6202     0 /bin/date
```

Рис. 4. Вывод мониторинга процессов для рассматриваемого примера. Слева для tenant1, справа для tenant2

Рассмотрим подробнее рисунок 4. Рамкой показаны процессы, относящиеся к одному контейнеру в одном тенанте. Однако, очевидно, что не все процессы в представленном журнале выстраиваются в единую цепочку родитель-потомок. Такие процессы без явного родителя отмечены на рисунке 4 стрелками. Это объясняется тем, что execsnoop.py

перехватывает лишь системный вызов exec (загрузки исполняемого образа в ОЗУ), в то время как новый процесс может быть создан системным вызовом fork без загрузки нового исполняемого образа в ОЗУ. Однако, в таком случае возможно определить принадлежность к контейнеру процесса посредством systemctl. А вопрос перехвата системного вызова fork является задачей дальнейших исследований. Также недостатком представленного вывода средства мониторинга является формат вывода времени перехваченного события, такой формат не удобен для дальнейшей машинной обработки и сопоставления с действиями пользователя на терминале. Но встроенные средства ОС позволяют его сконвертировать в более удобное целочисленное представление Unix-времени.

Решение [13] в составе системы мониторинга имеет модуль предварительной обработки журнала взаимодействия с терминалом, который конвертирует журнал в формат csvi формирует такие поля, как входная строка пользователя; уникальный идентификатор, формируемый на основе имени пользователя, тенанта и номера; предварительный класс записи; целочисленное представление Unix-времени; имя пользователя; текущая директория; вывод терминала. Поскольку выводной формат предложенной авторами реализации ttylog.pl идентичен, мы используем тот же механизм постобработки. Кроме того, в соответствии с дополнительной информацией, полученной с модуля сбора информации о запускаемых процессах имеется возможность дополнить эту информацию (при этом обработка должна производится в конвейерном режиме и также необходимо определять текущую директорию процесса, определить же имя исполняющего пользователя в контейнере извне не всегда представляется возможным, например, когда пользователь запускает программу, как службу). Для корреляции событий возможно использовать время, а в случае сложных многопользовательских ресурсов, включая разделенные между тенантами, требуется более детальное определение принадлежности процессов пользователям, а в некоторых случаях возможно ручной анализ. В конечном счете, получаем единый журнал действий в начале для каждого контейнера, а затем для тенанта в целом.

Для дальнейшей обработки решение [13] предлагает производить анализ полученных строк специально задаваемыми регулярными выражениями(вехами) на предмет соответствия следующих признаков имя узла, строки ввода и вывода. Изначально решение предложено для проверки хода выполнения виртуальных лабораторных работ, однако на наш взгляд при созданный подход применим и для обнаружения потенциально нежелательных и злонамеренных действий пользователя. Потенциально каждая веха является сигнатурой и позволяет маркировать события (назначать соответствующий класс) как потенциально опасные. Дальнейший анализ данных в CSV не является удобным в силу того, что требуется находить взаимосвязи между представленными действиями пользователя. В работе [22] представлен формат, удобный для машинной обработки на основе JSON, содержащий следующие поля: время, команда, пользователь, имя контейнера, рабочая директория, кроме того, в проекте [13] отмечается подход конвертации сформированных данных в указанный JSON-формат с обогащением его уникальным идентификатором и классом записи. Как правило, после первичного анализа нет необходимости в хранении вывода команд.

В итоге полученные журналы являются хорошо подлежащими машинной обработке и могут быть проанализированы в системах сбора, анализа, уведомлений и визуализации журналов (ELK, Graylog, Grafana и т.д), в том числе на предмет выявления признаков сложных цепочек подозрительных команд. Таким образом, данный подход мог бы найти свое применение в системах аудита сервисов, предоставляющих услуги контейнеризации (IaaS-платформ); специализированных модулях DLP-систем, а также при организации сред виртуальных лабораторных работ. Ключевым преимуществом, разработанного авторами подхода является полная неинтрузивность, относительно контейнеров тенанта, и прозрачность для пользователя. Недостатки подхода отражены по ходу статьи (проблемы с обработкой вызова fork, более сложное аннотирование журналов на стороне операционной системы), также можно отметить определенные проблемы с обслуживанием решений на базе технологии BPF в связи с ее активным развитием, в частности репозиториях Ubuntu 22.04 на момент написания статьи размещен пакет bpfcc-tools версии 0.18, при том, что используется по умолчанию используется ядро Linux линейки 5.15, с которой совместим лишь набор инструмен-

тов версии 0.23. Не все системные структуры BPF обладают хорошей обратной совместимостью, и поскольку strace весьма популярная утилита, ее работа, как правило, гарантируется с текущим ядром разработчиками дистрибутива. Более редкие же инструменты, например, ttysnoop.py (альтернативный инструмент перехвата информации с псевдотерминала) оказались в силу этого неработоспособны. Работа execsnoop.py пока обладает в целом обратной совместимостью (отсутствует лишь возможность фильтрации процессов по PID родительского), при этом работа не гарантируется при обновлении ядра. Ручное же пакетирование является затруднительным в силу некоторых специфичных особенностей реализации ядра в каждой ОС. В дальнейшем авторы планируют усовершенствовать механизмы выборки информации и обработки служебных данных, а также разработать демонстрационную базу сигнатур.

Литература

1. Юрий Семенюков, Контейнеризация в enterprise: взгляд практика. Jetinfo, №7-8 (307-308) декабрь 2021, 36-43, https://www.jetinfo.ru/wp-content/uploads/2021/12/jetinfo_07_08_2021.pdf

2. Антон Гаврилов, 5000 слов о защите контейнеров. Jetinfo, №7-8 (307-308) декабрь 2021, 44-57, https://www.jetinfo.ru/wp-content/uploads/2021/12/jetinfo_07_08_2021.pdf

3. Ghadeer, D. Security in Kubernetes: best practices and security analysis / D. Ghadeer, H. Jaafar, A. A. Vorobeva // Journal of the Ural Federal District. Information Security. – 2022. – No 2(44). – P. 63–69. – DOI 10.14529/secur220209. – EDN ZYDBOK.

4. ООО «Яндекс.Облако», Yandex Cloud Logging, 2022, https://cloud.yandex.ru/docs/logging/

5. Amazon Web Services, Inc., AWS Cloud Trail: Отслеживание действий пользователей и использования API, 2022, https://aws.amazon.com/ru/cloudtrail/

6. Google LLC, Cloud logging documentation, 2022, https://cloud.google.com/logging/docs

7. ООО «Яндекс.Облако», Yandex Audit Trails, 2022, https://cloud.yandex.ru/docs/logging/

8. Amazon Web Services, Inc., AWS Config: Запись и оценка конфигурации ресурсов AWS, 2022, https://aws.amazon.com/ru/config/

9. Taylor, C.; Arias, P.; Klopchic, J.; Matarazzo, C.; Dube, E. CTF: State-of-the-Art and building the next generation. In 2017 USENIX Workshop on Advances in Security Education (ASE 17); 2017. Available online: https://www.usenix.org/conference/ase17/workshop-program/presentation/taylor (accessed on 4 August 2021).

10. Davis, A.; Leek, T.; Zhivich, M.; Gwinnup, K.; Leonard, W. The Fun and Future of CTF. In Proceedings of the 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education, San Diego, CA, USA, 18 August 2014.

11. Richard Weiss, Michael E. Locasto, and Jens Mache. 2016. A Reflective Approach to Assessing Student Performance in Cybersecurity Exercises. In Proceedings of the 47th ACM Technical Symposium on Computing Science Education (SIGCSE '16). Association for Computing Machinery, New York, NY, USA, 597–602. https://doi.org/10.1145/2839509.2844646

12. Valdemar Švábenský, Richard Weiss, Jack Cook, Jan Vykopal, Pavel Čeleda, Jens Mache, Radoslav Chudovský, and Ankur Chattopadhyay. 2022. Evaluating Two Approaches to Assessing Student Progress in Cybersecurity Exercises. In Proceedings of the 53rd ACM Technical Symposium on Computer Science Education V. 1 (SIGCSE 2022). Association for Computing Machinery, New York, NY, USA, 787–793. https://doi.org/10.1145/3478431.3499414

13. Jelena Mirkovic, Aashray Aggarwal, David Weinman, Paul Lepe, Jens Mache, and Richard Weiss. 2020. Using Terminal Histories to Monitor Student Progress on Hands-on Exercises. In Proceedings of the 51st ACM Technical Symposium on Computer Science Education (SIGCSE '20). Association for Computing Machinery, New York, NY, USA, 866–872. https://doi.org/10.1145/3328778.3366935

14. R. Weiss, F. Turbak, J. Mache and M. E. Locasto, "Cybersecurity Education and Assessment in EDURange," in IEEE Security & Privacy, vol. 15, no. 3, P. 90–95, 2017, doi: 10.1109/MSP.2017.54.

15. Jan Vykopal, Valdemar Švábenský, Pavel Seda, and Pavel Čeleda. 2022. Preventing Cheating in Hands-on Lab Assignments. In Proceedings of the 53rd ACM Technical Symposium on Computer Science Education V. 1 (SIGCSE 2022). Association for Computing Machinery, New York, NY, USA, 78–84. https://doi.org/10.1145/3478431.3499420

16. M. A. Eriksen and M. Baker. Snoopy Logger. https://github.com/a2o/snoopy.

17. Karagiannis, S.; Ntantogian, C.; Magkos, E.; Ribeiro, L.L.; Campos, L. PocketCTF: A Fully Featured

Approach for Hosting Portable Attack and Defense Cybersecurity Exercises. Information 2021, 12, 318. https://doi.org/10.3390/info12080318

18. Moravcik, M.; Segec, P.; Kontsek, M.; Uramova, J.; Papan, J. Comparison of LXC and Docker Technologies. In Proceedingsof the 2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA), Košice, Slovenia,12–13 November 2020; P. 481–486

19. David Calavera, Lorenzo Fontana Linux Observability with BPF: Advanced Programming for Performance Analysis and Networking, ISBN: 9781492050209, December 24th, 2019

20. IOVisor community, BPF Compiler Collection https://github.com/iovisor/bcc.

21. Антон Протопопов, BPF для самых маленьких, часть первая: extended BPF, 11 августа 2020. https://habr.com/ru/post/514736/

22. Valdemar Švábenský, Jan Vykopal, Pavel Seda, Pavel Čeleda, Dataset of shell commands used by participants of hands-on cybersecurity training, Data in Brief, Volume 38, 2021, 107398, ISSN 2352-3409, https://doi.org/10.1016/j.dib.2021.107398.

References

1. Yuriy Semenyukov, Konteynerizatsiya v enterprise: vzglyad praktika. Jetinfo, №7-8 (307-308) December 2021, 36-43, https://www.jetinfo.ru/wp-content/uploads/2021/12/jetinfo_07_08_2021.pdf

2. Anton Gavrilov, 5000 slov o zashchite konteynerov. Jetinfo, №7-8 (307-308) December 2021, 44–57, https://www.jetinfo.ru/wp-content/uploads/2021/12/jetinfo_07_08_2021.pdf

3. Ghadeer, D. Security in Kubernetes: best practices and security analysis / D. Ghadeer, H. Jaafar, A. A. Vorobeva // Journal of the Ural Federal District. Information Security. – 2022. – No 2(44). – P. 63–69. – DOI 10.14529/secur220209. – EDN ZYDBOK.

4. Yandex.Cloud LLC, Yandex Cloud Logging, 2022, https://cloud.yandex.com/en-ru/docs/logging/

5. Amazon Web Services, Inc., AWS Cloud Trail: Track user activity and API usage, 2022, https://aws.amazon.com/cloudtrail/

6. Google LLC, Cloud logging documentation, 2022, https://cloud.google.com/logging/docs

7. Yandex.Cloud LLC, Yandex Audit Trails, 2022, https://cloud.yandex.ru/docs/logging/

8. Amazon Web Services, Inc., AWS Config: Record and evaluate configurations of your AWS resources, 2022, https://aws.amazon.com/config/

9. Taylor, C.; Arias, P.; Klopchic, J.; Matarazzo, C.; Dube, E. CTF: State-of-the-Art and building the next generation. In 2017 USENIX Workshop on Advances in Security Education (ASE 17); 2017. Available online: https://www.usenix.org/conference/ase17/workshop-program/presentation/taylor (accessed on 4 August 2021).

10. Davis, A.; Leek, T.; Zhivich, M.; Gwinnup, K.; Leonard, W. The Fun and Future of CTF. In Proceedings of the 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education, San Diego, CA, USA, 18 August 2014.

11. Richard Weiss, Michael E. Locasto, and Jens Mache. 2016. A Reflective Approach to Assessing Student Performance in Cybersecurity Exercises. In Proceedings of the 47th ACM Technical Symposium on Computing Science Education (SIGCSE '16). Association for Computing Machinery, New York, NY, USA, 597–602. https://doi.org/10.1145/2839509.2844646

12. Valdemar Švábenský, Richard Weiss, Jack Cook, Jan Vykopal, Pavel Čeleda, Jens Mache, Radoslav Chudovský, and Ankur Chattopadhyay. 2022. Evaluating Two Approaches to Assessing Student Progress in Cybersecurity Exercises. In Proceedings of the 53rd ACM Technical Symposium on Computer Science Education V. 1 (SIGCSE 2022). Association for Computing Machinery, New York, NY, USA, 787–793. https://doi.org/10.1145/3478431.3499414

13. Jelena Mirkovic, Aashray Aggarwal, David Weinman, Paul Lepe, Jens Mache, and Richard Weiss. 2020. Using Terminal Histories to Monitor Student Progress on Hands-on Exercises. In Proceedings of the 51st ACM Technical Symposium on Computer Science Education (SIGCSE '20). Association for Computing Machinery, New York, NY, USA, 866–872. https://doi.org/10.1145/3328778.3366935

14. R. Weiss, F. Turbak, J. Mache and M. E. Locasto, "Cybersecurity Education and Assessment in EDURange," in IEEE Security & Privacy, vol. 15, no. 3, P. 90–95, 2017, doi: 10.1109/MSP.2017.54.

15. Jan Vykopal, Valdemar Švábenský, Pavel Seda, and Pavel Čeleda. 2022. Preventing Cheating in Hands-on Lab Assignments. In Proceedings of the 53rd ACM Technical Symposium on Computer Science Education V. 1 (SIGCSE 2022). Association for Computing Machinery, New York, NY, USA, 78–84. https://doi.org/10.1145/3478431.3499420

16. M. A. Eriksen and M. Baker. Snoopy Logger. https://github.com/a2o/snoopy.

17. Karagiannis, S.; Ntantogian, C.; Magkos, E.; Ribeiro, L.L.; Campos, L. PocketCTF: A Fully Featured

Approach for Hosting Portable Attack and Defense Cybersecurity Exercises. Information 2021, 12, 318. https://doi.org/10.3390/info12080318

18. Moravcik, M.; Segec, P.; Kontsek, M.; Uramova, J.; Papan, J. Comparison of LXC and Docker Technologies. In Proceedingsof the 2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA), Košice, Slovenia,12–13 November 2020; P. 481–486

19. David Calavera, Lorenzo Fontana Linux Observability with BPF: Advanced Programming for Performance Analysis and Networking, ISBN: 9781492050209, December 24th, 2019

20. IOVisor community, BPF Compiler Collection https://github.com/iovisor/bcc.

21. Anton Protopopov, BPF dlya samykh malen'kikh, chast' pervaya: extended BPF, 11 August 2020. https://habr.com/ru/post/514736/

22. Valdemar Švábenský, Jan Vykopal, Pavel Seda, Pavel Čeleda, Dataset of shell commands used by participants of hands-on cybersecurity training, Data in Brief, Volume 38, 2021, 107398, ISSN 2352–3409, https://doi.org/10.1016/j.dib.2021.107398.

БАРИНОВ Андрей Евгеньевич, старший преподаватель кафедры защиты информации, специалист по защите информации, и.о. директора НОЦ «Информационная безопасность», ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, пр. Ленина, д. 76. E-mail: barinovae@susu.ru

МОРОЗОВ Игорь Александрович, младший научный сотрудник НОЦ «Информационная безопасность», ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, пр. Ленина, д. 76. E-mail: morozovia@susu.ru

МЕЛЬНИКОВ Константин Вадимович, студент кафедры защиты информации, ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, пр. Ленина, 76. E-mail: dexmoning@gmail.com

РУДЕНКО Евгений Александрович, студент кафедры защиты информации, ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, пр. Ленина, 76. E-mail: s1lentsorrow@yandex.ru

BARINOV Andrey Evgenyevich, Senior Lecturer of the Information Security Department, Information Security Specialist, Acting director of the Research and Educational Center "Information Security", South Ural State University (national research university). Russia, 454080, Chelyabinsk, Lenin Ave., 76. E-mail: barinovae@susu.ru

MOROZOV Igor Aleksandrovich, Junior Researcher of the Research and Educational Center "Information Security", South Ural State University (national research university). Russia, 454080, Chelyabinsk, Lenin Ave., 76. E-mail: morozovia@susu.ru.

MELNIKOV Konstantin Vadimovich, student of the Department of Information Security, South Ural State University (national research university). Russia, 454080, Chelyabinsk, Lenin Ave., 76. E-mail: dexmoning@gmail.com

RUDENKO Evgeniy Alexandrovich, student of the Department of Information Security, South Ural State University (national research university). Russia, 454080, Chelyabinsk, Lenin Ave., 76. E-mail: s1lentsorrow@yandex.ru

УДК 004.056

Вестник УрФО № 1(47) / 2023, с. 27–42

Хорев А.А.

DOI: 10.14529/secur230103

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ АКУСТООПТИЧЕСКОГО КАНАЛА УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ

В статье представлена математическая модель акустооптического канала утечки акустической речевой информации. В качестве показателя оценки возможностей лазерной системы акустической речевой разведки (ЛСАРР) используется словесная разборчивость речи Wc, рассчитываемая на линейном выходе ЛСАРР с учетом вероятности обнаружения отраженного от зондируемой поверхности лазерного излучения приемником оптического излучения ЛСАРР. Получены аналитические соотношения для расчета вероятности обнаружения отраженного сигнала для трех видов отражения: а) диффузное; б) зеркальное; в) смешенное. Для расчета словесной разборчивости используется вероятностная методика оценки разборчивости речи.

Ключевые слова: выделенное помещение, акустооптический канал утечки акустической речевой информации, лазерная система акустической речевой разведки, математическая модель, словесная разборчивость речи.

Horev A.A.

MATHEMATICAL MODEL OF THE ACOUSTO-OPTIC CHANNEL OF SPEECH INFORMATION LEAKAGE

The article presents a mathematical model of the acousto-optic channel of acoustic speech information leakage. As an indicator of the evaluation of the capabilities of the laser acoustic speech intelligence system (LSARR), the verbal intelligibility of Wc speech is used, calculated at the linear output of the LSARR, taking into account the probability of detection of laser radiation reflected from the probed surface by an optical radiation receiver. Analytical relations are obtained for calculating the probability of detecting a reflected signal for three types of reflection: a) diffuse; b) specular; c) mixed. To calculate the verbal intelligibility of speech, a probabilistic method of assessing speech intelligibility is used.

Keywords: dedicated room, acousto-optic channel of acoustic speech information leakage, laser system of acoustic speech intelligence, mathematical model, verbal intelligibility of speech.

Одним из наиболее опасных технических каналов утечки акустической речевой информации из выделенных помещений (ВП), позволяющим перехватывать речевую информацию из-за пределов контролируемой зоны объекта, является акустооптический технический канал утечки информации [1].

Перехват акустической речевой информации по акустооптическому каналу осуществляется с использованием лазерных систем акустической речевой разведки (ЛСАРР), часто называемых «лазерными микрофонами», путем лазерного «зондирования» отражающих поверхностей, например, оконных стекол, оконных штор, жалюзи или различных предметов, установленных в ВП [1, 2].

С целью оценки возможности перехвата акустической речевой информации из выделенных помещений по техническим каналам и выбора наиболее рациональных способов и средств защиты информации используются методики, в основу которых положены математические модели технических каналов утечки информации.

Под математической моделью будем понимать совокупность уравнений и других математических соотношений, отражающих процесс перехвата речевой информации из ВП лазерными системами акустической речевой разведки.

Учитывая, что целью перехвата речевой информации из ВП, является определение смыслового содержания перехваченного разговора, в качестве показателя оценки возможностей лазерной системой акустической речевой разведки (ЛСАРР) используется словесная разборчивость речи W_c, под которой понимается отношение правильно распознанных слов к общему количеству слов в перехваченном разговоре [1].

Вопросам, связанным с математическим моделированием акустооптического канала утечки речевой информации, посвящены работы [2, 3 – 6].

В работе [3] представлена модель акустооптического канала утечки речевой информации, учитывающая преобразования исходного информативного акустического сигнала и шумовых составляющих в точках «съема» информации ЛСАРР. Однако данная модель не учитывает характеристик ЛСАРР, отражающей поверхности, условий ведения разведки, а также особенностей восприятия зашумленных речевых сигналов оператором.

В статье [4] также предложена математическая модель акустооптического канала утечки речевой информации, в которой в качестве показателя эффективности перехвата речевой информации ЛСАРР используется словесная разборчивость речи, для расчета которой используется формантный метод оценки разборчивости речи. В качестве исходных данных для расчета словесной разборчивости речи используются отношения сигнал/шум на выходе звуковоспроизводящего устройства приемника ЛСАРР в 7-ми октавных полосах речевого диапазона частот, которые определяются отношением вибрационный сигнал/шум на отражающей поверхности. Однако предложенный подход не в полной мере учитывает особенности обнаружения приемником оптического излучения ЛСАРР отраженного от вибрирующей поверхности лазерного сигнала.

В статье [5] была решена задача выделения амплитудной и фазовой модуляции информативных сигналов в акустооптическом канале утечки речевой информации. Однако, учитывая, что в работе отсутствуют методические подходы и аналитические соотношения, позволяющие рассчитать разборчивость речи при перехвате информации по акустооптическому каналу, полученные результаты носят чисто научный характер.

В статье [6] показана возможность использования корреляционного подхода к определению разборчивости речи при перехвате информации по акустооптическому каналу. Однако в работе отсутствуют математические соотношения, позволяющие рассчитать разборчивость речи в зависимости характеристик речевого сигнала, характеристик ЛСАРР, отражающей поверхности и условий ведения разведки, что не позволяет использовать предложенный подход в практической деятельности.

Наиболее подробно вопросы, связанные с моделированием акустооптического канала утечки речевой информации, рассмотрены в монографии [2]. В этой работе приведена описательная модель акустооптического канала утечки речевой информации, рассмо-

трены принципы и особенности построения ЛСАРР, особенности отражения лазерного излучения от различных поверхностей, включая оптические призмы, влияние атмосферы на распространение лазерного излучения. В качестве показателя оценки возможности ЛСАРР использована разборчивость речи и предложены методические подходы ее расчета. В работе предпринята попытка разработки математической модели акустооптического канала утечки речевой информации. Однако в данной модели отсутствуют математические зависимости разборчивости речи от характеристик речевого сигнала, характеристик ЛСАРР, характеристик отражающей поверхности, и помех, воздействующих на отражающую поверхность, а также условий ведения разведки.

Целью данной работы является разработка математической модели акустооптического технического канала утечки речевой информации из выделенного помещения, учитывающей как характеристики речевого сигнала, так и характеристики ЛСАРР, характеристики отражающей поверхности, характеристики помех, воздействующих на отражающую поверхность, а также условий ведения разведки.

Анализ ЛСАРР показал, что наиболее вероятно они строятся на базе лазерных доплеровских виброметров (ЛДВ) [7], поэтому в основу математической модели акустооптического канала утечки речевой информации положим принципы построения и функционирования ЛДВ.

Упрощённая структурная схема ЛДВ, построенного по схеме интерферометра, приведена на рис. 1 [8, 9].

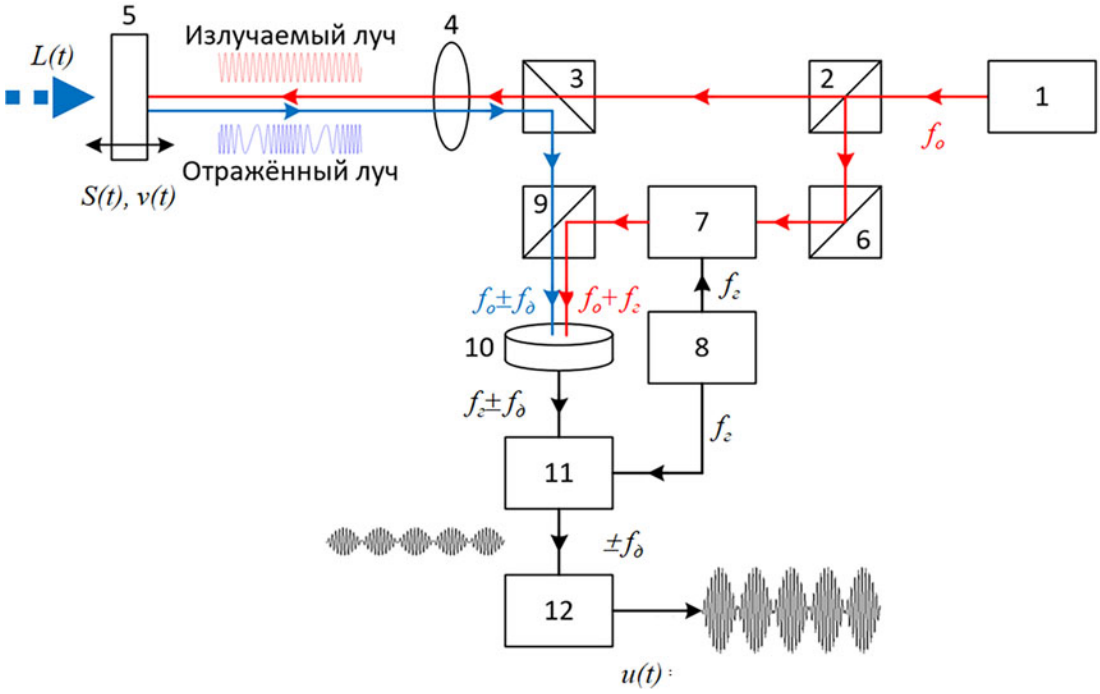


Рис. 1. Упрощённая структурная схема ЛДВ, построенного по схеме интерферометра

Принцип работы ЛДВ заключается в следующем.

Луч от источника лазерного излучения (1) с помощью призмы (2) разделяется на два луча с одинаковыми амплитудами – измерительный и опорный. Первый из них фокусируется с помощью линзы (4) на зондируемой отражающей поверхности (5).

Второй (опорный) луч через призму (6) подается на устройство сдвига частоты (7), которое применяется в схеме с целью формирования несущей частоты колебания выходного сигнала фотоприёмника. В качестве такого устройства наиболее часто используется ячейка Брэгга или электрооптический преобразователь. Частота сдвига опорного луча будет определяться частотой генератора (8).

Вследствие вибрации отражающей поверхности под воздействием акустического сигнала L(t) происходит доплеровский сдвиг частоты отраженного лазерного излучения f_∂, который рассчитывается по формуле [8, 9]

$$f_д(t) = \frac{2v(t)\cos\alpha}{\lambda}, \quad (1)$$

где v(t) – мгновенная скорость колебаний отражающей поверхности, мкм/с;

α – угол между линией визирования ЛСАРР и нормалью к отражающей поверхности (угол зондирования отражающей поверхности), град;

λ – длина волны излучения лазера, мкм.

С помощью призмы (9) опорный луч с частотой $f_о + f_г$ также направляется на приемник оптического излучения (10), в котором происходит формирование интерференционной картины, которое заключается в одновременном воздействии двух сигналов на нелинейный элемент электрической цепи (фотодетектор).

Результирующий сигнал на выходе приемника оптического излучения является типичным частотно-модулированным сигналом будет определяться уравнением [8,9]:

$$u_{пи}(t) = k_{пи} \cdot \left\{\cos\left[2\pi \cdot \left(f_г + f_д\right)t + \Delta\varphi\right]\right\} = \\ = k_{пи} \cdot \left\{\cos\left[2\pi \cdot \left(f_г + \frac{2v}{\lambda}\right)t + \Delta\varphi\right]\right\}, \quad (2)$$

где $k_{пи}$ – коэффициент, зависящий от чувствительности приемника излучения и мощности сигналов лазерного излучения;

Δφ – разность фаз измерительного и опорного лучей.

На частотный дискриминатор (11) подается сигнал с выхода приемника оптического излучения (10) с частотой $f_г + f_д$ и с выхода генератора (8) с частотой $f_г$. Методом частотной демодуляции частот $f_г$ вычитается цепью фазовой автоподстройки, а выходной сигнал выражается как [8,9]:

$$u(t) = k_{чд} \cdot \frac{2v(t)\cos\alpha}{\lambda}, \quad (3)$$

где $k_{чд}$ – коэффициент, зависящий от характеристик частотного дискриминатора.

Электрический сигнал с выхода частотного дискриминатора (11) усиливается по мощности с помощью усилителя (12).

Перехваченный разговор прослушивается оператором через динамики или головные наушники, сигнал на которые подается с линейного выхода приемника ЛСАРР.

Следовательно, разборчивость перехваченного разговора зависит от отношения сигнал/шум на линейном выходе приемника ЛСАРР.

Проведенные экспериментальные исследования показали, что ЛДВ нормально функционируют, если сигнал на входе приемника оптического излучения (ПОИ) превышает пороговое значение, при котором обеспечивается требуемая точность измерения виброскорости (виброускорения или виброперемещения).

Минимальное отношение сигнал/шум, при котором обеспечивается нормальное функционирование ЛДВ, часто называют пороговым отношением сигнал/шум, которое обычно составляет более 6 дБ [10].

Вероятность превышения сигнала на входе приемника оптического излучения порогового значения называют вероятностью обнаружения сигнала.

Учитывая вышесказанное, словесную разборчивость речи при перехвате ЛСАРР ($W_с$) можно рассчитать по формуле:

$$W_с = p \cdot W_{с.от}, \quad (4)$$

где p – вероятность обнаружения отраженного от зондируемой поверхности сигнала приемником оптического излучения ЛСАРР (вероятность превышения отраженного от зондируемой поверхности и падающего на приемник оптического излучения лазерного сигнала установленного порогового значения);

$W_{с.от}$ – словесная разборчивость речи на линейном выходе ЛСАРР, при условии обнаружения отраженного от зондируемой поверхности сигнала приемником оптического излучения ЛСАРР.

Предположим, что сигнал, поступающий на вход приемника оптического излучения, детерминированный с математическим ожиданием $P_с$, а шумы приемника имеют нормальную плотность распределения вероятности с математическим ожиданием, равным нулю, и дисперсией – $\sigma^2_ш$.

Используя критерий Неймана – Пирсона рассчитаем вероятность обнаружения сигнала приемником оптического излучения ЛСАРР [1]:

$$p = \Phi\left[q_{пи} - \Phi^{-1}\left(1 - p_{лт}\right)\right], \quad (5)$$

где $q_{пи}$ – отношение сигнал/шум (по мощности) на входе приемника оптического излучения ЛСАРР;

$p_{лт}$ – вероятность ложной тревоги;

$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} \exp\left(-\frac{t^2}{2}\right) dt$ – интеграл вероятности;

$\Phi^{-1}(x)$ – функция, обратная $\Phi(x)$.

Значение вероятности ложной тревоги может составлять от 10^{-3} до 10^{-6}. Например, $p_{лт} = 10^{-3}$ уравнение (5) примет вид

$$p \approx \Phi\left[q_{пи} - 3,2\right] \quad (6)$$

Следовательно, для расчета вероятности

обнаружения отраженного от зондируемой поверхности сигнала приемником оптического излучения ЛСАРР, необходимо рассчитать отношение сигнал/шум ($q_{пи}$) на входе приемника оптического излучения ЛСАРР.

При расчете отношения сигнал/шум на входе приемника оптического излучения ЛСАРР необходимо учитывать, что в качестве отражающей поверхности в ВП могут использоваться как оконные стекла, так и шторы и жалюзи (рис.1).

Отношение сигнал/шум на входе приемника оптического излучения ЛСАРР рассчитывается по формуле:

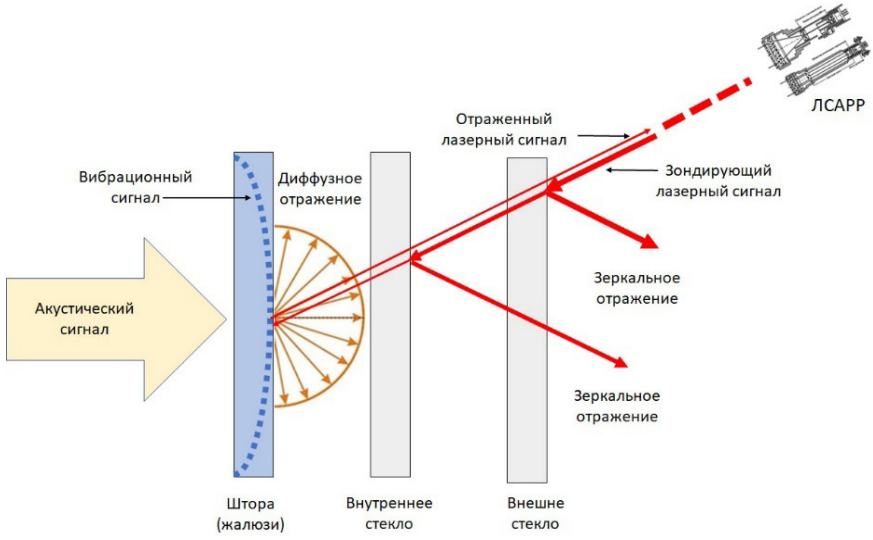


Рис. 1. Схема перехвата речевой информации из выделенного помещения лазерной системой акустической речевой разведки

$$q_{пи} = \frac{P_c}{P_ш}, \quad (7)$$

где P_c – мощность сигнала, отраженного от зондируемой поверхности и попавшая на приемник оптического излучения ЛСАРР, Вт;

$P_ш$ – мощность шумов на входе приемника оптического излучения ЛСАРР, Вт.

Расчет мощности сигнала, отраженного от зондируемой поверхности, на входе приемника оптического излучения проведем для трех видов отражения (рис. 2):

а) диффузное отражение лазерного излучения от зондируемой поверхности;

б) зеркальное отражение лазерного излучения от зондируемой поверхности;

в) смешенное отражение лазерного излучения от зондируемой поверхности.

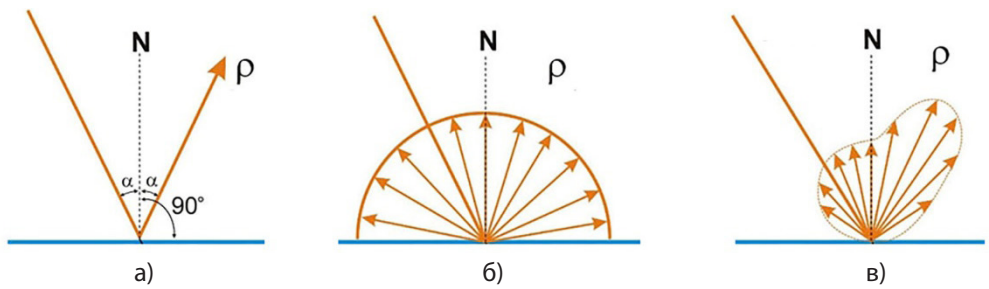


Рис. 2. Виды отражения лазерного излучения от зондируемой поверхности: а) диффузное отражение с равномерным отражением в верхнюю полусферу; б) зеркальное отражение; в) смешенное отражение

а) Диффузное отражение лазерного излучения от зондируемой поверхности

Рассмотрим случай диффузного отражения с равномерным отражением в верхнюю полусферу.

Плотность потока мощности лазерного излучения на зондируемой поверхности $П_{отр}$, Вт/м^2, рассчитаем по формуле [11]:

$$П_{отр} = \frac{P_{из} \cdot \tau_л \cdot \tau_{ср} \cdot cos\alpha}{\left(\pi d_л^2 / 4\right)} = \frac{4 \cdot P_{из} \cdot \tau_л \cdot \tau_{ср} \cdot cos\alpha}{\pi \left(D_н \cdot \theta\right)^2}, \quad (8)$$

где $P_{из}$ – мощность непрерывного лазерного излучения, Вт;

α – угол между линией визирования ЛСАРР и нормалью к отражающей поверхности (угол зондирования отражающей поверхности);

$d_л$ – диаметр пятна лазерного луча на отражающей поверхности, м;

$D_н$ – дальность от отражающей поверхности до аппаратуры разведки, м;

$τ_л$ – коэффициент пропускания передающей оптической системы ЛСАРР;

$τ_{ср}$ – коэффициент пропускания среды на пути распространения лазерного луча (коэффициент пропускания оконных стекол, пленок, установленных на оконных стеклах, атмосферы и т.д.);

θ – расходимость лазерного луча, рад.

Мощность, отраженная от зондируемой поверхности в направлении на приемник излучения $P_{отр}$, Вт, рассчитывается по формуле:

$$P_{отр}=П_{отр}\cdot S_{отр.д}\cdot \rho_д = \frac{4\cdot P_{из}\cdot \tau_л \cdot \tau_{ср}\cdot cos\alpha \cdot S_{отр.д}\cdot \rho_д}{\pi\left(D_н\cdot\theta\right)^2}, \quad (9)$$

где $S_{отр.д}$ – площадь поверхности диффузного отражения лазерного излучения, м²;

$\rho_д$ – коэффициент диффузного отражения поверхности на длине волны λ.

Площадь поверхности диффузного отражения лазерного излучения $S_{отр.д}$, м², рассчитаем по формуле:

$$S_{отр.д}=S_{отр}=\left(\pi d_л^2/4\right)/\cos\alpha=\pi\left(D_н\cdot\theta\right)^2/(4\cdot\cos\alpha), \quad (10)$$

где $S_{отр}$ – общая площадь поверхности отражения лазерного излучения, м².

Подставляя формулу (8) в формулу (7) получим

$$P_{отр}=\frac{4\cdot P_{из}\cdot\tau_л\cdot\tau_{ср}\cdot cos\alpha\cdot\rho_д}{\pi\left(D_н\cdot\theta\right)^2}\cdot\pi\left(D_н\cdot\theta\right)^2/(4\cdot\cos\alpha)=$$

$$=P_{из}\cdot\tau_л\cdot\tau_{ср}\cdot\rho_д. \quad (11)$$

Плотность потока мощности сигнала, отраженного от зондируемой поверхности в верхнюю полусферу, на объективе приемника оптического излучения $П_{пр}$, Вт/м², рассчитаем по формуле:

$$П_{пр}=\frac{P_{отр}\cdot\tau_{ср}}{\pi D_н^2/(4\cdot2)}=\frac{8\cdot P_{из}\cdot\tau_л\cdot\tau_{ср}^2\cdot\rho_д}{\pi D_н^2}. \quad (12)$$

При этом, мощность лазерного излучения, попавшая на объектив приемника $P_{пр.о}$, Вт, будет равна:

$$P_{пр.о}=П_{пр}\cdot\frac{\pi d_o^2}{4}=\frac{4\cdot P_{из}\cdot\tau_л\cdot\tau_{ср}^2\cdot d_o^2\cdot\rho_д}{D_н^2}, \quad (13)$$

где d_o – диаметр входного зрачка объектива приемного устройства ЛСАРР, м.

Оптическая система фокусирует принимаемое лазерное излучение на приемнике оптического излучения. Полагая, что площадь приемника оптического излучения не менее, чем площадь проекции пятна лазерного излучения, мощность излучения, попавшего на приемник излучения P_c, Вт, рассчитаем по формуле:

$$P_c=P_{пр.о}\cdot\tau_{пр}=\frac{4\cdot P_{из}\cdot\tau_л\cdot\tau_{пр}\cdot\tau_{ср}^2\cdot d_o^2\cdot\rho_д}{D_н^2}, \quad (14)$$

где $τ_{пр}$ – коэффициент пропускания объектива приемного устройства ЛСАРР.

Коэффициенты отражения некоторых поверхностей приведены в табл. 1 – 2, а зависимость коэффициента отражения оконного стекла от длины волны – в табл. 3 [2].

Таблица 1

Коэффициенты отражения в видимом диапазоне длин волн некоторых поверхностей

Тип поверхности	Значение коэффициента $\rho_д$
Автомобильное стекло	0,11
Оконное стекло	0,13
Армированное стекло	0,4
Витринное стекло	0,25
Узорчатое стекло	0,3

Таблица 2

Отражательная способность различных поверхностей

Поверхность	Вид отражения	Коэффициент отражения
Алебастр	Диффузное	0,92
Серебро полированное	Направленное	0,88 – 0,93
Матовое серебрение	Направленно – рассеянное	0,7
Стеклянное зеркало	Направленное	0,72 – 0,85

Окончание табл. 2

Поверхность	Вид отражения	Коэффициент отражения
Хромированная полированная поверхность	Направленное	0,60 – 0,70
Матовое хромирование	Направленно – рассеянное	0,50
Алюминий полированный	Направленное	0,65 – 0,75
Алюминии матированный	Направленно – рассеянное	0,55-0,60
Бумага белая матовая	Направленно – рассеянное	0,6 – 0,7
Белая гипсовая поверхность	Диффузное	0,85
Белая клеевая покраска по оштукатуренной поверхности	Приближается к диффузному	до 0,8
Оштукатуренная поверхность	Диффузное	0,4 – 0,45
Шелк белый	Смешанное	0,35 – 0,55
Черное сукно	Направленно – рассеянное	0,1 – 0,12
Черный бархат	Диффузное	0,01 – 0,03

Таблица 3

Зависимость коэффициента отражения оконного стекла от длины волны

Длина волны λ, мкм	Значение коэффициента ρ	Длина волны λ, мкм	Значение коэффициента ρ
0,2	$9,9 \cdot 10^{-1}$	1,06	$3,37 \cdot 10^{-2}$
0,3	$9,5 \cdot 10^{-1}$	1,153	$3,36 \cdot 10^{-2}$
0,4	$3,7 \cdot 10^{-2}$	3,39	$2,89 \cdot 10^{-2}$
0,91	$3,4 \cdot 10^{-2}$	5,1	$2,78 \cdot 10^{-2}$

б) Зеркальное отражение лазерного излучения от зондируемой поверхности

Плотность потока мощности лазерного излучения на зондируемой поверхности $П_{отр}$, Вт/м^2, рассчитывается по формуле (8).

Мощность, отраженная от зондируемой поверхности в направлении на приемник излучения $P_{отр}$, Вт, рассчитывается по формуле:

$$P_{отр} = П_{отр} \cdot S_{отр.з} \cdot \rho_з = \frac{4 \cdot P_{из} \cdot \tau_л \cdot \tau_{ср} \cdot cos\alpha \cdot S_{отр.з} \cdot \rho_з}{\pi (D_н \cdot \theta)^2}, \quad (15)$$

где $S_{отр.з}$ – площадь поверхности зеркального отражения лазерного излучения площадь отражающей поверхности лазерного излучения, м^2;

$\rho_з$ – коэффициент зеркального отражения поверхности на длине волны λ.

Площадь отражающей поверхности лазерного излучения $S_{отр.з}$, м^2, рассчитаем по формуле:

$$S_{отр.з} = S_{отр} = (\pi d_л^2 / 4) / \cos\alpha = \pi (D_н \cdot \theta)^2 / (4 \cdot \cos\alpha). \quad (16)$$

Подставляя формулу (14) в формулу (13) получим:

$$P_{отр} = \frac{4 \cdot P_{из} \cdot \tau_л \cdot \tau_{ср} \cdot cos\alpha \cdot \rho_з}{\pi (D_н \cdot \theta)^2} \cdot \pi (D_н \cdot \theta)^2 / (4 \cdot \cos\alpha) =$$

$$= P_{из} \cdot \tau_л \cdot \tau_{ср} \cdot \rho_з. \quad (17)$$

Полагая, что зеркально отраженное излучение полностью попадает в объектив приемного устройства ЛСАРР и площадь приемника оптического излучения не менее площади проекции пятна принимаемого лазерного излучения, мощность излучения, попавшего на приемник излучения , Вт, рассчитаем по формуле:

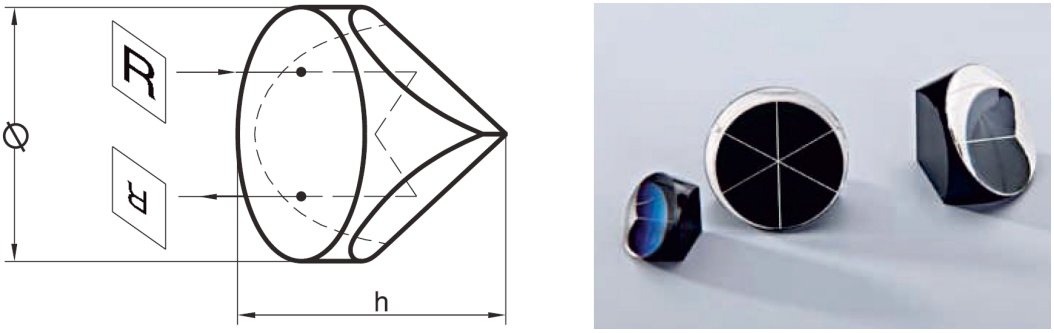
$$P_c = P_{отр} \cdot \tau_{пр} \cdot \tau_{ср} \cdot \rho_з = P_{из} \cdot \tau_л \cdot \tau_{пр} \cdot \tau_{ср}^{\ 2} \cdot \rho_з. \quad (18)$$

Для увеличения мощности отраженного сигнала в направлении на источник лазерного излучения, независимо от взаимного расположения ЛСАРР и обучаемой поверхности, на последней могут устанавливаться триппель-призмы или пленочные отражатели.

Трипель–призма представляет собой отражающий элемент, который обеспечивает возврат излучения в исходном направлении вне зависимости угла падения на входе.

Фактически трипель–призма представляет собой уголковый отражатель, выполненный в виде четырехгранной стеклянной пирамиды, на три грани которой, составляющие друг с другом прямые углы, нанесены зеркальные отражательные покрытия (рис. 3) [12, 13].

Размеры триппель–призм могут составлять от нескольких миллиметров до нескольких десятков миллиметров (табл. 4). Однако могут использоваться триппель-призмы, размеры которых менее 1 мм (рис. 4) [1, 2, 12, 13].



а) б)

Рис. 3. Триппель – призма: схема (а), внешний вид (б)

Таблица 4

Размеры некоторых триппель–призм

Модель триппель-призмы	Размеры		Отклонение светового пучка
	Ø, мм	h, мм	
CCR0080	8.0	6.5	180^0
CCR0150	15	11.3	180^0
CCR0250	25 (25,4)	19	180^0
CCR0380	38	28.5	180^0
CCR0500	50 (50,8)	37.5	180^0
GCL-030502	12,7	9,5	180^0±5″
GCL-030503	25,4	19,1	180^0±5″
GCL-030503	15,0	11,7	180^0±5″

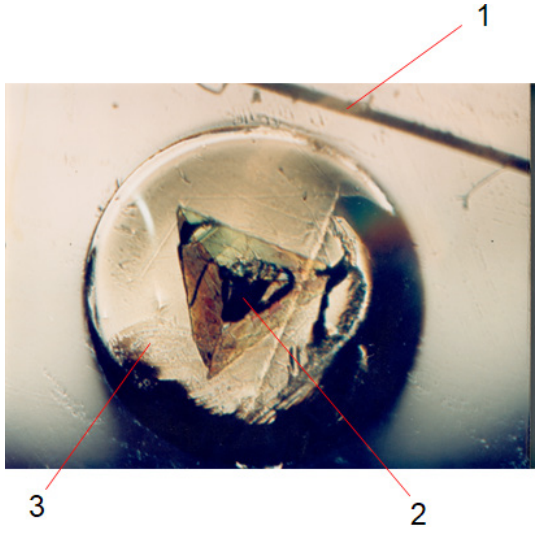


Рис. 4. Триппель-призма, установленная в оконном стекле: 1 – человеческий волос (0,05 – 0,07 мм); 2 – триппель-призма, установленная в углублении стекла; 3 – эпоксидная смола

Световозвращающая (светоотражающая) пленка представляет собой специальную самоклеящуюся наклейку, изготавливаемую из высококачественного материала, который содержит в своем внутреннем слое оптическую систему из сферических линз (микростеклошариков) либо микропризм (рис. 5) [14].

При попадании света на грани микропризм или микросфер, световой поток возвращается обратно по направлению к источнику света. Чтобы избежать нежелательной светопроницаемости и усилить интенсивность отражения света, под слой микросфер добавляется «серебряный» светоотражающий слой.

Микросферы могут иметь очень маленькие размеры 20 – 100 мкм, при этом толщина стенки может составлять 1 – 2 мкм. Например, в светоотражающих пленках «Orafol», размеры отражающих микросфер составляют от 80 – 260 мм [15].

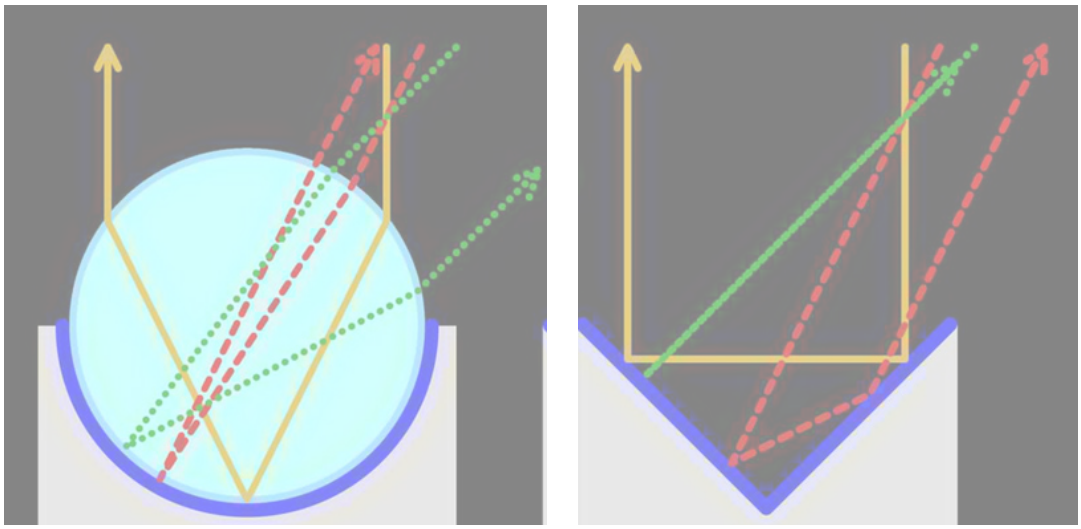
Световозвращающие пленки состоят из элементов (марок) с размерами от 20×20 мм до 90×90 мм и более (рис. 6) [15, 16].

При использовании световозвращающих пленок и триппель-призм, площадь которых превышает площадь пятна лазера на отражающей поверхности, и полагая, что $\rho \approx 1$ для них , формулу (18) запишем в виде:

$$P_c \approx P_{из} \cdot \tau_л \cdot \tau_{пр} \cdot \tau_{ср}^2. \qquad (19)$$

в) смешенное отражение лазерного излучения от зондируемой поверхности:

Режим смешенного отражения наблюдается, как правило в том случае, если на отражающей поверхности устанавливаются отра-



а) б)

Рис. 5. Схемы отражения света от сферических линз (а) и микропризм (б)

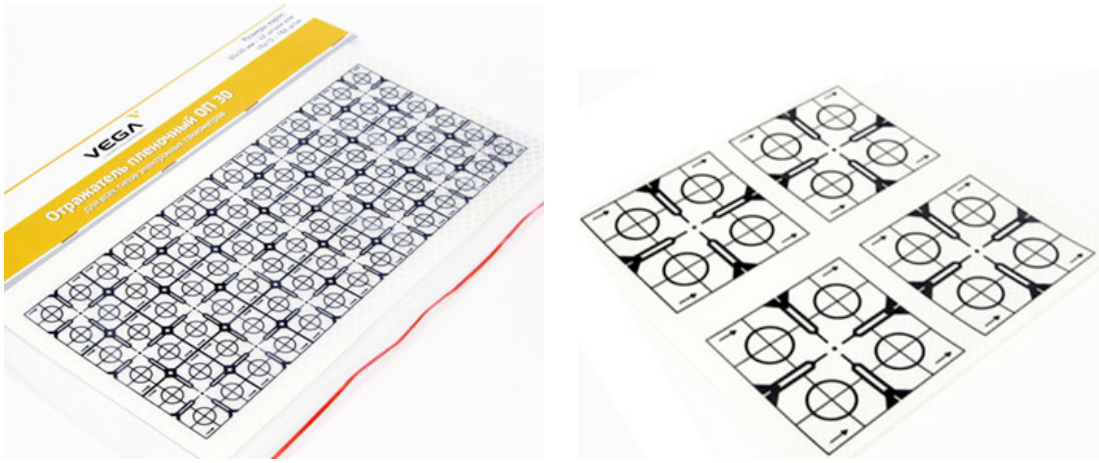


Рис. 6. Внешний вид световозвращающих пленок

жатели, которые по площади менее площади пятна лазера на отражающей поверхности.

Плотность потока мощности лазерного излучения на зондируемой поверхности $П_{отр}$, Вт/м^2, рассчитывается по формуле (8).

Мощность, отраженная от зондируемой поверхности в направлении на приемник излучения $P_{отр}$, Вт, рассчитывается по формуле:

$$P_{отр} = П_{отр} \cdot \left(S^*_{отр.з} \cdot \rho_з + S^*_{отр.д} \cdot \rho_д \right) =$$

$$= \frac{4 \cdot P_{из} \cdot \tau_л \cdot \tau_{ср} \cdot cos\alpha \cdot \left(S^*_{отр.з} \cdot \rho_з + S^*_{отр.д} \cdot \rho_д \right)}{\pi \left(D_н \cdot \theta \right)^2}, \quad (20)$$

где $S^*_{отр.з}$ – площадь поверхности зеркального отражения лазерного излучения, м^2;

$S^*_{отр.д}$ – площадь поверхности диффузного отражения лазерного излучения, м^2.

Площади поверхностей зеркального и диффузного отражения лазерного излучения рассчитаем по формулам:

$$S^*_{отр.з} = S_{пл} (при\ условии,\ что\ S_{пл} < S_{отр}); \quad (21)$$

$$S^*_{отр.д} = S_{отр} - S_{пл} = \pi (D_н \cdot \theta)^2 / (4 \cdot cos\alpha) - S_{пл}, \quad (22)$$

где $S_{пл}$ – площадь поверхности отражения световозвращающей пленки или триппель-призм, попадающих в пятно лазера, м^2.

Подставляя формулы (21) и (22) в формулу (20) получим:

$$P_{отр} = \frac{4 \cdot P_{из} \cdot \tau_л \cdot \tau_{ср} \cdot cos\alpha \cdot \left\{ S_{пл} \cdot \rho_з + \left[\pi \left(D_н \cdot \theta \right)^2 / (4 \cdot \cos\alpha) - S_{пл} \right] \cdot \rho_д \right\}}{\pi \left(D_н \cdot \theta \right)^2} =$$

$$= P_{из} \cdot \tau_л \cdot \tau_{ср} \cdot \left\{ \frac{4 \cdot cos\alpha \cdot S_{пл} \cdot \rho_з}{\pi \left(D_н \cdot \theta \right)^2} + \rho_д \cdot \left[1 - \frac{4 \cdot cos\alpha \cdot S_{пл}}{\pi \left(D_н \cdot \theta \right)^2} \right] \right\}. \quad (23)$$

Полагая, что зеркально отраженное излучение полностью попадает в объектив приемного устройства ЛСАРР и площадь приемника оптического излучения не менее площади проекции пятна принимаемого лазерного

излучения, мощность излучения, попавшего на приемник излучения , Вт, рассчитаем по формуле:

$$P_c = \frac{4 \cdot P_{из} \cdot \tau_л \cdot \tau_{ср} \cdot cos\alpha \cdot S_{пл} \cdot \rho_з \cdot \tau_{пр} \cdot \tau_{ср}}{\pi (D_н \cdot \theta)^2} +$$

$$+ \frac{4 \cdot P_{из} \cdot \tau_з \cdot \tau_{ср} \cdot cos\alpha \cdot \left\{ \left[\pi (D_н \cdot \theta)^2 / (4 \cdot \cos\alpha) - S_{пл} \right] \cdot \rho_о \right\} \cdot \tau_{пр} \cdot \tau_{ср} \cdot (\pi \cdot d_o^2 / 4)}{\pi (D_н \cdot \theta)^2 \cdot \pi D_н^2 / (4 \cdot 2)} =$$

$$= \frac{4 \cdot P_{из} \cdot \tau_з \cdot \tau_{пр} \cdot \tau^2_{ср} \cdot cos\alpha}{\pi (D_н \cdot \theta)^2} \left\{ S_{пл} \cdot \rho_з + \frac{2 \cdot \left[\pi (D_н \cdot \theta)^2 / (4 \cdot \cos\alpha) - S_{пл} \right] \cdot \rho_о \cdot d_o^2}{D_н^2} \right\} \cdot \quad (24)$$

Учитывая, что на практике $S_{пл} \cdot \rho_з >> >> \frac{2 \cdot \left[\pi (D_н \cdot \theta)^2 / (4 \cdot \cos\alpha) - S_{пл} \right] \cdot \rho_о \cdot d_o^2}{D_н^2}$, уравнение (24) запишем в виде:

$$P_c \approx \frac{4 \cdot P_{из} \cdot \tau_л \cdot \tau_{пр} \cdot \tau^2_{ср} \cdot cos\alpha \cdot S_{пл} \cdot \rho_з}{\pi (D_н \cdot \theta)^2}. \quad (25)$$

В общем случае мощность шумов оптического излучения на входе приёмной оптической системы ЛСАРР ($P_ш$) зависит от мощности внутренних шумов приёмника излучения $P_{ш.пи}$ и внешних шумов $P_{ш.вн}$, обусловленных мощностью фонового оптического излучения [17]:

$$P_ш = P_{ш.пи} + P_{швн}. \quad (26)$$

Мощность внутренних шумов приёмника излучения $P_{ш.пи}$, Вт, рассчитаем по формуле [17]

$$P_{ш.пи} = \frac{\sqrt{S_{пи} \cdot \Delta F}}{D^*}, \quad (27)$$

где $S_{пи}$ – площадь приемника оптического излучения, см^2;

ΔF – эквивалентная шумовая полоса частот, Гц;

D^* – удельная обнаружительная способность приёмника излучения, (Вт/см√Гц)$^{-1}$.

В качестве приемника оптического излучения в ЛСАРР используются матричные приемники.

Удельная обнаружительная способность современных приёмников излучения на основе фотодиодов составляет 10^9 – 10^{15} (Вт/см√Гц)$^{-1}$[17].

Эквивалентная шумовая полоса частот ΔF для ЛСАРР, будет определяться, прежде всего частотой сдвига, которая составляет несколько десятков МГц [18]:

$$\Delta F = f_{max} = F + f_{д.max} = F + \frac{2v_{max}}{\lambda}, \quad (28)$$

где v_{max} – максимальная виброскорость на отражающей поверхности, мкм/с;

λ – длины волны излучения лазера, мкм;

F – частота сдвига, Гц;

$f_{д.max}$ – максимальная доплеровская частота, Гц.

Значения виброскорости при громкой речи на различных отражающих поверхностях составляют от 0,1 до 44,6 мкм/с. Некоторые из этих значений приведены в табл. 5 [19].

Мощность внешних шумов ($P_{ш.вн}$), определяемая мощностью фона оптического излучения, попавшего в поле зрения приёмника лазерного излучения, может быть рассчитана по формуле [11]

Таблица 5

Измененные значения виброскорости при громкой речи на различных отражающих поверхностях

Частота, Гц	Уровень звукового давления, дБ	Виброскорость, мкм/с							
		Спинка кожаного кресла	Настольный календарь	Папка канцелярская	Диплом (бумага мелованная)	Бутылка стеклянная	Жалюзи вертикальные (ткань)	Внутреннее стекло стеклопакета	Лист комнатного растения
265	66	15,8	1,6	7,9	44,6	0,5	31,5	12,6	3,2
515	66	2	5	19,9	28,1	0,3	7,9	5,6	5,7
1015	61	10	5,6	2,8	5	0,3	2,8	2	5,9
2015	56	5	0,5	1,4	4	0,1	3,2	0,8	0,8
4015	53	0,2	1	1,1	1,6	0,1	1,6	0,2	1

$$P_{ш.вн} \approx (B_{λф.отр} + B_{λф.соб}) \cdot \Omega \cdot \Delta\lambda \cdot \tau_{пр} \cdot \tau_{ср} =$$

$$= (B_{ф.от} + B_{ф.соб}) \cdot \frac{\pi \cdot d_0^2}{4 \cdot F_0 \cdot D_н} \cdot \Delta\lambda \cdot \tau_{пр} \cdot \tau_{ср}, \quad (29)$$

где $B_{ф.отр}$ – спектральная яркость поверхно-

сти, попадающей в поле зрения приёмника излучения, освещенной внешним излучением, Вт/(м² • мкм • ср);

$B_{ф.соб}$ – спектральная яркость поверхности, попадающей в поле зрения приёмника излучения, обусловленная собственным излучением, Вт/(м² • мкм • ср);

Ω – телесный угол, под которым виден объектив приемника ЛСАРР, рад.;

Δλ – диапазон длин волн, в котором работает приемник оптического излучения, мкм;

F_o – фокусное расстояние объектива приемника излучения ЛСАРР, м;

d_o – диаметр объектива приемника излучения ЛСАРР, м.

Спектральная яркость поверхности, попадающей в поле зрения приёмника излучения, освещенной внешним излучением $B_{λ.ф.отр}$, Вт/(м² • мкм • ср), рассчитывается по формуле [11]

$$B_{\lambda.\text{ф.отр}} = \frac{1}{\pi} \cdot r_\lambda \cdot E_\lambda, \qquad (30)$$

где $E_λ$ – спектральная освещенность поверхности на длине волны λ, Вт/(м² • мкм);

$r_λ$ – спектральный коэффициент яркости поверхности на длине волны λ;

λ – длина волны лазерного излучения, мкм.

Методика расчета спектральной освещенность поверхности $E_λ$ проведена в [66].

Спектральная яркость поверхности, попадающей в поле зрения приёмника излучения, обусловленная собственным излучением $B_{λ.ф.соб}$, Вт/(мкм • м² • ср), рассчитывается по формуле [11]

$$B_{\lambda.\text{ф.соб}} = \frac{\varepsilon_\lambda \cdot {C_1}^*}{\lambda^5 \cdot \left(exp\left(C_2/(\lambda \cdot T)\right) - 1\right)}, \qquad (31)$$

где $ε_λ$ – спектральный коэффициент теплового излучения поверхности на длине волны λ;

T – температура объекта, °K.

C_1 – первая константа излучения, 3,7413 • $• 10^8$Вт • мкм⁴/м²;

C_2 – вторая константа излучения, 1,4388 • $• 10^4$ мкм • K.

$C_1^* = C_1/π = 1{,}1908 • 10^8$, Вт • мкм⁴/(м² • ср).

Величину Δλ , мкм, рассчитаем по формуле

$$\Delta\lambda = \frac{c}{f_o} - \frac{c}{f_o + \Delta F} = \lambda \cdot \left[1 - \frac{1}{1 + \left(F + \frac{2v_{\max}}{\lambda}\right)/f_o}\right] \approx$$

$$\approx \lambda \cdot \left[1 - \frac{1}{1 + F/f_o}\right], \qquad (32)$$

где c – скорость распространения оптического излучения (c = 299 792 458 м/с);

λ – длина волны лазерного излучения, мкм.

f_o – частота, соответствующая длине волны лазерного излучения, Гц.

Полагая, что приемное устройство ЛСАРР работает в линейном режиме и учитывая, что шумы на выходе ЛСАРР, вызванные вибрационными шумами отражающей поверхности, значительно больше собственных шумов низкочастотного тракта ЛСАРР, с учетом формулы (1) отношение сигнал/шум на выходе ЛСАРР можно рассчитать по формуле:

$$q_i = 20\lg\frac{u_c}{u_ш} = 20\lg\frac{k_{чд} \cdot 2v_c \cdot \cos\alpha \cdot \lambda}{\lambda \cdot k_{чд} \cdot 2v_ш \cdot \cos\alpha} =$$

$$= 20\lg\frac{v_c}{v_ш} = 20\lg\frac{a_c \cdot t}{a_ш \cdot t} = a_c^* - a_ш^*, \qquad (33)$$

где q_i – отношение сигнал/шум в i-й октавной полосе на выходе ЛСАРР, дБ;

v_c – виброскорость отражающей поверхности, вызванная воздействием на нее акустического сигнала, мкм/с;

$v_ш$ – виброскорость отражающей поверхности, вызванная воздействием на нее внешних шумов, мкм/с;

a_c – виброускорение отражающей поверхности, вызванное воздействием на нее акустического сигнала, мкм/с²;

$a_ш$ – виброускорение отражающей поверхности, вызванное воздействием на нее внешних шумов, мкм/с²;

a^*_c – виброускорение отражающей поверхности, вызванное воздействием на нее акустического сигнала, дБ;

$a^*_ш$ – виброускорение отражающей поверхности, вызванное воздействием на нее внешних шумов, дБ.

С учетом этого допущения для расчета словесной разборчивости речи ($W_{c.от}$) используем методику, в основу которой положен вероятностный метод оценки разборчивости речи [20, 21].

В соответствие с данной методикой расчет словесной разборчивости речи проводится в следующей последовательности [20, 21]:

1. Измеряются уровни информативного сигнала a^*_c и шума $a^*_ш$ на отражающей поверхности в точке отражения лазерного излучения, и рассчитываются отношения сигнал/шум q_i в каждой из пяти октавных полос $Δf_i$ (i = 2–6), характеристики которых приведены в табл. 6:

$$q_i = a^*_{c.i} - a^*_{ш.i}. \quad (34)$$

2. Рассчитывается вероятность слышимости звуков речи $P(\Delta f_i)$ в каждой из пяти октавных полос:

$$P(\Delta f_i) \approx \Phi(Q_{1.i} \cdot q_i - Q_{2.i}), \quad (35)$$

где $\Phi(x) = \frac{1}{2\pi} \int_{-\infty}^{x} e^{-\frac{t^2}{2}} \cdot dt$ – интеграл вероятности;

q_i – отношение сигнал/шум в i-й октавной полосе, дБ;

$Q_{1.i}$ и $Q_{2.i}$ – коэффициенты, зависящие от вида сигнала, вида шума и индивидуальных особенностей аудиторов (табл. 7).

3. Рассчитываются вероятности каждой из 32-х комбинаций октавных полос A_j, в которых оператор может услышать звуки речи $P(A_j)$ (табл. 8).

4. Для каждой комбинации A_j рассчитывается словесная разборчивость речи W_j при условии, что оператор услышит звуки речи в A_j комбинации, по формуле:

$$W_j = P(A_j) \cdot P(W \mid A_j), \quad (36)$$

где $P(W|A_j)$ – вероятность того, что оператор правильно распознает все слова текста при условии, что он услышит звуки речи в A_j комбинации (значения $P(W|A_j)$ приведены в табл. 9).

5. Рассчитывается словесная разборчивость речи W_c по формуле:

$$W_c = \sum_{j=1}^{M} W_j, \quad (37)$$

где N – количество сочетаний (комбинаций) октавных полос ($N = 2^M = 32$)

M – количество октавных полос ($M = 5$).

Таблица 6

Характеристики речевого сигнала в октавных полосах

Номер полосы, i	Среднегеометрическая частота полосы, f_i, Гц	Границы октавной полосы частот, Гц	Типовые уровни речи I_{ci}, измеренные на расстоянии 1 м от источника сигнала, дБ			
			$L_c = 64$	$L_c = 70$	$L_c = 76$	$L_c = 84$
1	125	90 – 175	47	53	59	67
2	250	175 – 350	60	66	72	80
3	500	350 – 700	60	66	72	80
4	1000	700 – 1400	55	61	67	75
5	2000	1400 – 2800	50	56	62	70
6	4000	2800 – 5600	47	53	59	67
7	8000	5600 – 11200	43	49	55	63

Таблица 7

Значения коэффициентов Q_1 и Q_2 в октавных полосах

Номер октавной полосы, i	Коэффициент $Q_{1.i}$	Коэффициент $Q_{2.i}$
2	0,42	– 1,24
3	0,12	– 1,43
4	0,14	– 1,20
5	0,23	– 3,32
6	0,31	– 0,54

Таблица 8

Формулы для расчета вероятности комбинаций октавных полос, в которых оператор может услышать звуки речи

Обозначение сочетания A_j	Включаемые октавные полосы f_i	Формулы для расчета вероятностей $P(A_j)$
A_0	Ø	$[1-P(\Delta f_2)] \times [1- P(\Delta f_3)] \times [1- P(\Delta f_4)] \times [1- P(\Delta f_5)] \times [1-P(\Delta f_6)]$
A_1	Δf_2	$P(\Delta f_2) \times [1- P(\Delta f_3)] \times [1- P(\Delta f_4)] \times [1- P(\Delta f_5)] \times [1-P(\Delta f_6)]$
A_2	Δf_3	$[1-P(\Delta f_2)] \times P(\Delta f_3) \times [1- P(\Delta f_4)] \times [1- P(\Delta f_5)] \times [1-P(\Delta f_6)]$
A_3	Δf_4	$[1-P(\Delta f_2)] \times [1- P(\Delta f_3)] \times P(\Delta f_4) \times [1- P(\Delta f_5)] \times [1-P(\Delta f_6)]$

Окончание табл. 8

Обозначение сочетания A_j	Включаемые октавные полосы f_i	Формулы для расчета вероятностей $P(A_j)$
A_4	Δf_5	$[1 - P(\Delta f_2)] \times [1 - P(\Delta f_3)][1 - P(\Delta f_4)] \times P(\Delta f_5) \times [1 - P(\Delta f_6)]$
A_5	Δf_6	$[1 - P(\Delta f_2)] \times [1 - P(\Delta f_3)] \times [1 - P(\Delta f_4)] \times [1 - P(\Delta f_5)] \times P(\Delta f_6)$
A_6	$\Delta f_2 U \Delta f_3$	$P(\Delta f_2) \times P(\Delta f_3) \times [1 - P(\Delta f_4)] \times [1 - P(\Delta f_5)] \times [1 - P(\Delta f_6)]$
A_7	$\Delta f_2 U \Delta f_4$	$P(\Delta f_2) \times [1 - P(\Delta f_3)] \times P(\Delta f_4) \times [1 - P(\Delta f_5)] \times [1 - P(\Delta f_6)]$
A_8	$\Delta f_2 U \Delta f_5$	$P(\Delta f_2) \times [1 - P(\Delta f_3)] \times [1 - P(\Delta f_4)] \times P(\Delta f_5) \times [1 - P(\Delta f_6)]$
A_9	$\Delta f_2 U \Delta f_6$	$P(\Delta f_2) \times [1 - P(\Delta f_3)] \times [1 - P(\Delta f_4)] \times [1 - P(\Delta f_5)] \times P(\Delta f_6)$
A_{10}	$\Delta f_3 U \Delta f_4$	$[1 - P(\Delta f_2)] \times P(\Delta f_3) \times P(\Delta f_4) \times [1 - P(\Delta f_5)] \times [1 - P(\Delta f_6)]$
A_{11}	$\Delta f_3 U \Delta f_5$	$[1 - P(\Delta f_2)] \times P(\Delta f_3) \times [1 - P(\Delta f_4)] \times P(\Delta f_5) \times [1 - P(\Delta f_6)]$
A_{12}	$\Delta f_3 U \Delta f_6$	$[1 - P(\Delta f_2)] \times P(\Delta f_3) \times [1 - P(\Delta f_4)] \times [1 - P(\Delta f_5)] \times P(\Delta f_6)$
A_{13}	$\Delta f_4 U \Delta f_5$	$[1 - P(\Delta f_2)] \times [1 - P(\Delta f_3)] \times P(\Delta f_4) \times P(\Delta f_5) \times [1 - P(\Delta f_6)]$
A_{14}	$\Delta f_4 U \Delta f_6$	$[1 - P(\Delta f_2)] \times [1 - P(\Delta f_3)] \times P(\Delta f_4) \times [1 - P(\Delta f_5)] \times P(\Delta f_6)$
A_{15}	$\Delta f_5 U \Delta f_6$	$[1 - P(\Delta f_2)] \times [1 - P(\Delta f_3)] \times [1 - P(\Delta f_4)] \times P(\Delta f_5) \times P(\Delta f_6)$
A_{16}	$\Delta f_2 U \Delta f_3 U \Delta f_4$	$P(\Delta f_2) \times P(\Delta f_3) \times P(\Delta f_4) \times [1 - P(\Delta f_5)] \times [1 - P(\Delta f_6)]$
A_{17}	$\Delta f_2 U \Delta f_3 U \Delta f_5$	$P(\Delta f_2) \times P(\Delta f_3) \times [1 - P(\Delta f_4)] \times P(\Delta f_5) \times [1 - P(\Delta f_6)]$
A_{18}	$\Delta f_2 U \Delta f_3 U \Delta f_6$	$P(\Delta f_2) \times (\Delta f_3) \times [1 - P(\Delta f_4)] \times [1 - P(\Delta f_5)] \times P(\Delta f_6)$
A_{19}	$\Delta f_2 U \Delta f_4 U \Delta f_5$	$P(\Delta f_2) \times [1 - P(\Delta f_3)] \times P(\Delta f_4) \times P(\Delta f_5) \times [1 - P(\Delta f_6)]$
A_{20}	$\Delta f_2 U \Delta f_4 U \Delta f_6$	$P(\Delta f_2) \times [1 - P(\Delta f_3)] \times P(\Delta f_4) \times [1 - P(\Delta f_5)] \times P(\Delta f_6)$
A_{21}	$\Delta f_2 U \Delta f_5 U \Delta f_6$	$P(\Delta f_2) \times [1 - P(\Delta f_3)] \times [1 - P(\Delta f_4)] \times P(\Delta f_5) \times P(\Delta f_6)$
A_{22}	$\Delta f_3 U \Delta f_4 U \Delta f_5$	$[1 - P(\Delta f_2)] \times P(\Delta f_3) \times P(\Delta f_4) \times P(\Delta f_5) \times [1 - P(\Delta f_6)]$
A_{23}	$\Delta f_3 U \Delta f_4 U \Delta f_6$	$[1 - P(\Delta f_2)] \times P(\Delta f_3) \times P(\Delta f_4) \times [1 - P(\Delta f_5)] \times P(\Delta f_6)$
A_{24}	$\Delta f_2 U \Delta f_5 U \Delta f_6$	$[1 - P(\Delta f_2)] \times P(\Delta f_3) \times [1 - P(\Delta f_4)] \times P(\Delta f_5) \times P(\Delta f_6)$
A_{25}	$\Delta f_4 U \Delta f_5 U \Delta f_6$	$[1 - P(\Delta f_2)] \times [1 - P(\Delta f_3)] \times P(\Delta f_4) \times P(\Delta f_5) \times P(\Delta f_6)$
A_{26}	$\Delta f_2 U \Delta f_3 U \Delta f_4 U \Delta f_5$	$P(\Delta f_2) \times P(\Delta f_3) \times P(\Delta f_4) \times P(\Delta f_5) \times [1 - P(\Delta f_6)]$
A_{27}	$\Delta f_2 U \Delta f_3 U \Delta f_4 U \Delta f_6$	$P(\Delta f_2) \times P(\Delta f_3) \times P(\Delta f_4) \times [1 - P(\Delta f_5)] \times P(\Delta f_6)$
A_{28}	$\Delta f_2 U \Delta f_3 U \Delta f_5 U \Delta f_6$	$P(\Delta f_2) \times P(\Delta f_3) \times [1 - P(\Delta f_4)] \times P(\Delta f_5) \times P(\Delta f_6)$
A_{29}	$\Delta f_2 U \Delta f_4 U \Delta f_5 U \Delta f_6$	$P(\Delta f_2) \times [1 - P(\Delta f_3)] \times P(\Delta f_4) \times P(\Delta f_5) \times P(\Delta f_6)$
A_{30}	$\Delta f_3 U \Delta f_4 U \Delta f_5 U \Delta f_6$	$[1 - P(\Delta f_2)] \times P(\Delta f_3) \times P(\Delta f_4) \times P(\Delta f_5) \times P(\Delta f_6)$
A_{31}	$\Delta f_2 U \Delta f_3 U \Delta f_4 U \Delta f_5 U \Delta f_6$	$P(\Delta f_2) \times P(\Delta f_3) \times P(\Delta f_4) \times P(\Delta f_5) \times P(\Delta f_6)$

Таблица 9

Вероятность распознавания слов для различных сочетаний октавных полос (рассчитанная по результатам артикуляционных испытаний)

Обозначение сочетания A_j	Включаемые октавные полосы f_i	Вероятность распознавания слов $P(W\|A_j)$
A_0	Ø	0
A_1	Δf2	0,006
A_2	Δf3	0,082
A_3	Δf4	0,149
A_4	Δf5	0,132
A_5	Δf6	0,066
A_6	Δf2UΔf3	0,302

Окончание табл. 9

Обозначение сочетания A_j	Включаемые октавные полосы f_i	Вероятность распознавания слов $P(W\|A_j)$
A_7	$\Delta f_2 U \Delta f_4$	0,435
A_8	$\Delta f_2 U \Delta f_5$	0,527
A_9	$\Delta f_2 U \Delta f_6$	0,313
A_{10}	$\Delta f_3 U \Delta f_4$	0,448
A_{11}	$\Delta f_3 U \Delta f5$	0,781
A_{12}	$\Delta f_3 U \Delta f_6$	0,692
A_{13}	$\Delta f_4 U \Delta f_5$	0,781
A_{14}	$\Delta f_4 U \Delta f_6$	0,732
A_{15}	$\Delta f_5 U \Delta f_6$	0,675
A_{16}	$\Delta f_2 U \Delta f_3 U \Delta f_4$	0,668
A_{17}	$\Delta f_2 U \Delta f_3 U \Delta f_5$	0,864
A_{18}	$\Delta f_2 U \Delta f_3 U \Delta f_6$	0,811
A_{19}	$\Delta f_2 U \Delta f_4 U \Delta f_5$	0,882
A_{20}	$\Delta f_2 U \Delta f_4 U \Delta f_6$	0,890
A_{21}	$\Delta f_2 U \Delta f_5 U \Delta f_6$	0,705
A_{22}	$\Delta f_3 U \Delta f_4 U \Delta f_5$	0,889
A_{23}	$\Delta f_3 U \Delta f_4 U \Delta f_6$	0,887
A_{24}	$\Delta f_2 U \Delta f_5 U \Delta f_6$	0,901
A_{25}	$\Delta f_4 U \Delta f_5 U \Delta f_6$	0,906
A_{26}	$\Delta f_2 U \Delta f_3 U \Delta f_4 U \Delta f_5$	0,934
A_{27}	$\Delta f_2 U \Delta f_3 U \Delta f_4 U \Delta f_6$	0,917
A_{28}	$\Delta f_2 U \Delta f_3 U \Delta f_5 U \Delta f_6$	0,926
A_{29}	$\Delta f_2 U \Delta f_4 U \Delta f_5 U \Delta f_6$	0,927
A_{30}	$\Delta f_3 U \Delta f_4 U \Delta f_5 U \Delta f_6$	0,940
A_{31}	$\Delta f_2 U \Delta f_3 U \Delta f_4 U \Delta f_5 U \Delta f_6$	1,000

Разработанная математическая модель акустооптического канала утечки речевой информации может быть положена в основу инструментально-расчетной методики оценки эффективности защиты речевой информации от утечки по акустооптическому каналу.

Литература

1. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. – М.: НПЦ «Аналитика», 2008 – 436 с.

2. Лысов А.В. Оптические системы зондирования акустически возбужденных поверхностей (Лазерные системы акустической разведки). – СПб.: Медиапапир, 2020. – 512 с.

3. Григорьев И.А., Тупота В.И. Разработка модели оптико-электронного канала утечки акустической речевой информации//Вестник воронежского государственного технического университета. – Воронеж, 2010. – № 2. – С. 85–87.

4. Авдеев В.Б., Анищенко А.В., Петигин А.Ф., Денисенко Н.Г. Методический подход к оценке дальности действия лазерного микрофона//Телекоммуникации. – Москва, 2022. - № 1. – С. 10 – 20.

5. Железняк В.К., Чернова И.С. Оценка модели оптико-электронного канала утечки речевой информации// Вестник Полоцкого государственного университета. Серия С, Фундаментальные науки. – Полоцк, 2015. – № 12. – С. 33–39

6. Глущенко Л.А., Нырков А.П., Швед Д.В. Применение корреляционного подхода к определению качества речевой информации, зарегистрированной лазерным микрофоном//Вестник государственного университета морского и речного флота им. адмирала С.О. Макарова. – С. Петербург, 2015. – № 6 (34). – С. 187–195.

7. Суровенков Д.Б., Хорев А.А., Рудченко Е.С., Савин А.Д. Анализ возможностей использования лазерных виброметров для перехвата акустической речевой информации // Международная конференция «Радиоэлектронные устройства и системы для инфотелекоммуникационных технологий – РЭУС-2020». Доклады. – М.: РНТОРЭС имени А.С.Попова. 2020. – С. 249 – 253.

8. Aufbau eines Scanning- Laservibrometers zur Visualisierung schwingender Oberflächen. [Электронный ресурс]. – Режим доступа: http://www.akustik.uni-oldenburg.de/literatur/Asendorf/Tobias_Asendorf_Laservibrometer.pdf, свободный (дата обращения 12.03.2023).

9. Milena Martarelli. Exploiting the Laser Scanning Facility for Vibration Measurements. A thesis submitted to the University of London for the degree of Doctor of Philosophy. - Imperial College of Science, Technology & Medicine University of London, 2001. [Электронный ресурс] – URL: https://www.imperial.ac.uk/media/imperial-college/research-centres-and-groups/dynamics/40373700.PDF (дата обращения: 12.03.2023).

10. VibroMet 500V: руководство пользователя. [Электронный ресурс] – URL: https://t-holding.ru/docs/files/VibroMet-500V-User-Manual-Rev-60-rus-1.pdf (дата обращения 12.03.2023).

11. Хорев А.А. Теоретические основы оценки возможностей технических средств разведки: Монография. – М.: МО РФ, 2000. – 255 с.

12. Минипризма EXTRA-SET GEOBOX. [Электронный ресурс]. – URL:https://www.aspector.ru/product/miniprizma-extra-set-geobox/. (дата обращения: 12.03.2023).

13. Триппель-призма GCL-0305. [Электронный ресурс]. – URL: https://lasercomponents.ru/product/optika/prizmy/trippel-prizma-gcl-0305/ (дата обращения: 12.03.2023)

14. Световозвращающие пленки на полимерной основе (обзор) [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/svetovozvraschayuschie-plenki-na-polimernoy-osnove-obzor/viewer (дата обращения: 12.03.2023).

15. Плёночные отражатели. [Электронный ресурс]. – URL:https://www.aspector.ru/category/plyonochnye-otrazhateli/ (дата обращения: 12.03.2023).

16. Отражатель пленочный ОП30/ОП50. [Электронный ресурс]. – URL: https://www.gsi.ru/catalog/other/op50 (дата обращения: 12.03.2023)

17. Гарнов С.В., Моисеева А.В., Носатенко П.Я., Фомин В.Н., Церевитинов А.Б. Оценка характеристик перспективного орбитального лазерного локатора для мониторинга космического мусора [Электронный ресурс]. – Режим доступа: https://old.gpi.ru/trudiof/Vol_70/page_26_70.pdf, свободный (дата обращения: 12.03.2023).

18. Aufbau eines Scanning- Laservibrometers zur Visualisierung schwingender Oberflächen. [Электронный ресурс]. – Режим доступа: http://www.akustik.uni-oldenburg.de/literatur/Asendorf/Tobias_Asendorf_Laservibrometer.pdf, свободный (дата обращения 12.03.2023).

19. Лысов А.В., Лысов В.В. Параметры типовых акустооптических модуляторов, используемых лазерными системами акустической разведки // Защита информации. Инсайд. – С. Петербург: 2020. – № 2 – С. 53 – 57.

20. Хорев А.А., Порсев И.С. Методика вероятностной оценки разборчивости речи //Защита информации. Инсайд. – С. Петербург: 2020. – № 2 – С. 44 – 52.

21. Хорев А.А., Порсев И.С. Методика вероятностной оценки разборчивости речи// XXVI Научно – практическая конференция «Комплексная защита информации» г. Минск, 25-27 мая 2021 г. – Минск: Издатель Владимир Сивчиков, 2021. – С. 53 – 58. ISBN 978-985-7030-87-3.

References

1. Khorev A.A. Tekhnicheskaya zashchita informatsii: ucheb. posobiye dlya studentov vuzov. V 3-kh t. T. 1. Tekhnicheskiye kanaly utechki informatsii. – M.: NPTS «Analitika», 2008 – 436 s.

2. Lysov A.V. Opticheskiye sistemy zondirovaniya akusticheski vozbuzhdennykh poverkhnostey (Lazernyye sistemy akusticheskoy razvedki). – SPb.: Mediapapir, 2020. – 512 s.

3. Grigor'yev I.A., Tupota V.I. Razrabotka modeli optiko-elektronnogo kanala utechki akusticheskoy rechevoy informatsii//Vestnik voronezhskogo gosudarstvennogo tekhnicheskogo universiteta. – Voronezh, 2010. – № 2. – C. 85–87.

4. Avdeyev V.B., Anishchenko A.V., Petigin A.F., Denisenko N.G. Metodicheskiy podkhod k otsenke dal'nosti deystviya lazernogo mikrofona//Telekommunikatsii. – Moskva, 2022. - № 1. – S. 10 – 20.

5. Zheleznyak V.K., Chernova I.S. Otsenka modeli optiko-elektronnogo kanala utechki rechevoy informatsii// Vestnik Polotskogo gosudarstvennogo universiteta. Seriya C, Fundamental'nyye nauki. – Polotsk, 2015. – № 12. – C. 33–39.

6. Glushchenko L.A., Nyrkov A.P., Shved D.V. Primeneniye korrelyatsionnogo podkhoda k opredeleniyu kachestva rechevoy informatsii, zaregistrirovannoy lazernym mikrofonom//Vestnik gosudarstvennogo

universiteta morskogo i rechnogo flota im. admirala S.O. Makarova. – S. Peterburg, 2015. – № 6 (34). – S. 187–195.

7. Surovenkov D.B., Khorev A.A., Rudchenko Ye.S., Savin A.D. Analiz vozmozhnostey ispol'zovaniya lazernykh vibrometrov dlya perekhvata akusticheskoy rechevoy informatsii // Mezhdunarodnaya konferentsiya «Radioelektronnyye ustroystva i sistemy dlya infotelekommunikatsionnykh tekhnologiy – REUS-2020». Doklady. – M.: RNTORES imeni A.S.Popova. 2020. – S. 249 – 253.

8. Aufbau eines Scanning- Laservibrometers zur Visualisierung schwingender Oberflächen. [Electronic resource]. – Access mode: http://www.akustik.uni-oldenburg.de/literatur/Asendorf/Tobias_Asendorf_Laservibrometer.pdf, free (accessed 03/12/2023).

9.Milena Martarelli. Exploiting the Laser Scanning Facility for Vibration Measurements. A thesis submitted to the University of London for the degree of Doctor of Philosophy. - Imperial College of Science, Technology & Medicine University of London, 2001. [Electronic resource] – URL: https://www.imperial.ac.uk/media/imperial-college/research-centres-and-groups/dynamics/40373700.PDF (accessed: 12.03.2023).

10.VibroMet 500V: user guide. [Electronic resource] – URL: https://t-holding.ru/docs/files/VibroMet-500V-User-Manual-Rev-60-rus-1.pdf (accessed12.03.2023).

11. Khorev A.A. Teoreticheskiye osnovy otsenki vozmozhnostey tekhnicheskikh sredstv razvedki: Monografiya. – M.: MO RF, 2000. – 255 s.

12. Miniprizma EXTRA-SET GEOBOX. [Elektronnyy resurs]. – URL:https://www.aspector.ru/product/miniprizma-extra-set-geobox/. (data obrashcheniya: 12.03.2023).

13. Trippel'-prizma GCL-0305. [Elektronnyy resurs]. – URL: https://lasercomponents.ru/product/optika/prizmy/trippel-prizma-gcl-0305/ (data obrashcheniya: 12.03.2023).

14. Svetovozvrashchayushchiye plenki na polimernoy osnove (obzor) [Elektronnyy resurs]. – URL: https://cyberleninka.ru/article/n/svetovozvraschayuschie-plenki-na-polimernoy-osnove-obzor/viewer (data obrashcheniya: 12.03.2023).

15. Plonochnyye otrazhateli. [Elektronnyy resurs]. – URL:https://www.aspector.ru/category/plyonochnye-otrazhateli/ (data obrashcheniya: 12.03.2023).

16. Otrazhatel' plenochnyy OP30/OP50. [Elektronnyy resurs]. – URL: https://www.gsi.ru/catalog/other/op50 (data obrashcheniya: 12.03.2023).

17. Garnov S.V., Moiseyeva A.V., Nosatenko P.YA., Fomin V.N., Tserevitinov A.B. Otsenka kharakteristik perspektivnogo orbital'nogo lazernogo lokatora dlya monitoringa kosmicheskogo musora [Elektronnyy resurs]. – Rezhim dostupa: https://old.gpi.ru/trudiof/Vol_70/page_26_70.pdf, svobodnyy (data obrashcheniya: 12.03.2023).

18. Aufbau eines Scanning- Laservibrometers zur Visualisierung schwingender Oberflächen. [Электронный ресурс]. – Режим доступа: http://www.akustik.uni-oldenburg.de/literatur/Asendorf/Tobias_Asendorf_Laservibrometer.pdf, свободный (дата обращения 12.03.2023).

19. Lysov A.V., Lysov V.V. Parametry tipovykh akustoopticheskikh modulyatorov, ispol'zuyemykh lazernymi sistemami akusticheskoy razvedki // Zashchita informatsii. Insayd. – S. Peterburg: 2020. – № 2 – S. 53 – 57.

20. Khorev A.A., Porsev I.S. Metodika veroyatnostnoy otsenki razborchivosti rechi //Zashchita informatsii. Insayd. – S. Peterburg: 2020. – № 2 – S. 44 – 52.

21. Khorev A.A., Porsev I.S. Metodika veroyatnostnoy otsenki razborchivosti rechi// XKHVI Nauchno – prakticheskaya konferentsiya «Kompleksnaya zashchita informatsii» g. Minsk, 25-27 maya 2021 g. – Minsk: Izdatel' Vladimir Sivchikov, 2021. – S. 53 - 58. ISBN 978-985-7030-87-3.

ХОРЕВ Анатолий Анатольевич, доктор технических наук, профессор, заведующий кафедрой «Информационная безопасность», «Национальный исследовательский университет «МИЭТ». 124498, г. Москва, г. Зеленоград, площадь Шокина, дом 1, МИЭТ. E-mail: horev@miee.ru

HOREV Anatoly Anatolevich, doctor of technical Sciences, Professor, head of the Department «Information security», National Research University of Electronic Technology. 124498, Moscow, Zelenograd, Shokin square, house 1, MIET. E-mail: horev@miee.ru

УДК 004.056.5 Вестник УрФО № 1(47) / 2023, с. 43–50

Акбулякова Л.М., Шабуров А.С.

DOI: 10.14529/secur230104

О СОВЕРШЕНСТВОВАНИИ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ВЗАИМОДЕЙСТВИИ ОПЕРАТОРА С РЕГИОНАЛЬНЫМ СЕГМЕНТОМ «ЕГИС3»

В статье рассматривается решение по модернизации защиты информационной системы персональных данных, с целью устранения ее уязвимостей при информационном взаимодействии. Сформулирована проблема поиска оптимальных решений по обеспечению информационной безопасности при централизованной обработке данных. Определены наиболее уязвимые процессы действующей информационной системы персональных данных. Проанализированы применяемые методы и средства защиты информации, удовлетворяющие требованиям при взаимодействии с «ЕГИС3». Предложено решение по устранению выявленных уязвимостей на основе открытого программного обеспечения. Проведена оценка эффективности внедрения программного обеспечения на основе выбранных показателей эффективности.

Ключевые слова: *центр обработки данных, защита информации, информационная система персональных данных, демилиторизированная зона, показатель эффективности.*

ON IMPROVEMENT OF THE SYSTEM OF PROTECTION OF PER-SONAL DATA IN THE INTERACTION OF THE OPERATOR WITH THE REGIONAL SEGMENT «EGISZ»

The article discusses the decision to modernize the protection of the infor-mation system of personal data, in order to eliminate its vulnerabilities during in-formation interaction. The problem of finding optimal solutions to ensure infor-mation security in the case of centralized data processing is formulated. The most vulnerable processes of the current information system of personal data are deter-mined. The applied methods and means of information protection that meet the re-quirements when interacting with the EGISZ are analyzed. A solution is proposed to eliminate the identified vulnerabilities using Elastic Stack. An assessment of the ef-fectiveness of the implementation of information security tools was carried out by comparing performance indicators.

Keywords: *data processing center, information security, personal data infor-mation system, demilitarized zone, performance indicator.*

Повсеместное внедрение единых центров обработки данных (ЦОД) позволяет обеспечить качественно более совершенный набор сервисов информационного обеспечения, повысить оперативность информационного обмена, обеспечить множество иных преимуществ. Кроме того, подобные решения информационных систем предполагают внедрение новых, эффективных моделей и методов обеспечения информационной безопасности. В тоже время, способы проникновения вредоносной информации в подобные информационные системы также может модифицироваться, что предполагает поиска и применения как новых средств и методов защиты, так и оптимизации архитектуры информационных систем. Например, совершенствование архитектуры информационного взаимодействия оператора ИСПДн с Единой государственной информационной системой в сфере здравоохранения (ЕГИСЗ), позволяет повысить эффективность обеспечения защиты информации, при этом, обеспечивая выполнение заданных характеристик самой системы [1, 2]. В то же время, развитие процессов информационного взаимодействия требует поиска новых, более совершенных решений по защите информации. Это особенно важно в условиях роста количества и сложности кибератак, прекращения функционирования и ухода с российского рынка отдельных поставщиков информационных услуг, а также временных и финансовых ограничений.

При разработке средств, методов и мероприятий обеспечения информационной безопасности необходимо учитывать большое количество различных факторов: возможные источники угроз, уязвимости, ценность информации, которую необходимо защищать, техническая оснащенность объекта информатизации и т.д. В данной работе в качестве объекта защиты информации рассмотрена информационная система персональных данных (ИСПДн), предназначенная для обработки данных при взаимодействия оператора ИСПДн с ЕГИСЗ (рис. 1).

Цель исследования заключалась в поиске

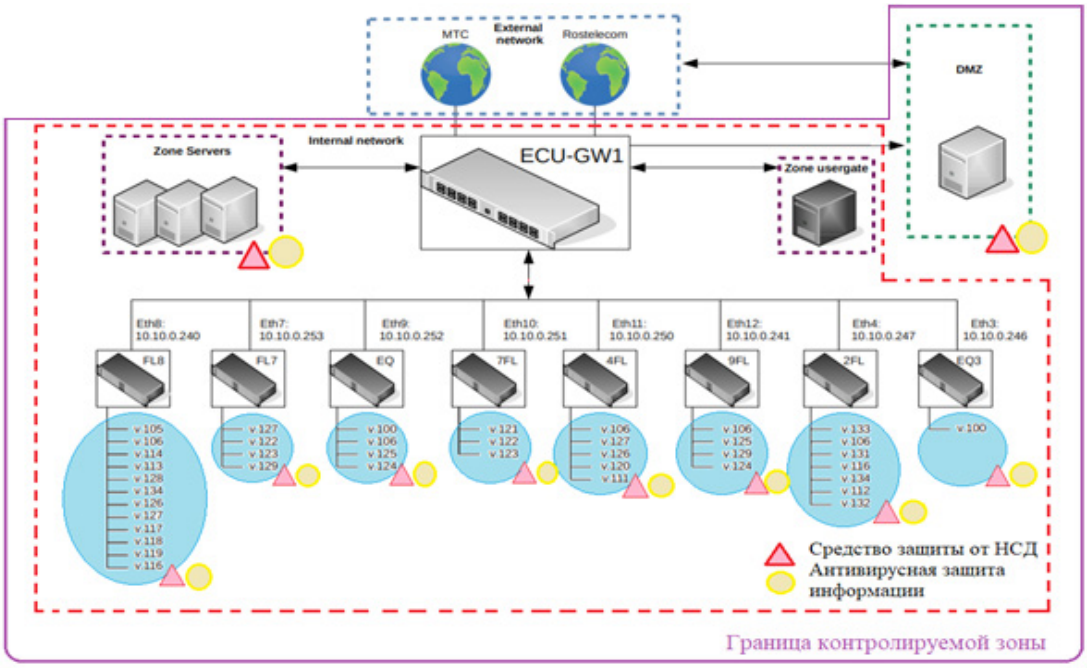


Рис. 1. Структурная схема оъекта защиты

оптимальных решений по обеспечению информационной безопасности ИСПДн, за счет определения характеристик внедренной системы защиты информации, установление взаимосвязей между ее характеристиками и показателями эффективности защиты в отдельных аспектах информауионной безпасности.

Особенностью реализованной структуры СЗИ является разделение защищаемой сети на несколько вланов, что позволяет логически ограничивать сетевое взаимодействие между автоматизированными рабочими местами (АРМ), выполняеющих различные функции. В структуре сети предусмотрена демилиторизированная зона (ДМЗ), в которой размещается веб-сервер объекта защиты, имеющий прямой и обратный доступ к внешней сети, но ограниченый по взаимодействию с внутренней сетью организации. Подобная конфигурация направлена на усиление безопасности внутренней сети организации, в которой открытые для общего доступа сервера находятся в отдельном изолированном сегменте. Данная концепция обеспечивает отсутствие контактов между открытыми для общего доступа серверами и другими сегментами сети в случае несанкционированного доступа к серверу.

Применение UserGate, как основного средства защиты инфмации, представляещего собой универсальный шлюз, объединяющий межсетевой экран, маршрутизацию, шлюзовой антивирус, систему обнаружения и предотвращения вторжений, систему фильтрации, модуль мониторинга и статистики и многие другие функции позволяет реализовать основные требования по обеспечению безопасности информации для ИСПДн [3]. Анализ функционирования данного средства ЗИ позволяет сделать вывод о достаточно эффективном управлении информационной безопасностью информационной системы, оптимизировать трафик информационного взаимодействия, и эффективно предотвращать основные угрозы безопасности информации.

В качестве средства защиты информации от несанкционированного доступа (НСД) применяется Secret Net Studio и технология ViPNet, как комплексное решение для защиты рабочих станций и серверов на уровне данных, приложений, сети, операционной системы и периферийного оборудования. Программно-аппаратные средства позволяют эффективно блокировать неавторизованных пользователей, а технические средства предназначены для исключения физического проникновения посторонних субъектов в пределы контролируемой зоны [4].

Антивирусная защита организована на основе внедрения программного антивирусного средства Dr.Web, что обеспечивает выявление широкого спектра вредоносных

программ, восстановления поврежденных файлов, предохранение операционной системы или отдельных файлов от заражения.

Взаимодействие четырех сегментов сети необходимо осуществляется внутри контролируемой зоны объекта и обеспечивается средствами защиты от НСД, а также средствами антивирусной средство защиты информации. Детализированная схема взаимодействия сети на основе разделения на изолированные сегменты, с применением средств защиты информации представлена на рис. 2.

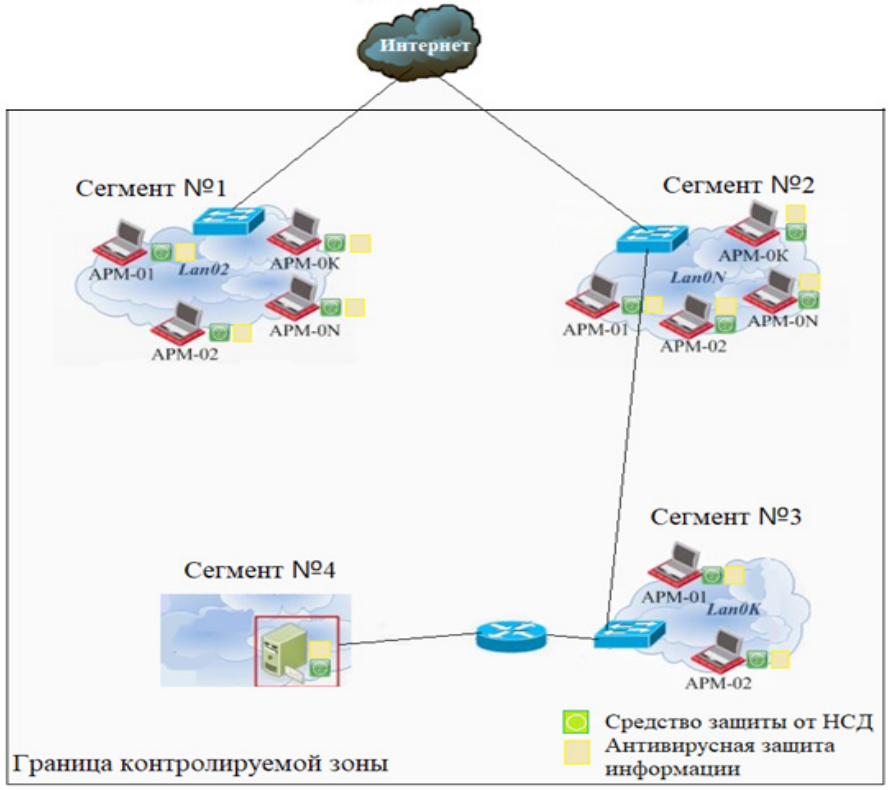


Рис. 2. Схема взаимодействия сегментов сети

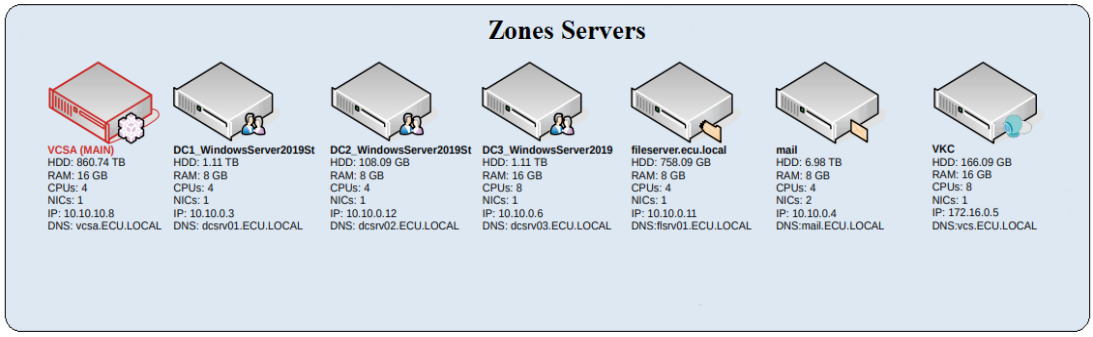


Рис. 3. Зона серверного оборудования объекта защиты

Функционирование объекта защиты осуществляется на основе специализированного серверного оборудования структурно объединенных в зону серверов (рис. 3).

В зону серверного оборудования входят семь серверных станций, выполняющих основные функции по обработке данных, такие как: контроль и создание учетных записей, хранение информации объекта информатизации, почтовое взаимодействие, организация физической защиты информации, а также взаимодействие по видеосвязи [5].

В процессе плановой эксплуатации ИСПДн была выявлена уязвимость сервера электронной почты Zimbra, работающего с использованием пакета программного обе-

спечения для совместной работы. Уязвимость заключалась в значительном количестве несанкционированных запросов, что в конечном итоге могло способствовать реализации угрозы типа «отказ в обслуживании».

Для предотвращения выявленной уязвимости было использовано программное обеспечение с открытым исходным кодом ElasticStack с помощью сервиса централизованного ведения журнала на основе Rsyslog. В частности, были установлены центральный сервер ведения журналов и эластичный стек, обновления. В этом журнале был настроен сервер RSyslog для принудительного использования TLS. Также были разработаны сертификаты TLS для сервера и клиента Rsyslog.

Для корректной работы сервера Rsyslog потребовалась его настройка, в соответствии с глобальными директивами. Данная конфигурация необходима для применения шифрования TLS и аутентификации в RSyslog и обеспечивает доступ на почтовый сервер только доверенных клиентов.

В целях визуализации оценки эффективности принятого решения было использовано программное обеспечение с открытым исходным кодом, позволившее провести анализ журналов и временных рядов, а также мониторинг приложений и текущих процессов.

Выбор необходимых компонентов программного обеспечения и их настроек позволил проанализировать несанкционированные попытки входа в информационную систему. Для этого с помощью журнала регистрации событий было выявлено, что за 1.5 минуты были осуществлены 3 несанкционированные попытки входа в систему через пользовательские учетные записи. На основе детального анализа логов были выделены соответствующие ip-адреса за экспериментальный промежуток времени. В результате эксперимента были выявлены несанкционированные попытки входа в систему со 190 посторонних ip-адресов. Подобная статистика не является критичной, но при определенных обстоятельствах может привести к перегрузке серверного оборудования из-за возрастания очереди запросов.

Рис. 4. Результат оценки несанкционированных попыток доступа

На рис. 5 представлено графическое представление результатов анализа логов несанкционированного входа в информационную систему.

Для оценки эффективности предлагаемого решения отслеживалось состояние всех процессов, происходящих на сервере. В качестве основных показателей эффективности обеспечения безопасного взаимодействия были выбраны:

1) t – промежуток времени, за которое происходят попытки входа в систему;

2) p – количество неуспешных попыток входа в систему;

3) i – количество ip-адресов, посредством которых происходят несанкционированные доступы в систему.

За экспериментальный период продолжительностью 7 дней были проведены контрольные оценки выбранных показателей

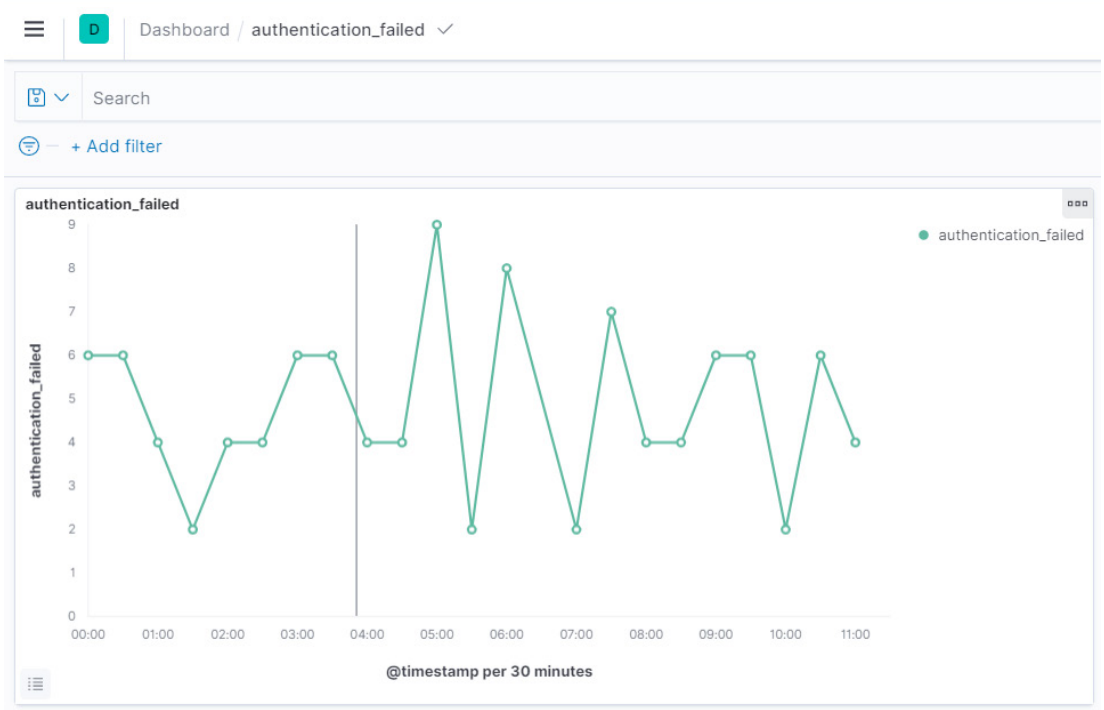


Рис. 5. Анализ логов несанкционированного входа в систему

эффективности без учета применения и с применением программного обеспечения ElasticStack. Результаты контрольных оценок представлены в таблицах 1–3.

Таблица 1

Значения показателя t

n	Значение t до внедрения (ч)	Значение t после внедрения (ч)
1	0,33	4,5
2	0,33	5,5
3	0,5	6,5
4	0,5	4,5
5	0,67	5,5
6	0,67	7,5
7	0,67	7,5

Таблица 2

Значения показателя p

n	Значение p до внедрения	Значение p после внедрения
1	193	6
2	205	5
3	217	4
4	208	6
5	211	5
6	220	3
7	231	3

Количественное сравнение неуспешных попыток входа в систему и ip-адресов, с помощью которых происходят несанкционированные входы в систему до и после внедрения ElasticStack за экспериментальный период представлен на рис. 6.

Таблица 3

Значения показателя i

n	Значение i до внедрения	Значение i после внедрения
1	190	5
2	200	4
3	215	4
4	207	5
5	210	4
6	220	3
7	230	3

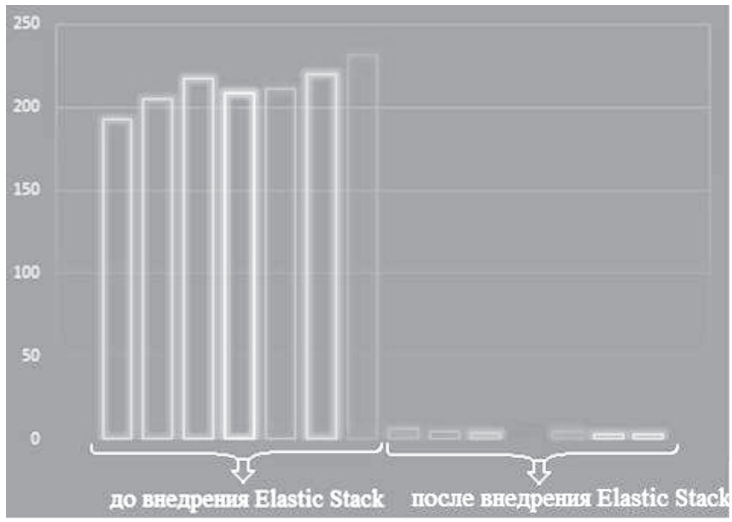


Рис. 6. Количественное сравнение неуспешных попыток входа в систему

Анализ полученных данных показывает, что после блокирования ip-адресов с помощью которых происходят попытки доступа, значительно уменьшается количество неуспешных попыток несанкционированного входа в информационную систему. В свою очередь, значение показателя t -промежуток времени, за которое происходят попытки входа в систему, наоборот возрастает, что также свидетельствует об уменьшении количества попыток несанкционированного доступа и эффективности предлагаемого решения.

Таким образом, на основе внедрения программного обеспечения ElasticStack была решена задача блокирования потенциально опасных ip-адресов, уменьшения нагрузки на серверное оборудование и всю информационную систему, что способствует уменьшению вероятности угроз безопасности информации в ИСПДн. Данное решение может являться временным, с учетом требований по импортозамещению. В то же время, в отдельных ситуациях подобные решения позволяют повышать эффективность обеспечения информационной безопасности за счет свободно распространяемого программного обеспечения, в сочетании с применением штатных методов и средств защиты информации, в том числе и при взаимодействии оператора ИСПДн с региональным сегментом ЕГИСЗ.

Литература

1. Акбулякова Л.М., Шабуров А.С. «О совершенствовании архитектуры информационной системы персональных данных при взаимодействии оператора с сегментом «ЕГИСЗ»// Вестник УрФО. Безопасность в информационной сфере. 2021. № 4(42). С 15–23.

2. Постановление правительства Российской Федерации от 09.02.2022 № 140 «О единой государственной информационной системе в сфере здравоохранения (ЕГИСЗ)»

3. Методические рекомендации медицинским организациям по организации криптографической защиты каналов при взаимодействии в рамках единой государственной информационной системы в сфере здравоохранения: официальный сайт. – Москва. – 2018. – URL: https://portal.egisz.rosminzdrav.ru (дата обращения 15.11.2022).

4. Решения по комплексному обеспечению информационной безопасности в ЕГИСЗ: официальный сайт. – Москва. – 2019. – URL: https://portal.egisz.rosminzdrav.ru (дата обращения 15.11.2022).

5. Техническое задание «Оказание услуги комплексного сервиса в целях обеспечения сервисной поддержки функционирования медицинской организации в рамках регионального сегмента единой государственной информационной системы в сфере здравоохранения»: официальный сайт. – Москва. - 2020. - URL: https://vkr.pspu.ru/uploads (дата обращения 20.11.2022).

References

1. Akbulyakova L.M., SHaburov A.S. «O sovershenstvovanii arhitektury informacionnoj sistemy personal'nyh dannyh pri vzaimodejstvii operatora s segmentom «EGISZ»// Vestnik UrFO. Bezopasnost' v informacionnoj sfere. 2021. № 4(42). S 15–23.

2. Postanovlenie pravitel'stva Rossijskoj Federacii ot 09.02.2022 № 140 «O edinoj gosudarstvennoj informacionnoj sisteme v sfere zdravoohrane-niya (EGISZ)»

3. Metodicheskie rekomendacii medicinskim organizaciyam po organizacii kriptograficheskoj zashchity kanalov pri vzaimodejstvii v ramkah edinoj gosudarstvennoj informacionnoj sistemy v sfere zdravoohraneniya: oficial'nyj sajt. – Moskva. – 2018. – URL: https://portal.egisz.rosminzdrav.ru (data obrashche-niya 15.11.2022).

4. Resheniya po kompleksnomu obespecheniyu informacionnoj bezopasnosti v EGISZ: oficial'nyj sajt. – Moskva. – 2019. – URL: https://portal.egisz.rosminzdrav.ru (data obrashcheniya 15.11.2022).

5. Tekhnicheskoe zadanie «Okazanie uslugi kompleksnogo servisa v celyah obespecheniya servisnoj podderzhki funkcionirovaniya medicinskoj organizacii v ramkah regional'nogo segmenta edinoj gosudarstvennoj informacionnoj sistemy v sfere zdravoohraneniya»:oficial'nyj sajt. – Moskva. – 2020. – URL: https://vkr.pspu.ru/uploads (data obrashcheniya 15.11.2021).

ШАБУРОВ Андрей Сергеевич, кандидат технических наук, доцент, доцент кафедры автоматики и телемеханики, Пермский национальный исследовательский политехнический университет. Россия, 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: shans@at.pstu.ru

АКБУЛЯКОВА Лилия Маратовна, студент, Пермский национальный исследовательский политехнический университет. Россия, 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: akbulyakowa@mail.ru

SHABUROV Andrey Sergeevich, Candidate of Technical Sciences, Associate Professor of the Department of Automation and Telemechanics. Perm National Research Polytechnic University. 614990, Perm, Komsomolsky Ave, 29. E-mail: shans@at.pstu.ru

AKBULYAKOVA Liliya Maratovna, student, Department of Automation and Telemechanics. Perm National Research Polytechnic University. 614990, Perm, Komsomolsky Ave, 29. E-mail: akbulyakowa@mail.ru

УДК 004.056.5 Вестник УрФО № 1(47) / 2023, с. 51–58

Афанасьева С.В., Кузьмина У.В.

DOI: 10.14529/secur230105

ОСНОВНЫЕ ПРОБЛЕМЫ ПРИ РАБОТЕ С ЦЕНТРАМИ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В настоящее время количество киберугроз постоянно увеличивается, а их техники и тактики совершенствуются. Для мониторинга, обнаружения, а также последующего реагирования на инциденты информационной безопасности организации создают Security Operation Center (далее - SOC) или центры мониторинга информационной безопасности. В данной статье рассматриваются важные проблемы, с которыми сталкиваются IT-специалисты при работе с центрами мониторинга информационной безопасности. Подробный анализ этих проблем позволит начинающим специалистам не допускать ошибок при работе с центрами мониторинга информационной безопасности, а для опытных специалистов станет вектором движения при улучшении центров мониторинга.

Ключевые слова: *информационная безопасность, SOC, центр мониторинга информационной безопасности, инцидент информационной безопасности, киберугроза, реагирование на инциденты информационной безопасности.*

Afanaseva S.V., Kuzmina U.V.

MAIN PROBLEMS WORKING WITH SECURITY OPERATION CENTER

Nowadays cyber threats are steadily increasing and their quality is improving in terms of techniques and tactics. To monitor, detect, and subsequently respond to information security incidents, organizations are establishing Security Operation Centers (SOC) or Information Security Monitoring Centers. This article discusses important challenges that IT professionals face when dealing with information security monitoring centers. Understanding these problems will enable newcomers to avoid mistakes when working with information security monitoring centers, and for experienced professionals it will serve as a vector for improving monitoring centers.

Keywords: *information security, SOC, information security monitoring center, information security incident, cyber threat, information security incident response.*

Центром мониторинга информационной безопасности называется подразделение или отдел информационной безопасности (далее - ИБ), в котором на регулярной основе или постоянно выполняется мониторинг событий ИБ, поступающих как от средств защиты информации (далее - СЗИ), так и от других источников информации. Кроме того, базовыми функциями SOC являются реагирование на инциденты ИБ, последующее их расследование и создание рекомендаций по предотвращению инцидента в будущем. SOC состоит из квалифицированных специалистов по информационной безопасности, средств защиты информации и сопутствующих методов, а также из совокупности процессов, объединяющих людей и технологии в противодействии нарушителю ИБ организации.

Предпосылками к созданию SOC являются:

• Требования ФСТЭК России и ФСБ России (Федеральный закон №187 «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017), где внедрение SOC является обязательной процедурой;

• Отсутствие организованного постоянного контроля происходящего в инфраструктуре организации;

• Активное развитие инфраструктуры организации, а также ее полная модернизация;

• Не продуманная концепция выбора и установки СЗИ;

• Появление новых угроз и уязвимостей, актуальных для организации.

• Таким образом, внедрение SOC становится процедурой, имеющей рекомендательный характер для каждой организации и обязательной для субъектов критической информационной инфраструктуры.

К основным задачам SOC относится:

• определение ключевых показателей эффективности работы SOC-Центра - критериев KPI (Key Performance Indicators,);

• получение деталей подключения информационных и защитных систем защищаемого объекта организации к инфраструктуре SOC-Центра, а также данных об изменениях конфигурации защищаемого объекта на всех его уровнях;

• выстраивание процессов мониторинга, обнаружения, реагирования на инциденты информационной безопасности;

• повышение состояния защищенности объектов посредством внедрения дополнительных средств и мер защиты;

• постоянное совершенствование работы SOC, например, путем проведения «тренировок» персонала по возможным угрозам (например, фишинговая рассылка).

Между тем с каждым годом методики по созданию SOC пытаются внести новые элементы и усовершенствованные алгоритмы, несмотря на то, что большинство организаций еще не решили текущие проблемы технического, программного и нормативно-правового характера. Ниже будут рассмотрены и кратко описаны основные проблемы, с которыми сталкиваются специалисты при создании и обслуживании центров мониторинга информационной безопасности.

1. Выбор модели развертывания SOC: внешний или внутренний.

Существует два способа развертывания центра мониторинга ИБ: непосредственно в контуре предприятия (внутренний) и SOC на аутсорсинге (внешний) [6]. Ниже в таблице представлены основные преимущества и недостатки при выборе модели развертывания SOC.

Кроме того, с недавних пор применяют гибридный способ, когда создается внутренний SOC, в котором работает несколько человек и следит за тем, что выполняет внешний SOC. В свою очередь, основные обязанности по мониторингу, обнаружению и реагированию на события ИБ выполняет именно внешний SOC.

В выборе модели развертывания SOC стоит учитывать потребности организации, ее потенциал, штат сотрудников и их компетенции, наличие СЗИ и сопутствующего оборудования. Дополнительно стоит провести анализ в области сервис-провайдеров, оценить финансовые возможности организации.

При оценке SOC на аутсорсинге стоит начать с проверки наличия сертификатов ФСТЭК России на деятельность по мониторингу, ФСБ России на работу со средствами криптозащиты, заключенного согласия с НКЦКИ. Далее стоит провести собеседование с компанией, предоставляющей услугу, и оценить ожидания организации на возможности компании. В качестве дополнительного шага можно запросить рецензию клиентов этой компании.

2. Распределение задач в SOC

Каждая организация использует свой подход в распределении задач для сотрудников SOC. Стоит выделить три основных подхода распределения задач: разделение по

Таблица 1

Преимущества и недостатки при выборе модели развертывания SOC

Модель развертывания	Преимущества	Недостатки
Внешний SOC	• Не нужно нанимать квалифицированный персонал; • Режим 24/7 будет поддерживать аутсорсинговая компания, а не штат организации; • На базе методик и стандартов аутсорсиноговой компании будут активнее запускаться процессы, реализуемые SOC; • Более низкие финансовые затраты, чем при построении внутреннего SOC; • Обработка и хранение событий ИБ в инфраструктуре исполнителя; • Экономия на содержании технических компонентов и обслуживающем персонале; • Организация может сосредоточить внимание на своих основных бизнес-процессах.	• Высокие требования к каналам между площадками заказчика и исполнителя, так как для обработки передается большой поток данных; • Необходимо потратить время на анализ бизнес-проблем организации и внедрить сквозные процессы с участием внутренних и внешних сотрудников; • Данные хранятся и анализируются за пределами периметра организации, появляются дополнительные риски, связанные с утечкой информации.
Внутренний SOC	• Данные хранятся и обрабатываются внутри периметра согласно всем внутренним требованиям организации; • Внутренние сотрудники лучше знают инфраструктуру организации, а также все «подводные» камни; • Есть постоянный доступ к данным (в случае отсутствия Интернета со внешнего SOC нельзя будет использовать данные).	• Дефицит квалифицированного персонала; • Закупка дорогостоящих компонентов SOC; • Несовместимость средств защиты информации в результате неправильной настройки; • Построение может занять годы и не всегда гарантирует результат.

уровню квалификации и ответственности, по векторам атак или видам угроз, по очередности [5].

Первый подход заключается в выделении нескольких линий с различными компетентностями сотрудников: первая линия обрабатывает все поступающие события и по мере сил с ними справляется. Если инцидент является более сложным, то он отправляется ко второй линии, где сотрудники обладают большим опытом и навыками работы с усложненными ситуациями. Соответственно, если сотрудники второй линии не справляются с инцидентом, то ему назначается статус «критический» и переход осуществляется к третьей линии, где сотрудники являются узконаправленными специалистами в таких областях, как угрозы операционных систем, сетевые угрозы, угрозы отказа в обслуживании и т.д.

Преимуществом данного подхода несомненно является накопление опыта и практики для сотрудников первой линии, совершенствование знаний и навыков для сотрудников второй и третьей линий. Недостатком является огромный объем работ при подготовке инструкций по реагированию на инциденты ИБ для всех линий сотрудников SOC.

Второй подход подразумевает разделение специалистов по разным векторам атак или видам угроз, на которых они специализируются (например, вредоносное программное обеспечение, фишинг, сетевые атаки и т.д.). Кроме того, разделение может осуществляться по типам систем (автоматизированные рабочие места, специализированные приложения, центр обработки данных и т.д.) или по степени важности систем (инциденты, относящиеся к критически важным системам, сразу переходят ко второй линии).

Отрицательной чертой данного подхода может быть незаменимость сотрудников, работающих в определенной области, а положительной – возможность для сотрудника сфокусироваться на интересной ему области и наращивать потенциал в выбранном направлении.

Третий подход реализует «живую» очередь из инцидентов ИБ, в которой сотрудники способны справляться с инцидентом без пере-

дачи его к более сильному специалисту. При этом первой линией в данном подходе может выступать искусственный интеллект, который убирает лишнюю информацию в виде ложных срабатываний и передает дальнейшие сведения единому фронту сотрудников SOC.

Такой подход, в отличии от предыдущего, позволяет сотрудникам работать со всеми типами инцидентов, тем самым повышая их знания в различных областях. Тогда проблемой становится поиск квалифицированных сотрудников, способных справится со всевозможными инцидентами ИБ.

При выборе подхода стоит руководствоваться квалификацией сотрудников и их наличием в SOC. Кроме того, можно заметить, что подходы возможно объединять между собой, получая при этом гибридный вариант, который в свою очередь может стать подходящим для организации.

3. Инструментарий SOC

Базовым инструментом для каждого SOC принято считать Security Information and Event Management (далее - SIEM). Но просто установка SIEM не позволит в полной мере исполнять основные задачи SOC. Ниже приведены основные инструменты, которые могут быть внедрены в SOC, и примеры продуктов отечественного и зарубежного рынка. Некоторые из них входят в состав других, но так или иначе являются отдельными инструментами SOC.

Исследовательская компания Gartner считает, что базой каждого SOC является

Таблица 2

Инструментарий SOC

Инструмент	Пример
Security Information and Event Management (SIEM)	Ankey SIEM, MaxPatrol SIEM, RuSIEM, КОМРАД, SearchInform SIEM
Endpoint Detection and Response (EDR)/ Extended Detection and Response (XDR)	Kaspersky EDR, Positive Technologies XDR, Managed XDR Group-IB
Network Traffic Analysis (NTA)/ Network Detection and Response (NDR)	Positive Technologies Network Attack Discovery, Group-IB Threat Detection System, Kaspersky Anti Targeted Attack, «Гарда Монитор»
Incident Response Platform (IRP)/ Security Orchestration, Automation and Response (SOAR)	Jet Signal, R-Vision Incident Response Platform, Security Vision Incident Response Platform
Threat Intelligence Platform (TIP)	Group-IB TI, Kaspersky TI, PT Cybersecurity Intelligence, R-Vision TIP
Intrusion Detection System (IPS)/ Intrusion Prevention System (IDS)	Traffic Inspector Next Generation, ViPNet IDS 3, «Аргус», «СОВ Континент», «Рубикон», «С-Терра СОВ»
Managed Detection and Response (MDR)	Group-IB MDR Services, Kaspersky MDR, Positive Technologies Expert Security Center
Сервисы для анализа поведения пользователей	InfoWatch Prediction, SearchInform ProfileCenter
Средства контроля и анализа защищенности	RedCheck, XSPIDER, Сканер-ВС, Ревизор сети
Технологии хранения данных и резервного копирования	Эльбрус-2000, Норси-Транс, Aerodisk, DEPO, RCNTEC, RuBackup, Handy Backup
Сервисы по форензике	Elcomsoft Premium Forensic Bundle, ePlat4m Security GRC, EtherSensor

«SIEM + NTA + EDR» [4]. Для обогащения данной комбинации, а также для повышения эффективности работы SOC следует рассмотреть следующие инструменты: IRP/SOAR решения, сервисы TIP, IPS/IDS, средства контроля и анализа защищенности, технологии хранения данных и резервного копирования, MDR, сервисы для анализа поведения пользователей, сервисы по форензике.

4. Процесс управления жизненным циклом инцидента

Управление инцидентами ИБ является одним из важнейших процессов, реализуемых в SOC [1]. Если хотя бы на одном из этапов возникнут сложности, это может привести к полному провалу всего процесса, что является недопустимым. На рис. 1 приведены этапы реагирования на инцидент ИБ и их описание.

Для начала необходимо рассмотреть отечественные и иностранные стандарты, такие как:

Рис. 1. Этапы реагирования на инцидент

• National Institute of Standards and Technology. NIST SP 800-61;

• Carnegie Mellon University. CMU/SEI-2018-TR-007;

• Национальный стандарт РФ ГОСТ Р ИСО/МЭК ТО 18044-2007 «Менеджмент инцидентов информационной безопасности»;

• РС БР ИББС-2.5-2014 «Менеджмент инцидентов ИБ»;

• ENISA «Руководство по эффективной практике для управления инцидентами».

Стандарты в полной мере определяют жизненный цикл инцидента, роли и область ответственности в данном процессе, ключевые показатели эффективности, рекомендации по управлению инцидентами. Но даже при наличии обширной теории, на практике вопросы и проблемы все равно возникают:

• Организация работает только с реагированием – из-за этого невозможно полностью видеть картину происходящего;

• Неточные или неполные сценарии для реагирования на определенный инцидент – время реагирования на инцидент увеличивается из-за задержки на получение точных указаний;

• Нет улучшения процесса управления инцидентом – без совершенствования процесса невозможно предотвратить актуальные угрозы и уязвимости.

5. Показатели эффективности SOC

Оценка эффективности SOC является значимым параметром на пути развития информационной безопасности в организации. Без этого организация не сможет вовремя обнаружить и исправить актуальные угрозы, что в свою очередь ведет к потери ключевой информации для бизнеса [9].

При создании или подключении SOC на начальном этапе должно прописываться соглашение об уровне услуг (Service Level Agreement, SLA) – договор, внутри подразде-

ления или между клиентом и заказчиком, в котором содержатся описание услуги, обязанности сторон, а также уровень качества предоставления данной услуги. В нем присутствуют базовые метрики, такие как время реагирования на инцидент, количество ложных срабатываний, время оповещения персонала, скорость обработки инцидента и т.п. Более того, не стоит забывать про основной ключевой показатель эффективности (Key Performance Indicator, KPI) для любого SOC – недопущение инцидентов, приносящих ущерб организации. Чтобы убедиться в эффективности работы SOC, стоит провести тренировку, которая имитирует реальные угрозы.

6. Определение основных источников информации для SOC

Для эффективной работы SOC необходимо обеспечить сотрудников актуальной информацией, касающейся инфраструктуры организации, изменениях в ней. Кроме того, постоянно должна отслеживаться информация о новых угрозах и уязвимостях [2]. Условно источники информации можно разделить на внутренние и внешние. Ниже приведены основные источники информации для SOC.

В данной таблице представлен основной

Таблица 3

Основные источники информации

Внутренние источники информации	Внешние источники информации
События безопасности с инфраструктурных компонентов (операционные системы, автоматизированные системы оповещения, прикладное программное обеспечение и др.)	Информация от ведомственных и корпоративных центров в рамках соглашений по информационному обмену (ФСТЭК России, ФСБ России, ЦБ России)
События со средств защиты информации (антивирус, межсетевой экран, NTA, EDR и др.)	Сообщества в социальных сетях, форумы в Интернете или Даркнете
Актуальные данные об активах (база данных управления конфигурацией, таблицы маршрутизации и др.)	Информация о новых инструментах (средствах защиты информации) от вендоров
Дополнительная информация от внутренних сотрудников	Данные об угрозах и уязвимостях (Threat Intelligence, Open Source Intelligence и др.)

объем источников информации для SOC. При выборе источника стоит руководствоваться наличием тех или иных средств защиты информации, а также заинтересованностью сотрудников в поиске актуальной информации, касающейся новых угроз и уязвимостей [10].

7. Организационная структура SOC

Корректно сформированная команда специалистов является одним из важных показателей для эффективной работы SOC [3]. Ниже представлена организационная структура SOC (рис. 2).

Одна из важнейших групп для любого SOC – это группа мониторинга и реагирования, которая выполняет первостепенные задачи SOC, описанные в начале статьи. В зави-

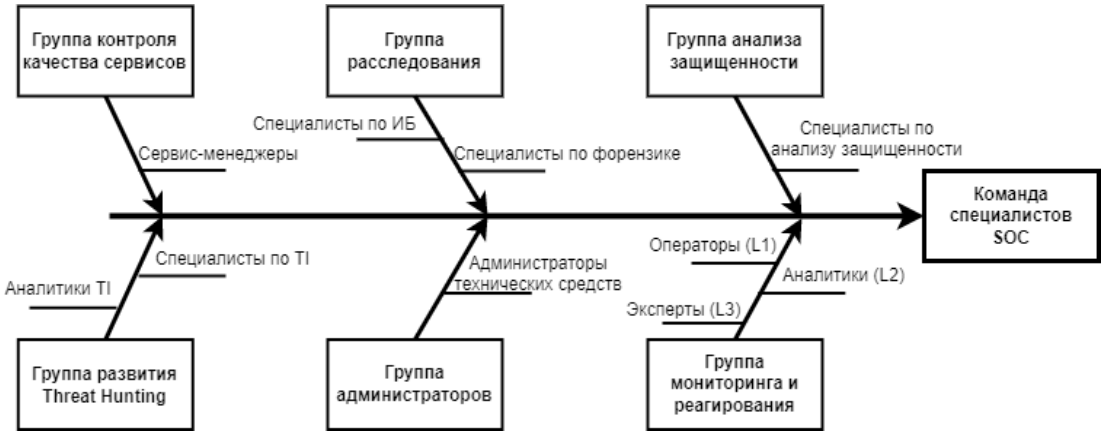


Рис. 2. Организационная структура SOC

симости от выбора подхода распределения задач в SOC может состоять из операторов, аналитиков и экспертов, распределенных по нескольким линиям. Операторы выполняют первичную фильтрацию событий ИБ, полученных от различных источников, регистрируют инциденты ИБ, выполняют действия, изложенные в инструкции по реагированию на инциденты, соответствующие первой линии. Аналитики проводят анализ инцидентов или поступающих угроз, прогнозируют их развитие, создают превентивные меры, а также могут активно участвовать в реагировании на инцидент ИБ на любом из его этапов. В свою очередь, эксперты являются узконаправленными специалистами в области ИБ, которые совершенствуют базу знаний всего SOC. Более того, эксперты также участвуют в работе операторов и аналитиков, например, в случае, если инцидент является критическим [7].

Группа администраторов, состоящая из администраторов технических средств, выполняет работы, относящиеся к программно-аппаратным средствам, СЗИ, сетевым техническим средствам и т.д. Специалисты из группы развития Threat Hunting собирают информацию об актуальных угрозах, новых уязвимостях, занимаются разработкой мер по защите от угроз или нарушителей, проверяют информацию из внешних источников данных. Группа контроля качества сервиса отвечает за выполнение и соблюдение SLA, в том числе за организацию всех процессов взаимодействия. Специалисты из группы расследования должны собрать и зафиксировать всю информацию, касающуюся инцидента, проанализировать весь объем данных, определить какой вред получила организация от инцидента и принять меры в отношении виновных лиц. Группа анализа защищенности отвечает за тестирование систем на проникновение, анализ рисков ИБ в SOC, состояние защищенности как организации, так и самого SOC.

Безусловно исходить нужно от размеров SOC и численности команды. Опираться необходимо на функции, который SOC организации должен исполнять. После этого необходимо выбрать группы, которые войдут в состав SOC. Для каждой группы должны быть определены руководители, распределена ответственность, основные должностные обязанности [8].

В данной статье проанализированы основные проблемы, с которыми сталкиваются специалисты ИБ при работе с центрами мониторинга информационной безопасности, а также подобно представлены возможные варианты решения данных проблем. Кроме того, даны базовые рекомендации для принятия оптимальных решений в тех или иных случаях.

Проведенный анализ позволяет сделать вывод, что для решения описанных проблем необходимо создание общих стандартов и методик, которые бы регламентировали процесс создания SOC, введение в эксплуатацию и дальнейшую работу. Эти документы должны быть одобрены федеральными органами исполнительной власти, такими как ФСТЭК России и ФСБ России.

Более того, необходимо аккумулировать опыт ведущих отечественных компаний ИБ для создания центров мониторинга ИБ следующего поколения: SOC с полной автоматизацией деятельности человека на этапе мониторинга и реагирования, а также четко выстроенной организационной структурой. В этом случае может получиться действительно эффективный инструмент, который будет защищать организацию от новых угроз современного мира.

Литература

1. Энсон С. Реагирование на компьютерные инциденты. // Wiley, 2021. 436 с.

2. Калугина О., Баранкова И., Михайлова У. Разработка инструмента моделирования угроз безопасности информационной системы предприятия // 2nd ICECCE 2020. 2. 2020. С. 1–5.

3. Ройс Д. Искусство тестирования на проникновение в сеть // Manning Shelter Island, 2021. 312 с.

4. Васильева И.Н. Расследование инцидентов информационной безопасности // Издательство СПбГЭУ, 2019. 113 с.

5. Солдатов С. Организация работы и обработка уведомлений в SOC // Лаборатория Касперского, 2022. URL: https://www.kaspersky.ru/blog/soc-alert-processing/33948/.

6. Натанс Д. Проектирование и строительство SOC // Syngress, 2014. 276 с.

7. Баранкова И.И., Михайлова У.В., Лукьянов Г.И. Формирование компетенций специалиста по ин-

формационной безопасности // Актуальные проблемы современной науки, техники и образования: тезисы докладов 77-й международной научно-технической конференции. 2019. С. 428.

8. Анисимова А.А. Менеджмент в сфере информационной безопасности. // Национальный Открытый Университет "ИНТУИТ", 2016. 213 с.

9. Дронова Г.А. Управление информационной безопасностью // Новосибирск: НГТУ, 2016. 28 с.

10. Баранкова И.И., Михайлова У.В., Лукьянов Г.И. Прогнозирование локальных и внешних угроз на информационные серверы предприятия // Актуальные проблемы современной науки, техники и образования. 2017. Т. 1. С. 217–220.

References

1. Enson S. Reagirovaniye na komp'yuternyye intsidenty. // Wiley, 2021. 436 s.

2. Kalugina O., Barankova I., Mikhaylova U. Razrabotka instrumenta modelirovaniya ugroz bezopasnosti informatsionnoy sistemy predpriyatiya // 2nd ICECCE 2020. 2. 2020. S. 1–5.

3. Roys D. Iskusstvo testirovaniya na proniknoveniye v set' // Manning Shelter Island, 2021. 312 s.

4. Vasil'yeva I.N. Rassledovaniye intsidentov informatsionnoy bezopasnosti // Izdatel'stvo SPbGEU, 2019. 113 s.

5. Soldatov S. Organizatsiya raboty i obrabotka uvedomleniy v SOC // Laboratoriya Kasperskogo, 2022. URL: https://www.kaspersky.ru/blog/soc-alert-processing/33948/.

6. Natans D. Proyektirovaniye i stroitel'stvo SOC // Syngress, 2014. 276 s.

7. Barankova I.I., Mikhaylova U.V., Luk'yanov G.I. Formirovaniye kompetentsiy spetsialista po informatsionnoy bezopasnosti // Aktual'nyye problemy sovremennoy nauki, tekhniki i obrazovaniya: tezisy dokladov 77-y mezhdunarodnoy nauchno-tekhnicheskoy konferentsii. 2019. S. 428.

8. Anisimova A.A. Menedzhment v sfere informatsionnoy bezopasnosti. // Natsional'nyy Otkrytyy Universitet "INTUIT", 2016. 213 s.

9. Dronova G.A. Upravleniye informatsionnoy bezopasnost'yu // Novosibirsk: NGTU, 2016. 28 s.

10. Barankova I.I., Mikhaylova U.V., Luk'yanov G.I. Prognozirovaniye lokal'nykh i vneshnikh ugroz na informatsionnyye servery predpriyatiya // Aktual'nyye problemy sovremennoy nauki, tekhniki i obrazovaniya. 2017. T. 1. S. 217–220.

АФАНАСЬЕВА Светлана Викторовна, студент 5 курса кафедры Информатики и Информационной безопасности, Магнитогорский государственный технический университет им. Г.И. Носова. Россия, 455000, г. Магнитогорск, пр. Ленина 38. E-mail: afasvetlana0@gmail.com

КУЗЬМИНА Ульяна Владимировна, кандидат технических наук, доцент кафедры Информатики и Информационной безопасности, Магнитогорский государственный технический университет им. Г.И. Носова. Россия, 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: ylianapost@gmail.com

AFANASEVA Svetlana Viktorovna, 5th year student of the Department of Informatics and Information, Security of Nosov Magnitogorsk State Technical University. 455000, Magnitogorsk, Lenin Ave. 38. E-mail: afasvetlana0@gmail.com

KUZMINA Ulyana Vladimirovna, Candidate of Technical Sciences, Associate Professor of the Department of Informatics and Information, Security of Nosov Magnitogorsk State Technical University. 455000, Magnitogorsk, Lenin Ave. 38. E-mail: ylianapost@gmail.com

УДК 342.41 + 342.511.5 Вестник УрФО № 1(47) / 2023, с. 59–68

Бухарев Д. А., Соколов А.Н., Рагозин А.Н.

DOI: 10.14529/secur230106

ПРИМЕНЕНИЕ ИЕРАРХИЧЕСКОГО КЛАСТЕРНОГО АНАЛИЗА ДЛЯ КЛАСТЕРИЗАЦИИ ДАННЫХ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ АСУ ТП, ПОДВЕРГАЮЩИХСЯ ВОЗДЕЙСТВИЮ КИБЕРАТАК [1]

Техническое развитие промышленных средств автоматизации и увеличение уровня интеграции промышленных и корпоративных сетей приводит к увеличению рисков проведения успешных кибератак. Реализация таких кибератак может подразумевать получение доступа к управлению важными промышленными установками, что влечет за собой риск остановки производства или создания аварийной ситуации. Практическое обеспечение информационной безопасности автоматизированных систем управления технологическими процессами (АСУ ТП) требует своевременного обнаружения кибератак, как известного, так и неизвестного типа. Эти кибератаки можно выделить в виде аномалий в динамических процессах, регулярно регистрируемых при работе АСУ ТП. В контексте решения задачи обнаружения атак на информационные системы АСУ ТП, кластерный анализ применяется как один из методов, реализующих обнаружение аномалий. Исследуется применение иерархического кластерного анализа для кластеризации данных информационных процессов АСУ ТП, подвергающихся воздействию различным кибератак, решается задача выбора уровня иерархии кластеров, соответствующий минимальному набору кластеров, агрегирующих раздельно нормальные и аномальные данные. Показано, что метод Уорда реализует наилучшее разделение на кластеры. Следующим этапом исследования предполагается решение задачи классификации сформированного минимального набора кластеров, то есть определения какой кластер является нормальным, какой кластер является аномальным.

Ключевые слова: *Автоматизированная система управления технологическим процессом, кибератака, классификация кибератак, иерархическая кластеризация, обнаружение аномалий.*

[1] Исследование поддержано грантом Российского научного фонда (проект № 22-71-10095).

APPLICATION OF HIERARCHICAL CLUSTER ANALYSIS FOR CLUSTERING THE DATA OF ICS INFORMATION PROCESSES AFFECTED BY CYBERATTACKS

The technical development of industrial automation tools and an increase in the level of integration of industrial and corporate networks leads to an increase in the risks of successful cyberattacks. The implementation of such cyberattacks may involve gaining access to the control of important industrial installations, which entails the risk of stopping production or creating an emergency. The practical provision of information security for industrial control systems (ICS) requires the timely detection of cyberattacks, both known and unknown. These cyber-attacks can be identified as anomalies in dynamic processes that are regularly recorded during the operation of ICS. In the context of solving the problem of detecting attacks on ICS information systems, cluster analysis is used as one of the methods that implement anomaly detection. The application of hierarchical cluster analysis for clustering data of ICS information processes exposed to various cyberattacks is studied, the problem of choosing the level of the cluster hierarchy corresponding to the minimum set of clusters aggregating separately normal and abnormal data is solved. It is shown that Ward's method implements the best division into clusters. The next stage of the study involves solving the problem of classifying the formed minimum set of clusters, that is, determining which cluster is normal and which cluster is abnormal.

Keywords: *Industrial control systems, cyberattack, cyberattack classification, hierarchical clustering, anomaly detection.*

Современные автоматизированные системы управления технологическими процессами (АСУ ТП) организованы в сеть, соединяющую множество контрольно-измерительной аппаратуры, программируемых логических контроллеров, станций оператора, SCADA систем и другого сетевого оборудования. Такая обширная сеть позволяет эффективно управлять производством и реагировать на различные ситуации, возникающие в ходе функционирования производства. Однако, инциденты информационной безопасности промышленной сети передачи данных могут привести к выводу из строя дорогостоящего оборудования, а также стать причиной экологической катастрофы. Злоумышленники, также могут проводить несанкционированный доступ к защищенной информации о технологическом производстве. Актуальной является задача обнаружения атак как известного, так и не известного типов, а также реализация возможности классификации воздействующих различных типов атак

Системы обнаружения атак (СОА), основанные на методах обнаружения аномалий, показывают высокие показатели эффективности обнаружения атак, как известного, так и не известного типов. Одним из методов интеллектуального анализа данных, который может быть применен для решения задачи обнаружения атак, а также их последующей классификации, является кластерный анализ. Предполагается, что нормальные данные, соответствующие штатному режиму работы системы, образуют большие плотные кластеры, или плотные скопления небольших нормальных кластеров, а аномальные данные, соответствующие аномальному режиму работы системы, распределяются в более маленькие и разрозненные аномальные кластеры, силь-

но удаленных от выделенных кластеров нормального поведения исследуемой системы.

В исследовании проведен анализ возможности использования агломеративной иерархической кластеризации для целей построения системы кластеров, соответствующих нормальным и аномальным состояниям исследуемой системы. В результате анализа наблюдаемого набора данных исследуемой системы, формируется иерархическая система кластеров, отображаемая в виде дендрограммы. Самый нижний уровень дендрограммы соответствует исходному (начальному) набору данных, самый верхний уровень дендрограммы, соответствует одному кластеру, включающего в себя все исходные начальные данные. Промежуточные уровни иерархии кластеров, отображаемой в виде дендрограммы, соответствуют системе кластеров, агрегирующих нормальные и аномальные исходные данные с соответствующим уровнем обобщения. Очевидно, существует максимальный уровень иерархической кластеризации исходных данных, отображаемой в виде дендрограммы, соответствующий минимальному количеству кластеров, агрегирующих раздельно (без перекрытия) нормальные и аномальные исходные данные. При этом, в формируемом минимальном наборе кластеров, одна часть кластеров соответствует только нормальным исходным данным (нормальные кластеры), другая часть кластеров соответствует только аномальным исходным данным (аномальные кластеры). Соответствующее отображение на дендрограмме выделенного минимального набора нормальных и аномальных кластеров содержит информацию для идентификации вида кластеров, то есть, идентификации отдельно нормальных кластеров и идентификации отдельно аномальных кластеров. Идентификация видов кластеров соответствует решению задачи двух классовой классификации кластеров, то есть разделения кластеров на нормальные и аномальные кластеры.

Построение системы обнаружения аномалий в наблюдаемых данных технической системы, возникающих вследствие воздействия кибератак, предполагает построение иерархии кластеров исходных данных, далее, предполагается выбор уровня иерархии кластеров, соответствующий минимальному набору кластеров, агрегирующих раздельно нормальные и аномальные данные, далее предполагается решение задачи классификации сформированного минимального набора кластеров, то есть определения какой кластер является нормальным, какой кластер является аномальным.

В проведённом исследовании рассматриваются первые два этапа: построение иерархии кластеров исходных данных, затем, рассматриваются выбор оптимального уровня иерархии кластеров, соответствующий минимальному набору кластеров, агрегирующих раздельно нормальные и аномальные данные.

Метод кластерного анализа заключается в выделении таких характеристик из сетевого трафика или записей состояния АСУ ТП, которые позволят разбить классифицируемые объекты на группы, соответствующие нормальному функционированию системы или сети. Все остальные экземпляры, которые не попадают в построенные области, классифицируются как аномальные [1]. В каждом конкретном методе кластерного анализа используется своя метрика, которая позволяет оценивать принадлежность наблюдаемого вектора параметров процессов системы одному из кластеров или выход за границы сформированных кластеров.

Современные тенденции предполагают объединение индустриальных и корпоративных сетей, поскольку это, с одной стороны, позволяет уменьшать затраты бизнеса и делать эксплуатацию индустриальных объектов более удобной, но с другой увеличивает риски проведения успешных кибератак. Это связано с необходимостью открытия удаленного доступа для контроля и анализа технологического процесса на предприятии. Такой доступ позволяет не находиться непосредственно на предприятии, но также дает злоумышленнику возможность получить доступ к промышленному оборудованию внутри промышленной сети. Кластерный анализ позволяет производить одновременную обработку разнородных данных, наблюдаемых как в контрольных точках корпоративных сетей, также данных, наблюдаемых с сенсоров или актуаторов АСУ ТП промышленных систем.

На основании анализа векторов обучающей выборки производится построение кластеров, описывающих нормальное поведение системы (в виде совокупности кластеров), после чего выполняет поиск аномалий – кластеров состояний, сильно удаленных от выделенных кластеров нормального поведения системы, то есть кластеров, соответству-

ющих аномальным состояниям системы, возникающих в следствии воздействия атак. Также, кластерный анализ позволяет формировать систему кластеров, соответствующих различным типам воздействующих атак, то есть проводить непрерывное обучение СОА в процессе текущей работы.

Обзор методов кластерного анализа приведён в работе [2]. Обзор иерархических методов кластерного анализа приведён в работе [3]. Применение методов кластерного анализа для обнаружения аномалий на основе анализа выбросов в данных рассмотрено в работах [4–7]. Обнаружение аномалий в данных с использованием кластерного анализа при делении выбросов на локальные и глобальные, рассмотрено в работах [8, 9].

Для определения оптимальных параметров агломеративной иерархической кластеризации в первую очередь требуется определиться с метрикой, на основании которой будет происходить сравнение. При получении готовой разбивки на кластеры данных, у которых есть метки аномальности, мы можем разделить их на 2 группы – содержащие аномальные данные и содержащие нормальные данные. Разделение на группы происходит на основании наличия в кластере хотя бы одной аномальной точки. После получения размеченных кластеров можно рассчитать следующие значения: N_a – общее количество аномальных кластеров; N_{an} – количество аномальных кластеров, содержащих нормальные данные; N_{aa} – количество аномальных кластеров, не содержащих нормальные данные. По этим значениям рассчитываются следующие метрические параметры (метрики):

$$R_{an} = \frac{N_{an}}{N_a} \quad (1)$$

– доля аномальных кластеров, содержащих нормальные данные;

$$R_{aa} = \frac{N_{aa}}{N_a} \quad (2)$$

– доля аномальных кластеров, не содержащих нормальные данные.

Метрики (1), (2) можно использовать для определения качества кластеризации, а также для определения оптимального уровня иерархии кластеров. Основной метрикой, которая использовалась в рамках данного исследования, является метрика R_{aa}, которая показывает, на сколько точно распределены данные по кластерам, содержащие аномальные данные. Для получения наиболее информативного анализа параметров кластеризации производится серия экспериментов, в которой рассчитывается кривая значений R_{aa} в зависимости от увеличения числа разбиения на кластеры (диапазон от 1 до 1000). Получив группу кривых, можно определить оптимальное значение параметра кластеризации и оптимальный уровень иерархии кластеров.

Для определения оптимального уровня иерархии кластеров с использованием метрики R_{aa} необходимо получить точку перегиба для кривой R_{aa}, которая будет являться базовым уровнем. Для получения точки перегиба можно применить интерполяционный полином, на основе которого вычисляется вторая производная.

В будущих работах также планируется исследовать возможность проведения классификации кластеров, полученных в результате работы иерархической кластеризации. Полученные кластеры должны подаваться на некоторый классификатор, который будет создавать две группы – аномальную и нормальную. Корректное разделение классификатором набора кластеров будет означать точное выделение аномальных точек в наборе данных. После получения таких групп возможно внедрение процесса постоянного анализа поступающих данных для выделения аномалий в режиме реального времени.

В качестве набора данных для проведения исследования при помощи методов иерархического кластерного анализа использовался набор данных Secure Water Treatment (SWaT) [10]. Набор данных генерируется моделью, имитирующую реальное водоочистное сооружение. Моделируемое водоочистное сооружение содержит промышленное оборудование, в котором присутствует несколько программируемых логических контроллера, SCADA система, а также сетевое оборудование промышленного образца. Структурная схема макета водоочистного сооружения представлена на рис. 1.

Набор данных, используемый в работе, состоит из 14996 записей, каждая из которой описывает состояние 77 датчиков или механизмов водоочистного сооружения в конкретный момент времени. В формируемом моделью SWaT наборе данных были сформированы и промаркированы шесть кибератак на информационную инфраструктуру водоочистного сооружения, в ходе которых производилось несанкционированное изменение параметров системы, отражающей работу во-

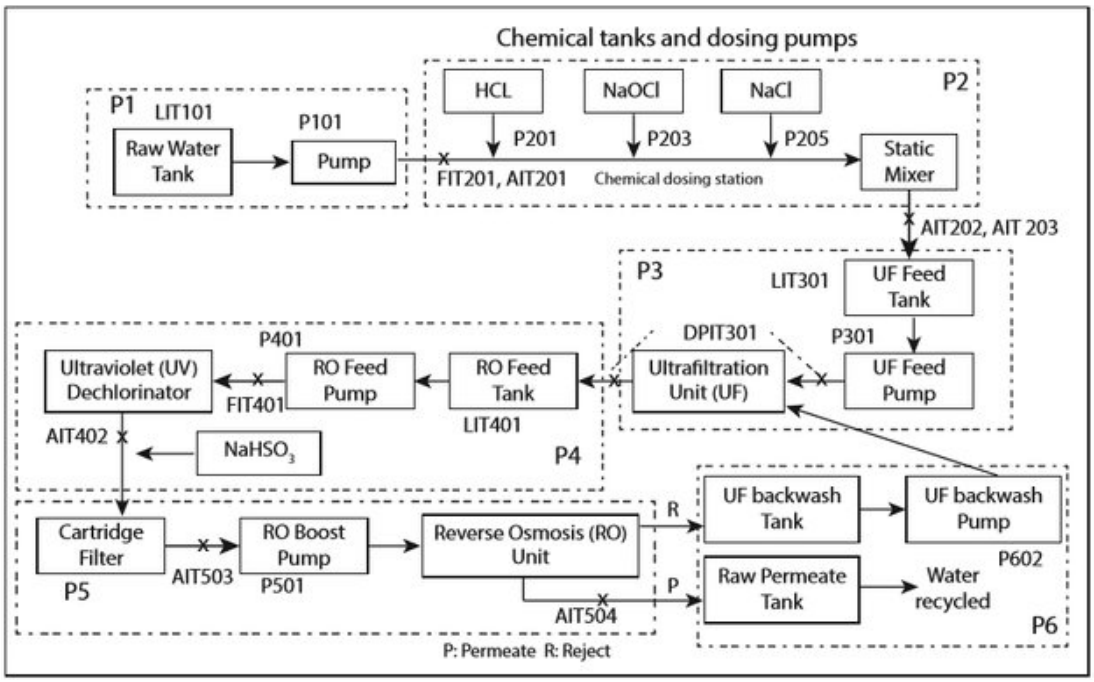


Рис. 1. Структурная схема макета SWaT [10]

Рис. 2. Распределение атак на систему с течением времени (атаки обозначены красными столбцами)

доочистного сооружения. Расположение этих атак на наборе данных изображено на рис. 2. Доля точек данных, в которых производились атаки по отношению к общему количеству точек данных – 14%.

Для обработки данных модели SWaT в исследовании использован агломеративный метод иерархического кластерного анализа. В качестве метрики расстояния в применяемом методе кластеризации была использована евклидова метрика, при этом, в качестве метода связи кластеров использовался метод полной связи кластеров.

В ходе вычислительного эксперимента исследовались различные методы разбиения на кластеры с использованием иерархической кластеризации. Применялись методы разбиения: Уорда, средней связи, центроидный, полной связи, одиночной связи. В качестве метрики расстояния использовалась ев-

клидова метрика. Результаты эксперимента отражены в табл. 1 и рис. 3, 4.

В таблице 1 приведены численные значения R_{aa} для рассмотренных методов при числе разбиении на кластеры в 500 и 1000 кластеров. По результатам эксперимента видно, что метод Уорда является наилучшим методом разбиения в обоих случаях, т.к. метрика R_{aa} обладает наиболее высоким значением. Это означает, что при кластеризации с использованием метода Уорда получались наиболее «чистые» аномальные кластеры, без примесей нормальных данных.

На рис. 4 изображен график второй про-

Таблица 1

Значения R_{aa} различных методов разделения на кластеры при использовании евклидовой метрики

Кол-во кластеров при разбиении	Метод	R_{aa}
500	Уорда	0,8657
1000	Уорда	0,9433
500	Средней связи	0,7719
1000	Средней связи	0,8909
500	Центроидный	0,7705
1000	Центроидный	0,8948
500	Полной связи	0,8376
1000	Полной связи	0,9162
500	Одиночной связи	0,5704
1000	Одиночной связи	0,7767

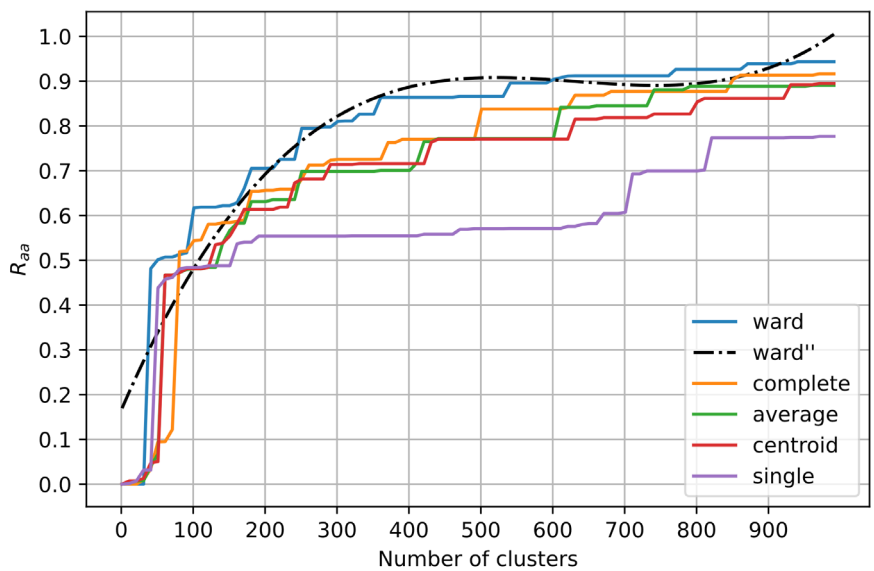


Рис. 3. График кривых R_{aa} различных методов разделения на кластеры при использовании евклидовой метрики

изводной для кривой R_{aa}. На графике можно увидеть, что кривая имеет точку перегиба в районе от 500 до 600 кластеров – 520 кластеров. Эта точка является оптимальным уровнем иерархии кластеров, при котором возможно достичь достаточно точного разбиения на аномальные и нормальные кластеры.

Для увеличения точности кластеризации возможно дополнять исходные данные историческими точками. В данном эксперименте показано, как изменяется точность кластеризации при добавлении 1, 2 и 3 предыдущих точек. Результаты эксперимента отражены в табл. 2 и рис. 5.

В таблице 3 приведены численные значения R_{aa} для рассмотренных отсчетов при числе разбиении на кластеры в 500 и 1000 кластеров. Также для сравнения представлены результаты, когда дополнительные данные не использовались. В таблице 3 видно, что до-

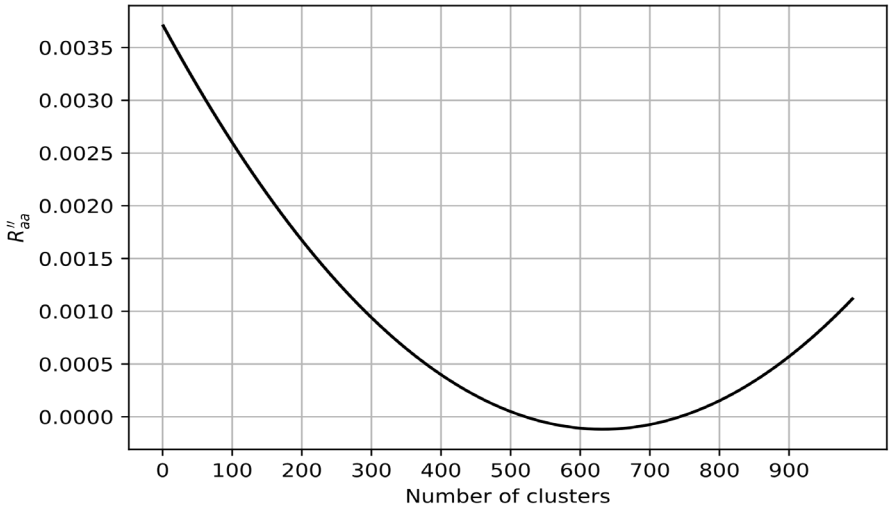


Рис. 4. График второй производной для кривой R_{aa} (метод Уорда)

Таблица 2

Значения R_{aa} при различном количестве исторических данных при анализе

Кол-во кластеров при разбиении	Кол-во отсчетов	R_{aa}
500	0	0,8657
1000	0	0,9433
500	1	0.88
1000	1	0.9347
500	2	0.8576
1000	2	0.93
500	3	0.8823
1000	3	0.9309

бавление исторических данных не дает весомого прироста в точности. В случае, когда добавляется 3 точки исторических данных при 500 кластерах, мы видим прирост в 0,0116. При анализе на большем количестве кластеров при разбиении точность снижается. На рис. 5 также можно заметить, что добавление исторических данных визуально не позволяет явно понять, что дополнительные отсчеты добавляют точности кластеризации.

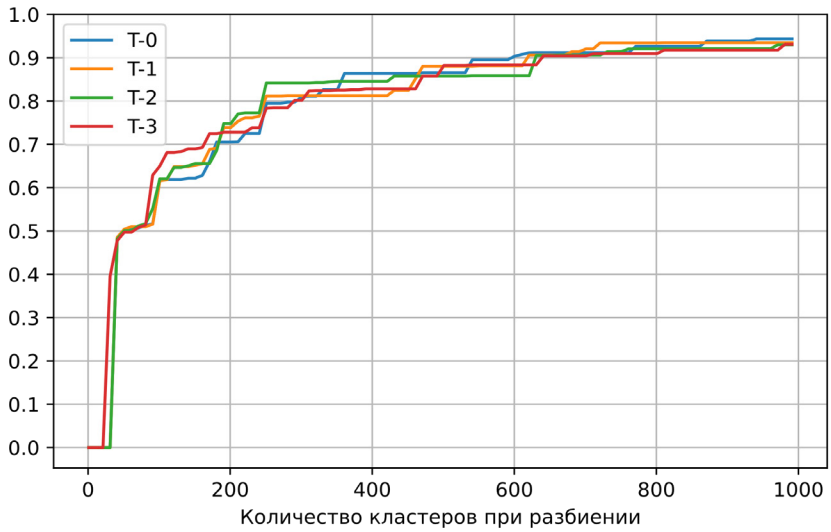


Рис. 5. График кривых R_{aa} при различном количестве исторических данных (евклидова метрика, метод Уорда)

При отнесении кластера к аномальным изначально использовалось предположение о том, что при наличии в кластере хотя бы одной аномальной точки этот кластер считался аномальным. Изменение такого критерия (принятие кластера аномальным при допустимом большем количестве аномальных точек внутри кластера) позволит нам уменьшить уровень разбиения на кластеры. В рамках этого эксперимента сравнивалось 6 различных критериев отнесения кластера к аномальным: < 1 точки, < 2, < 3, < 5, < 10, < 20. Результаты эксперимента отражены на рис. 6.

По рисунку 6 видно, что изменение критерия в большую сторону позволяет снизить количество кластеров при разбиении на нормальные и аномальные кластеры и получить более низкий уровень иерархической кластеризации для определения минимального количества кластеров, но при этом снижается качество разбивки на кластеры анализируемых данных наблюдаемых процессов, за счёт увеличения метрики R_{aa}.

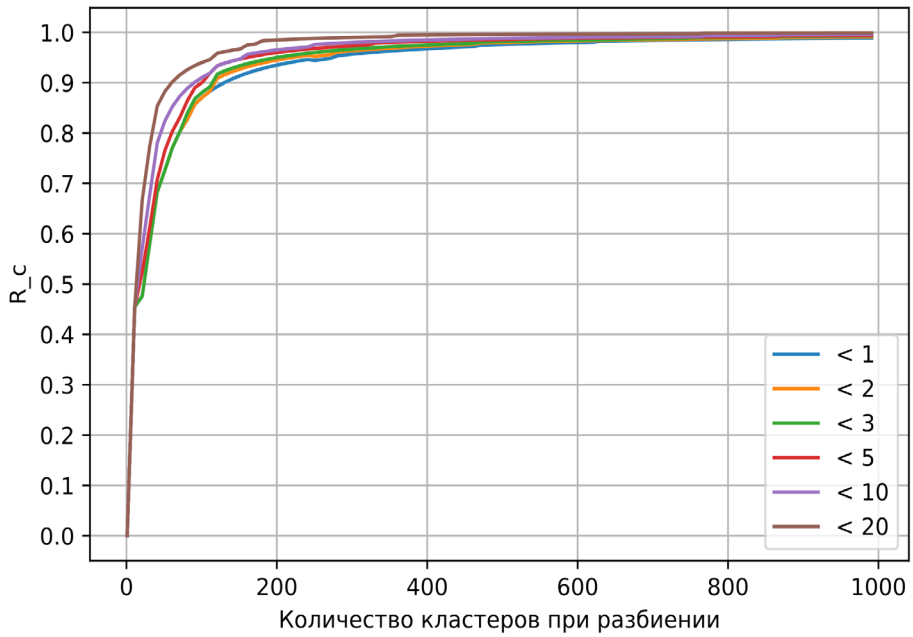


Рис. 6. График кривых Raa при различных критериях принятия кластера как аномального (евклидова метрика, метод Уорда)

Проведено исследование метода агломеративной иерархической кластеризации для определения минимального количества кластеров данных информационных процессов АСУ ТП, подвергающихся воздействию кибератак.

Показана возможность использования метода агломеративной иерархической кластеризации для целей построения системы не перекрывающихся кластеров, соответствующих раздельно нормальным и аномальным состояниям исследуемой системы.

Разработаны и исследованы критерии для определения максимального уровня иерархической кластеризации исходных данных, отображаемой в виде дендрограммы, соответствующий минимальному количеству кластеров, агрегирующих раздельно (без перекрытия) нормальные и аномальные исходные данные информационных процессов АСУ ТП, подвергающихся воздействию кибератак.

Показана эффективность определения оптимального уровня иерархической кластеризации на основе вычисления метрики R_{aa}, которая отражает степень качества (чистоты) кластеризации. Показано, что метод Уорда агломеративной иерархической кластеризации является наилучшим для решения задачи определения аномалий в информационных процессах АСУ ТП, подвергающихся воздействию кибератак.

Соответствующее отображение на дендрограмме определённого минимального набора не перекрывающихся нормальных и аномальных кластеров содержит информацию для дальнейшей идентификации вида кластеров, то есть разделения кластеров на нормальные и аномальные кластеры, без

предварительной разметки исходных данных, что делает возможным в ходе дальнейших исследований и разработок реализовать систему обнаружения аномалий в наблюдаемых динамических потоках данных АСУ ТП, подвергающихся воздействию кибератак.

Литература

1. Волкова В. Н. Основы теории систем и системного анализа: учебник / В. Н. Волкова, А. А. Денисов. – СПб: Изд-во СПбГТУ, 1999. – 512 с.

2. Флейшман Б. С. Основы системологии / Б. С. Флейшман. – М.: Радио и связь. 1982. – 368 с.

3. Тырсин А. Н. О математическом моделировании сложных организационных систем / А. Н. Тырсин // Организация и управление эффективностью и производительностью производственных и социальных систем: Матер. межд. научно-практ. конф. – Новочеркасск: ЮРГТУ (НПИ), 2005. – С. 49–50.

4. Биргер И. А. Техническая диагностика / И. А. Биргер. – М.: Наука, 1978. – 239 с.

5. Debar H., Dacier M., Wespi A. Towards a taxonomy of intrusion-detection systems // Computer Networks. 1999. vol. 31. Issue 8. P. 805–822.

6. Браницкий А. А., Котенко И. В., Анализ и классификация методов обнаружения сетевых атак // Тр. СПИИРАН, 2016, выпуск 45, 207–244 DOI: https://doi.org/10.15622/sp.45.13 [A. A. Branitskiy, I. V. Kotenko, Analiz i klassifikatsiya metodov obnaruzheniya setevykh atak, Tr. SPIIRAN, 2016, vypusk 45, 207–244 DOI: https://doi.org/10.15622/sp.45.13].

7. Herve Debar, Monique Becker, and Didier Siboni, "A neural network omponent for an intrusion detection system." // Proceedings of the 1992 IEEE Computer Sociecty Symposium on Research in Security and Privacy, pages 240–250, Oakland, CA, USA, May 1992.

8. Rasool Jalili, Fatemeh Imani-Mehr, Morteza Amini, Hamid Reza Shahriari, "Detection of Distributed Denial of Service Attacks Using Statistical Pre- Processor and Unsupervised Neural Networks." // Lecture notes in computer science, 2005.

9. Смелянский Р.Л., Качалин А.И. "Применения нейросетей для обнаружения аномального поведения объектов в компьютерных сетях"./ Факультет Вычислительной Математики и Кибернетики, МГУ им. М. В. Ломоносова, Москва, 2004.

10. Neural network and artificial immune systems for malware and network intrusion detection / V. Golovko [et al.] // Studies in computational intelligence. – Heidelberg, 2010. – Vol. 263: Advances in machine learning II. – P. 485–513.

11. Muna, A. H., Moustafa, N., & Sitnikova, E. (2018). Identification of malicious activities in industrial internet of things based on deep learning models. Journal of Information Security and Applications, 41, 1–11.

12. Sung Jin Kim, Woo Yeon Jo, Taeshik Shon. APAD: Autoencoder-based Payload Anomaly Detection for industrial IoE. December 2019 Applied Soft Computing 88:106017. DOI: 10.1016/j.asoc.2019.106017.

13. Baldi P. Autoencoders, unsupervised learning, and deep architectures //Proceedings of ICML workshop on unsupervised and transfer learning. – 2012. – С. 37–49.

14. Schmidhuber J. Deep learning in neural networks: An overview //Neural networks. – 2015. – Т. 61. – С. 85–117.

15. Goodfellow I. et al. Generative adversarial nets //Advances in neural information processing systems. – 2014. – С. 2672–2680.

16. Madry A. et al. Towards deep learning models resistant to adversarial attacks //arXiv preprint arXiv:1706.06083. – 2017.

17. Donahue J., Krähenbühl P., Darrell T. Adversarial feature learning //arXiv preprint arXiv:1605.09782. – 2016.

References

1. Volkova V.N. Osnovy teorii sistem i sistemnogo analiza / V.N. Volkova, A.A. Denisov. – SPb: Izd-vo SPbGTU, 1999. – 512 s.

2. Fleyshman B.S. Osnovy sistemologii / B.S. Fleyshman. – M.: Radio i svyaz'. 1982. – 368 s.

3. Tyrsin A.N. O matematicheskom modelirovanii slozhnykh organizatsionnykh sistem // Organizatsiya i upravlenie effektivnost'yu i proizvoditel'nost'yu proizvodstvennykh i sotsial'nykh sistem: Mater. mezhd. nauchno-prakt. konf. – Novocherkassk: YuRGTU (NPI), 2005. – S. 49 – 50.

4. Birger I.A. Tekhnicheskaya diagnostika. – M.: Nauka, 1978. – 239 s.

5. Debar H., Dacier M., Wespi A. Towards a taxonomy of intrusion-detection systems // Computer Networks. 1999. vol. 31. Issue 8. P. 805–822.

6. Branitskiy A.A., Kotenko I.V. Analiz i klassifikatsiya metodov obnaruzheniya setevykh atak. – Trudy SPIIRAN. – 2016. – Vyp. 45 – S. 207 – 244.

7. Herve Debar, Monique Becker, and Didier Siboni, "A neural network omponent for an intrusion detection system." // Proceedings of the 1992 IEEE Computer Sociecty Symposium on Research in Security and Privacy, pages 240–250, Oakland, CA, USA, May 1992.

8. Rasool Jalili, Fatemeh Imani-Mehr, Morteza Amini, Hamid Reza Shahriari, "Detection of Distributed Denial of Service Attacks Using Statistical Pre- Processor and Unsupervised Neural Networks." // Lecture notes in computer science, 2005.

9. Smelyanskiy R.L., Kachalin A.I. Primeneniya neyrosetey dlya obnaruzheniya anomal'nogo povedeniya ob"ektov v komp'yuternykh setyakh //Fakul'tet Vychislitel'noy Matematiki i Kibernetiki, MGU im. M. V. Lomonosova, Moskva, 2004.

10. Neural network and artificial immune systems for malware and network intrusion detection / V. Golovko [et al.] // Studies in computational intelligence. – Heidelberg, 2010. – Vol. 263: Advances in machine learning II. – P. 485–513.

11. Muna, A. H., Moustafa, N., & Sitnikova, E. (2018). Identification of malicious activities in industrial internet of things based on deep learning models. Journal of Information Security and Applications, 41, 1–11.

12. Sung Jin Kim, Woo Yeon Jo, Taeshik Shon. APAD: Autoencoder-based Payload Anomaly Detection for industrial IoE. December 2019 Applied Soft Computing 88:106017. DOI: 10.1016/j.asoc.2019.106017.

13. Baldi P. Autoencoders, unsupervised learning, and deep architectures //Proceedings of ICML workshop on unsupervised and transfer learning. – 2012. – С. 37–49.

14. Schmidhuber J. Deep learning in neural networks: An overview //Neural networks. – 2015. – Т. 61. – С. 85–117.

15. Goodfellow I. et al. Generative adversarial nets //Advances in neural information processing systems. – 2014. – С. 2672–2680.

16. Madry A. et al. Towards deep learning models resistant to adversarial attacks //arXiv preprint arXiv:1706.06083. – 2017.

17. Donahue J., Krähenbühl P., Darrell T. Adversarial feature learning //arXiv preprint arXiv:1605.09782. – 2016.

БУХАРЕВ Дмитрий Александрович, аспирант кафедры защиты информации, ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: bukharevdmitrii@gmail.com

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

РАГОЗИН Андрей Николаевич, кандидат технических наук, доцент кафедры защиты информации, ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: ragozinan@susu.ru

BUKHAREV Dmitriy Aleksandrovich, Post-graduate student of the Department of Information Security, South Ural State University (national research university). Russia, 454080, Chelyabinsk, Lenin Ave., 76. E-mail: bukharevdmitrii@gmail.com

SOKOLOV Alexander Nikolaevich, Ph.D., Associate professor, Head of the Department of Information Security, South Ural State University (national research university). Russia, 454080, Chelyabinsk, Lenin Ave., 76. E-mail: sokolovan@susu.ru

RAGOZIN Andrey Nikolaevich, Ph.D., Associate Professor of the Department of Information Security, South Ural State University (national research university). Russia, 454080, Chelyabinsk, Lenin Ave., 76. E-mail: ragozinan@susu.ru

УДК 004.056.57 Вестник УрФО № 1(47) / 2023, с. 69–80

Гибилинда Р. В., Коллеров А. С., Фартушный А. В. DOI: 10.14529/secur230107

АВТОМАТИЗАЦИЯ ПРОЦЕССА МАРКИРОВКИ ПАКЕТОВ СЕТЕВОГО ТРАФИКА СЕРВИСОВ МГНОВЕННОГО ОБМЕНА СООБЩЕНИЯМИ ПРИ РАССЛЕДОВАНИИ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В статье предлагается решение задачи автоматизации процесса маркировки пакетов сетевого трафика в контексте выявления утечек информации. Маркировка сетевых пакетов зашифрованного трафика осуществляется с использованием методов кластеризации и классификации, инициируемых с помощью сервисов мгновенного обмена сообщениями. В основе решения лежит принцип «минимальной длины описания» (minimum description length – MDL), предназначенный для расчета оптимального количества кластеров. Авторами предлагается метод, позволяющий автоматизировать процесс отбора и маркировки пакетов сетевого трафика для формирования «обучающей выборки», с учетом обоснованного выбора размерности признакового пространства в целях повышения скорости работы метода, а также алгоритмической оценки результатов кластеризации.

Ключевые слова: *инцидент информационной безопасности, кластеризация, трафик, мессенджер.*

AUTOMATION OF INSTANT MESSAGING SERVICES NETWORK TRAFFIC PACKETS MARKING PROCESS IN INFORMATION SECURITY INCIDENTS INVESTIGATION

The article proposes a solution to the task of automating network traffic packets marking process. This solution allows marking network packets of encrypted traffic using clustering and classification methods for detecting information leaks initiated through instant messaging services. The proposed solution is based on the «minimum description length» principle (MDL), designed to calculate the optimal number of clusters. Authors propose network traffic packets marking and selection process automatization method for «training set» creation based on justified selection of feature space dimension in order to increase method working speed and algorithmic evaluation of clustering results.

Keywords: *information security incident, clustering, traffic, messenger.*

Введение

Деятельность любой компании приводит к появлению конфиденциальной информации (коммерческая тайна, персональные данные клиентов, банковская тайна и др.), для которой необходимо обеспечивать защиту от утечки. Наиболее освещаемые в средствах массовой информации утечки указанной информации происходят из-за наличия нелояльных к компании сотрудников (примеры статей, по которым были привлечены к уголовной ответственности сотрудники различных компаний – ч. 2 ст.138, ч. 3 ст. 272, ч. 4 ст. 274.1 УК РФ). Одним из каналов утечки, которым могут воспользоваться нелояльные сотрудники, являются сервисы мгновенного обмена сообщениями (далее – мессенджеры), установленные или запускаемые на рабочих станциях или корпоративных мобильных телефонах. При этом устройства взаимодействуют/работают в корпоративной сети с возможностью передачи информации в сеть Интернет. Согласно результатам исследования [1], 90% опрошенных компаний используют мессенджеры для решения рабочих вопросов (52% российских компаний используют некорпоративные мессенджеры для коммуникаций между сотрудниками). При использовании некорпоративных мессенджеров отсутствует возможность контроля передачи информации по зашифрованному каналу. В итоге специалистам по информационной безопасности организаций (далее – специалист) затруднительно своевременно реагировать и расследовать возникающие инциденты, связанные с утечками.

Существующие системы защиты от утечек (data leakage prevention – DLP) имеют ограниченный функционал (в области анализа зашифрованного трафика) [2], в связи с этим специалисту приходится анализировать поток пакетов сетевого трафика (далее – СТ), исходящий с рабочих устройств сотрудников для определения несанкционированного использования мессенджеров. Следует учитывать, что пакеты СТ мессенджеров, в подавляющем большинстве случаев, передаются в зашифрованном виде. Процесс такого анализа включает применение алгоритмов классификации для определения типа используемого мессенджера [3]. Обучение классификатора предполагает отбор и маркировку пакетов

СТ для формирования «обучающей выборки». В условиях больших объемов передаваемых данных и появления новых типов мессенджеров процесс «ручной» маркировки пакетов СТ становится трудозатратным. В связи с этим возникает потребность в автоматизированном процессе отбора пакетов СТ и их маркировки, позволяющем формировать наборы данных для последующей классификации в любых признаковых пространствах.

Авторами предлагается метод, позволяющий автоматизировать процесс отбора и маркировки пакетов СТ для формирования «обучающей выборки».

1. Выбор признакового пространства для подготовки СТ к обработке алгоритмами классификации

В проведенном ранее исследовании [3] анализировался зашифрованный СТ и предложено использование методов классификации для решения задачи идентификации мессенджеров. Для проведения экспериментов применялся СТ мессенджеров (с указанием количества пакетов): WhatsApp (43100), Discord (45631) и Skype (68453) в суммарном объеме 157184 пакетов. В качестве шума для имитации фоновой активности СТ использовались пакеты почтового клиента и веббраузера в суммарном объеме 108576. Указанный трафик был записан с помощью личных мобильных устройств авторов посредством «зеркалирования» пакетов с личных беспроводных точек доступа.

Учитывая объемы циркулирущего СТ в ходе проведенных экспериментов, а также наличие шифрования данных, для идентификации мессенджеров методами классификации необходимо автоматизировать процесс формирования «обучающей выборки».

В [3] обосновано использование только части пакета зашифрованного СТ без служебной информации, содержащего полезные данные, (полезная нагрузка, payload) для его дальнейшего анализа. Согласно [3], полезная нагрузка представлена в виде вектора переменной длины T = (b_1, b_2, b_3, ... b_h), где b_i – значение i-ого байта пакета, bi ∈ [0,255], h = $h = \overline{1,1460}$ и ограничена максимальным размером блока данных одного пакета (maximum transmission unit – MTU – 1460 байт) [4]. Размерность формируемых векторов приведена к значению 1460 (недостающие элементы дополняются символом 256, который не встречается в стандартных пакетах). Результирующее количество признаков, используемых для анализа, совпадает с размерностью вектора T. Таким образом преобразованный вектор T = (b_1, b_2, b_3, ... b_{1460}), где b_i – i-ый количественный признак, $b_i \in [0,256]$. Из векторов, являющихся промаркированными (соотнесенными с некоторыми классами – мессенджерами) пакетами СТ, создается «обучающая выборка», представленная в виде множества $\mathbb{T} = \{T_n | n = \overline{1,N}\}$, где N – количество векторов.

2. Представление пакетов СТ в виде точек, распределенных в пространстве. Выбор алгоритмов кластеризации

Метод оценки результатов группировки пакетов СТ для формирования «обучающей выборки», предлагаемый авторами, основан на использовании кластерного анализа для элементов множества $\mathbb{T}$. Группировка в дальнейшем позволит производить маркировку (соотнесение с классами – мессенджерами) не каждого пакета в отдельности, а их набора (группы). Рассмотрим подробнее процесс группировки.

Для начала вектор T_n взаимно-однозначно отображается в точку T'_n = (b_1, b_2, b_3, ... b_h), которая является элементом признакового пространства $\mathcal{B}^{1460}$, где $b_h \in [0,256]$.

Отображение пакетов СТ в виде точек T'_n в признаковом пространстве $\mathcal{B}^{1460}$ позволяет применять кластерный анализ с использованием широко распространенных неиерархических алгоритмов DBSCAN [5] и OPTICS [6]. Выбор алгоритмов обоснован произвольной геометрической формой кластеров, образуемых точек T'_n. Так как размерность признакового пространства превышает 3, то отображение данных, в возможном для восприятия трехмерном пространстве, не представляется реализуемым без их предварительной обработки, например, методом главных компонент (МГК, PCA – principal component analysis), как показано на рис. 1. Из рис. 1 видно, что отображение с помощью МГК данных в трехмерном пространстве позволяет предположить возможность группировки данных в кластеры, даже в тех случаях, когда кластеры не имеют строгой геометрической формы.

Существуют несколько зарекомендовавших себя методов («локтя» [7] и «силуэтов» [8]), позволяющих определить значения входных параметров алгоритмов. С их помощью возможно косвенно оценить значения входных параметров алгоритмов DBSCAN (ε и minPts) и OPTICS (minPts) – через определение количества получаемых кластеров k. Па-

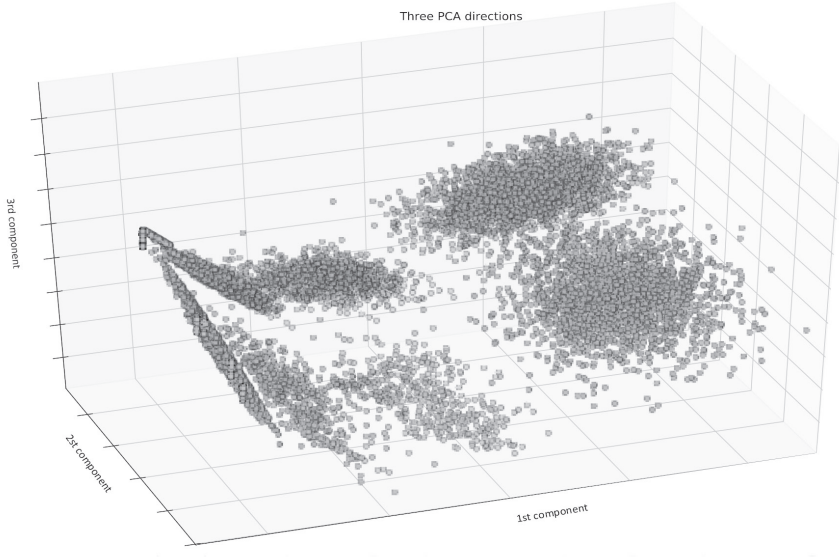


Рис. 1. Пример трехмерного сечения пространства $\mathcal{B}^{1460}$, полученного с использованием МГК

раметр ε – максимальный «размер» окрестности точки, в которой осуществляется поиск ее «соседей». minPts – минимальное число точек в ε окрестности, необходимых для продолжения формирования текущего кластера. Если точки корректно распределены в нужное количество кластеров, то полученные значения входных параметров удовлетворяют условию решаемой задачи группировки. В то же время, данные методы не позволяют автоматизировать процесс подбора входных параметров алгоритма без участия специалиста.

Учитывая указанный недостаток существующих методов определения оптимального значения k, ниже предлагается рассмотреть «принцип минимальной длины описания» (minimum description length – MDL) [9]. Идея MDL заключается в следующем: «Любая закономерность в заданном наборе данных может быть использована для сжатия данных, то есть описания данных с использованием меньшего набора символов, чем нужно для описания данных буквально» [10]. В роли количественной оценки величины, которая необходима для описания набора данных, выступает длина описания L(x). В соответствии с MDL, нахождение минимального значения L(x) позволяет определить оптимальный способ описания данных. Под набором данных понимаются точки на плоскости, связанные с пакетами CT, а закономерностью является принадлежность точек кластерам. В соответствии с MDL, ожидаемым результатом является представление точек на плоскости кластерами, количество которых меньше, чем точек.

В работах [10, 11] показано, что расчет L(x) исследуемых случайно распределённых величин с помощью используемой модели (в рамках исследования моделью является разбиение точек на кластеры) осуществляется по формуле (1):

$$L(x) = -\sum_{x \in X} \log_2 p(x) + \frac{1}{2} P \log_2 |X| \quad (1)$$

Первым слагаемым является отрицательное значение логарифмической функции правдоподобия [12, 11] для всех x ∈ X, где X – множество значений, преобразованных к одномерным скалярным величинам, которые являются компонентами используемой модели. Второе слагаемое – «штраф» за увеличение количества оцениваемых параметров P модели.

Для того, чтобы рассчитать оптимальное значения k необходимо преобразовать дискретно распределенные в пространстве точки к одномерным скалярным величинам. Авторы, по аналогии с работой [13], предлагают воспользоваться расчетом нормы вектора между точкой в пространстве и геометрическим центром кластера. Далее расчет производится с учетом изменений в формуле (1) [14]:

$$L(T', C) = -\sum_{n=1}^{N} \log_2 p(\|T'_n - C\|) + k \log_2 |\mathbb{T}|, \quad (2)$$

где T'_n – точка, ассоциированная с вектором T_n; C – центральная точка кластера (определенная с помощью алгоритма k-медоидов[1]), которому T'_n принадлежит; $p(\|T'_n - C\|)$ – плотность распределения вероятности

[1] Применение алгоритма k-медоидов [15] к сформированному с помощью DBSCAN/OPTICS кластеру позволит определить его центральную точку.

(probability density function – PDF) нормы вектора между T'_n и C; $|\mathbb{T}|$ – количество анализируемых точек.

В ходе экспериментов расчет L(T', C) проводился анализ по оценке применимости различных функций плотности распределения вероятностей и были выбраны оптимальные для применения в MDL быстроубывающие при удалении от центра рассеивания функции плотности распределения вероятности, в отличие от работы [13], где рассматривалось только Гамма-распределение. Дополнительно проведен анализ оптимальных границ диапазонов значений параметров распределений (в рамках решаемой авторами задачи), как указано в табл. 1.

Таблица 1

Значения параметров плотности распределения, используемых при определении оптимального количества кластеров k

Тип распределения	Параметр	Диапазон значений параметра / Оптимальное значение параметра
Нормальное распределение	μ	0-2 / 0
	σ	0.5-1.5 / 1
Гамма-распределение	α	0.5; 1; 2 / 1
	β	0.8-1.1 / 0.9
Распределение χ^2	ν	1-5 / 2

Согласно MDL, оптимальное значение k соответствует минимальному значению L(T', C), рассчитанному по формуле (2). По результатам нахождения оптимального значения k к точкам T'_n применяются выбранные ранее алгоритмы кластеризации DBSCAN или OPTICS с теми значениями входных параметров ε и minPts, при которых получено минимальное . Это возможно осуществить путем перебора параметров алгоритмов DBSCAN (ε и minPts) и OPTICS (только minPts), и на каждом этапе для полученного набора кластеров производить вычисление L(T', C).

Для осуществления перебора параметров алгоритмов необходимо ввести для них граничные значения. Нижней и верхней границами параметра ε будут являться соответственно минимальное и максимальное расстояние между точками T'_n. minPts = 1 не имеет смысла, иначе любая точка будет кластером, следовательно minPts ∈ [2, $|\mathbb{T}|$].

Прерывание цикла перебора значений

Алгоритм № 1: анализ

Input: PDF parameters $\big((\mu,\sigma)|(\alpha,\beta)\big)$, Data ($\mathbb{T}$), Points Amount ($N$)
Result: Clusterized Data (C^*)
1. $\varepsilon_{start}, \varepsilon_{stop}, \varepsilon_{step}$ = processDistances($\mathbb{T}$)
2. $minPts_{start} = 2, minPts_{stop} = N$
3. C^* = clustrize$\Big(\mathbb{T}, minPts_{start}, minPts_{stop}, \varepsilon_{start}, \varepsilon_{stop}, \varepsilon_{step}, (\mu,\sigma)|(\alpha,\beta)\Big)$
4. **return** C^*

Алгоритм № 2: функция «processDistances»

Input: Data ($\mathbb{T}$)
Result: $\varepsilon_{start}, \varepsilon_{stop}, \varepsilon_{step}$
1. $\varepsilon_{start} = \|T'_1 - T'_2\|, \varepsilon_{stop} = 0.0, \varepsilon_{step} = 1.0$
2. **foreach** $T'_n \in \mathbb{T}$ **do**
3. **foreach** $T'_j \in \mathbb{T} \wedge T'_j \neq T'_n$ **do**
4. $d = \|T'_n - T'_j\|$
5. **if** $d > \varepsilon_{stop}$ **then**
6. $\varepsilon_{stop} = d$
7. **end**
8. **if** $d < \varepsilon_{start}$ **then**
9. $\varepsilon_{start} = d$

Окончание таблицы (Алгоритм №2)

```
            end
        end
    end
    if ε_stop < 2.0 then
        ε_step = 0.1
    end
    else if ε_start > 2.0 then
        ε_step = 1.0
    end
    return ε_start, ε_stop, ε_step
```

Алгоритм № 3: функция «clusterize» (for DBSCAN)

Input: Data ($\mathbb{T}$), $minPts_{start}$, $minPts_{stop}$, ε_{start}, ε_{stop}, ε_{step}, PDF Parameters$\big((\mu,\sigma)|(\alpha,\beta)\big)$
Result: Clusterized Data (C^*)

```
foreach ε = overline(ε_start, ε_stop, ε_step) do
    foreach minPts = overline(minPts_start, minPts_stop) do
        O = DBSCAN(𝕋, ε, minPts)
        if ∀ o ∈ O o = noise then
            break
        end
        C = centroids (O, 𝕋, minPts_stop)
        L(T', C) = countDL(O, C, 𝕋, (μ, σ)|(α, β))
        𝕃 ← {L(T', C), ε, minPts}
    end
end
MDL = min(𝕃)
ε, minPts ← MDL
C* = DBSCAN(𝕋, ε, minPts)
return C*
```

Алгоритм № 4: функция «centroids»

Input: Points Cluster Labels (O), Data ($\mathbb{T}$), Points Amount ($minPts_{stop}$)
Result: Cluster Centroids Array (C)

```
foreach cNum ∈ unique(O) do
    foreach pointIndex ∈ overline(0, minPts_stop) do
        if O(T'_pointIndex ∈ 𝕋) = cNum then
            mergedPointsArray← T'_pointIndex
        end
    end
    C ←(cNum, KMedoids(nClusters = 1, mergedPointsArray))
end
return C
```

minPts осуществляется в том случае, если алгоритм кластеризации определил все точки как шум. Для процедуры определения значений параметров DBSCAN выход из цикла перебора minPts приводит к увеличению ε, а для OPTICS – к окончанию процедуры.

Тестирование метода проводилось с использованием типовых наборов данных с известным количеством кластеров (рис. 4). Результаты работы MDL (реальное количество кластеров – количество кластеров с применением оценки MDL) представлены в табл. 2.

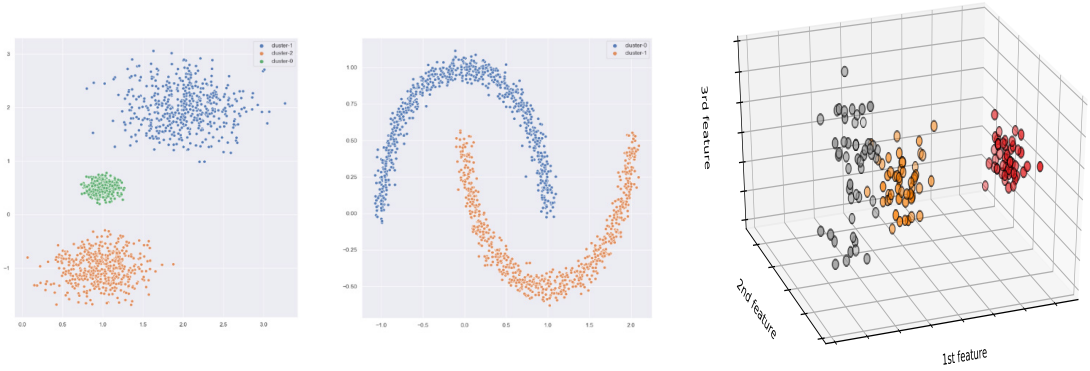
Предложенный метод не во всех случаях позволяет достичь абсолютной точности определения оптимальных параметров кластеризации, особенно когда точки «разреже-

Алгоритм № 5: функция «countDL»

Input: Points Cluster Labels (O), Cluster Centroids Array (C), Data ($\mathbb{T}$), Points Amount ($minPts_{stop}$), PDF Parameters$\big((\mu,\sigma)|(\alpha,\beta)\big)$

Result: Description Length $L(T',C)$

1. $likelyHoodFunctionValue = 0$
2. **foreach** $pointIndex \in \overline{0, minPts_{stop}}$ **do**
3. $cNum = O(T'_{pointIndex} \in \mathbb{T}^*)$
4. $value = \log\left(\text{PDF}\left(\left\|T'_{pointIndex} - C(cNum)\right\|, (\mu,\sigma)|(\alpha,\beta)\right)\right)$
5. $likelyHoodFunctionValue = likelyHoodFunctionValue + value$
6. **end**
7. $L(T',C) = -likelyHoodFunctionValue + \text{size}(C)*\|\mathbb{T}\|$
8. **return** $L(T',C)$



а) б) в)

Рис. 4. Типовые наборы данных: а) Blobs, б) NoisyMoons, в) Iris

Таблица 2

Определение количества кластеров с применением MDL

Набор данных	Кол-во кластеров	DBSCAN, точек		OPTICS, точек	
		150	1500	150	1500
Blobs	3	3	3	3	3
NoisyMoons	2	**5**	2	**4**	2
Iris	2	2		2	

ны» в пространстве. Примеры некорректных значений выделены жирным шрифтом в табл. 2.

3. Применение принципа минимальной длины описания для метода отбора пакетов СТ

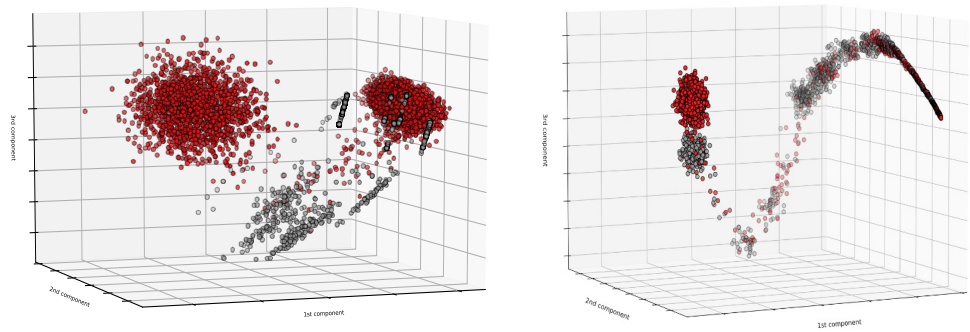
Предложенная оценка входных параметров алгоритмов кластеризации через расчет оптимального k с использованием MDL применена для метода отбора пакетов СТ с целью их группировки и последующей маркировки.

Входными данными являются точки T'_n, соответствующие векторам $T_{n'}$, описывающим пакеты СТ, содержащего в том числе пакеты мессенджеров (пример трехмерных сечений пространства $\mathcal{B}^{1460}$ для мессенджеров WhatsApp и Discord на рис. 5).

Результаты работы метода для алгоритма DBSCAN приведены в табл. 3, а для OPTICS – в табл. 4.

Из значений табл. 4 и 5 видно, что MDL для алгоритмов OPTICS и DBSCAN равен 25,09, при этом точки T'_n были объединены в один кластер. Разбиение точек на два кластера, совпадающее с количеством классов в используемом наборе данных, достигается при L(x) равном 37,64.

Полученная группировка точек на кластеры в последующем должна быть промаркирована специалистом, т.е. соотнесена с классами – мессенджерами. Так, исходя из данных, представленных на рис. 5 и в табл. 4, видно, что сгруппированные в 2 кластера точки (при значении L(x) равном 37,64) мар-



а) б)

Рис. 5. Примеры отображения трехмерных сечений пространства $\mathcal{B}^{1460}$ (точки T'_n, содержащие пакеты мессенджеров WhatsApp и Discord)

Таблица 3

Результаты MDL для оценки работы DBSCAN

L(x)	ε	minPts	Кол-во кластеров
25,09	4	303	1 и шум[2]
37,64	3	298	2 и шум
50,19	3	301	3 и шум
62,73	3	304	4 и шум
75,28	3	306	5 и шум
87,82	3	307	6 и шум
100,37	3	311	7 и шум
112,92	3	314	8 и шум
…			

Таблица 4

Результаты MDL для оценки работы OPTICS

L(x)	minPts	Кол-во кластеров
25,09	5 – 161	1 и шум
25,09	351-650	1 и шум
37,64	161 – 350	2 и шум
100,37	4	7 и шум
263,47	3	20 и шум
2802,63	2	219 и шум

кируются следующим образом: левая и правая верхние группы («шарообразные» кластеры) маркируются как класс WhatsApp, а нижняя группа (кластер произвольной формы) – как Discord.

4. Ускорение подсчета MDL за счет уменьшения признакового пространства

Большое количество признаков снижает скорость кластеризации, анализа данных, а также может отрицательно повлиять на точность результатов [3]. Возникает необходимость обоснованного выбора признаков в целях снижения размерности пространства $\mathcal{B}^{1460}$. Применение алгоритма XGBoost [16] при решении задачи классификации позволило построить диаграмму значимости признаков (рис. 6). Расчет метрики F-мера [17] для построенных моделей с разным количеством признаков от 1460 до 3, отсортированных по важности, приведен в таблице 5. Из расчетов видно, что значимыми для обучения модели являются h*=17 признаков из 1460 (для мессенджера WhatsApp показатели метрики повысились, а для остальных уменьшение размерности признакового пространства не повлияло на F-мера).

Таким образом, вектор T преобразуется в T*, содержащий 17 признаков (список вы-

[2] Разрозненные точки в пространстве, не отнесенные ни к одному кластеру

бранных признаков: 4, 5, 6, 8, 10, 11, 295, 452, 456, 863, 1205, 1399, 1404, 1407, 1412, 1435, 1439). Полученное множество векторов $\mathbb{T}^* = \{T_n^* | n = \overline{1, N}\}$ будет являться входными данными для последующего отбора пакетов СТ.

Результаты работы метода в пространстве $\mathcal{B}^{17}$ для алгоритма DBSCAN приведены в табл. 6, а для OPTICS – в табл. 7.

Из значений табл. 3 и 6 видно, что MDL для алгоритма DBSCAN в пространствах $\mathcal{B}^{17}$ и $\mathcal{B}^{1460}$ равен 37,64, полученное количество кластеров соответствует количеству мессенджеров в трафике, при этом скорость подсчета MDL для пространства, содержащего 17 признаков, на порядок выше.

Применение MDL к алгоритму OPTICS в пространстве $\mathcal{B}^{17}$ (табл. 7) показывает худшие

Рис. 6. График распределения признаков по степени их значимости

Таблица 5

Результаты расчета метрики F-мера для моделей с разным количеством признаков

Кол-во признаков	Мессенджер			
	Discord	WhatsApp	Skype	Шум (https)
3	0,97	0,87	0,89	0,78
…				
7	0,97	0,89	0,92	0,84
8	0,97	0,9	0,91	0,82
9	0,97	0,9	0,92	0,83
10	0,97	0,9	0,92	0,82
11	0,97	0,91	0,91	0,82
…				
16	0,97	0,91	0,92	0,83
17	**0,97**	**0,92**	**0,92**	**0,83**
18	0,97	0,91	0,92	0,83
19	0,97	0,91	0,92	0,83
…				
30	0,97	0,91	0,91	0,82
…				
1460	0,97	0,91	0,92	0,85

Таблица 6

Результаты MDL для оценки работы DBSCAN в признаковом пространстве $\mathcal{B}^{17}$

L(x)	ε	minPts	Кол-во кластеров
37,64	111	5	2 и шум
50,19	106	4	4
50,19	111	4	4
62,73	113	4	5
547,59	1	118	3
554,3	1	117	3
576,27	116	6	3

Таблица 7

Результаты MDL для оценки работы OPTICS в признаковом пространстве $\mathcal{B}^{17}$

L(x)	minPts	Кол-во кластеров
109518,64	32	24
112777,21	3	720
113383,46	26	32
115623,88	27	29
119265,05	4	486
124971,38	33	25
129084,96	31	26

результаты в сравнении с DBSCAN. Это объясняется тем, что процедура определения ε в OPTICS завершается раньше, чем достигается минимальное значение расстояния между точками T'_n в наборе данных.

Исходя из представленного количества точек, маркировка кластеров существенно сокращает временные затраты на формирование «обучающей выборки» в сравнении с маркировкой каждого пакета по отдельности.

Заключение

Предложенный метод группировки пакетов СТ (соотнесенных через векторы T_n, взаимно-однозначно отображенные в точки T'_n) в разных признаковых пространствах позволяет автоматизировать процесс их отбора в целях маркировки для формирования «обучающей выборки». В последующем обученный на основании такой выборки классификатор позволит проанализировать данные в тех признаковых пространствах, которые не могут быть представлены для «ручного» анализа специалистом, но наблюдаются при определении несанкционированного использования мессенджеров.

Литература

1. Большинство российских компаний используют мессенджеры для рабочих вопросов [Электронный ресурс]. URL: https://new-retail.ru/novosti/retail/bolshinstvo_rossiyskikh_kompaniy_ispolzuyut_messendzhery_dlya_rabochikh_voprosov3492. (дата обращения: 01.08.2022).

2. Shabtai A., Elovici Y., Rokach L. A Survey of Data Leakage Detection and Prevention Solutions. Boston, Springer, 2021.

3. Kollerov A.S., Pyr'ev M.S., Fartushnyy A.V. Analysis of Node Interaction Using the TLS Protocol by Means of Machine Learning Tools // 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT 2020), P. 524–526.

4. RFC 1191 - Path MTU Discovery [Электронный ресурс]. URL: https://datatracker.ietf.org/doc/html/rfc1191. (дата обращения: 01.08.2022).

5. Ester M., Kriegel H.P., Sander J., Xiaowei Xu. A density-based algorithm for discovering clusters in large spatial databases with noise // Proceedings of the Second International Conference on Knowledge Discovery and Data Mining (KDD-96), 1996, P. 226–231.

6. Ankerst M., Breunig M.M., Kriegel H.P., Sander J. OPTICS: Ordering Points To Identify the Clustering Structure // ACM SIGMOD International Conference on Management of Data (1999), P. 49–60.

7. Thorndike R.L. Who belongs in the family? // Psychometrika, vol. 18 (1953), P. 267–276.

8. Rousseeuw P.J. Silhouettes: a Graphical Aid to the Interpretation and Validation of Cluster Analysis // Computational and Applied Mathematics, vol. 20 (1987), P. 53–65.

9. Rissanen J. Modeling by shortest data description // Automatica, vol. 14 (1978), P. 465–471.

10. Rissanen J. A Universal Prior for Integers and Estimation by Minimum Description Length // The Annals of Statistics, vol. 11 (1983), no. 2, P. 416–431.

11. Roberts S. J. Novelty Detection using Extreme Value Statistics // IEE Proceedings – Vision Image and Signal Processing, vol. 146 (1999), no. 3, P. 124–129.

12. Fisher R. On the mathematical foundations of theoretical statistics // Philosophical Transactions of the Royal Society, vol. 222 (1922), P. 309–368.

13. Using minimum description length to optimize the 'k' in k-medoids. [Электронный ресурс]. URL: http://erikerlandson.github.io/blog/2016/08/03/x-medoids-using-minimum-description-length-to-identify-the-k-in-k-medoids. (дата обращения: 21.03.2022).

14. Гибилинда Р.В. Кластеризационный метод идентификации воздействий на файлы с применением алгоритма k-средних, используемый при расследовании инцидентов информационной безопасности // Вестник УрФО. Безопасность в информационной сфере. – 2020. – Вып. 35 – № 1. – С. 35–47.

15. Kaufman L., Rousseeuw P.J. Clustering by means of medoids // Statistical Data Analysis Based on the L1-Norm and Related Methods, North-Holland, Elsevier (1987), P. 405–416.

16. XGBoost [Электронный ресурс]. https://github.com/dmlc/xgboost. (дата обращения: 01.08.2022).

17. Rijsbergen C.J. Information Retrieval. 2nd Edition. Butterworth, 1979.

References

1. Bol'shinstvo rossiyskikh kompaniy ispol'zuyut messendzhery dlya rabochikh voprosov [Elektronnyy resurs]. URL: https://new-retail.ru/novosti/retail/bolshinstvo_rossiyskikh_kompaniy_ispolzuyut_messendzhery_dlya_rabochikh_voprosov3492. (data obrashcheniya: 01.08.2022).

2. Shabtai A., Elovici Y., Rokach L. A Survey of Data Leakage Detection and Prevention Solutions. Boston, Springer, 2021.

3. Kollerov A.S., Pyr'ev M.S., Fartushnyy A.V. Analysis of Node Interaction Using the TLS Protocol by Means of Machine Learning Tools // 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT 2020), P. 524–526.

4. RFC 1191 - Path MTU Discovery [Elektronnyy resurs]. URL: https://datatracker.ietf.org/doc/html/rfc1191. (data obrashcheniya: 01.08.2022).

5. Ester M., Kriegel H.P., Sander J., Xiaowei Xu. A density-based algorithm for discovering clusters in large spatial databases with noise // Proceedings of the Second International Conference on Knowledge Discovery and Data Mining (KDD-96), 1996, P. 226–231.

6. Ankerst M., Breunig M.M., Kriegel H.P., Sander J. OPTICS: Ordering Points To Identify the Clustering Structure // ACM SIGMOD International Conference on Management of Data (1999), P. 49–60.

7. Thorndike R.L. Who belongs in the family? // Psychometrika, vol. 18 (1953), P. 267–276.

8. Rousseeuw P.J. Silhouettes: a Graphical Aid to the Interpretation and Validation of Cluster Analysis // Computational and Applied Mathematics, vol. 20 (1987), P. 53–65.

9. Rissanen J. Modeling by shortest data description // Automatica, vol. 14 (1978), P. 465–471.

10. Rissanen J. A Universal Prior for Integers and Estimation by Minimum Description Length // The Annals of Statistics, vol. 11 (1983), no. 2, P. 416–431.

11. Roberts S. J. Novelty Detection using Extreme Value Statistics // IEE Proceedings – Vision Image and Signal Processing, vol. 146 (1999), no. 3, P. 124–129.

12. Fisher R. On the mathematical foundations of theoretical statistics // Philosophical Transactions of the Royal Society, vol. 222 (1922), P. 309–368.

13. Using minimum description length to optimize the 'k' in k-medoids. [Elektronnyy resurs]. URL: http://erikerlandson.github.io/blog/2016/08/03/x-medoids-using-minimum-description-length-to-identify-the-k-in-k-medoids. (data obrashcheniya: 21.03.2022).

14. Gibilinda R.V. Klasterizatsionnyy metod identifikatsii vozdeystviy na fayly s primeneniem algoritma k-srednikh, ispol'zuemyy pri rassledovanii intsidentov informatsionnoy bezopasnosti // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2020. – Vyp. 35 – № 1. – C. 35-47.

15. Kaufman L., Rousseeuw P.J. Clustering by means of medoids // Statistical Data Analysis Based on the L1-Norm and Related Methods, North-Holland, Elsevier (1987), P. 405–416.

16. XGBoost [Elektronnyy resurs]. https://github.com/dmlc/xgboost. (data obrashcheniya: 01.08.2022).

17. Rijsbergen C.J. Information Retrieval. 2nd Edition. Butterworth, 1979.

ГИБИЛИНДА Роман Владимирович, кандидат технических наук, доцент учебно-научного центра «Информационная безопасность», Институт радиоэлектроники и информационных технологий-РтФ Уральский федеральный университет им. первого Президента России Б.Н. Ельцина. Россия, 620002, г. Екатеринбург, ул. Мира, 19. E-mail: r.v.gibilinda@urfu.ru

КОЛЛЕРОВ Андрей Сергеевич, кандидат технических наук, доцент, доцент учебно-научного центра «Информационная безопасность» Институт радиоэлектроники и информационных технологий-РтФ Уральский федеральный университет им. первого Президента России Б.Н. Ельцина. Россия, 620002, г. Екатеринбург, ул. Мира, 19. E-mail: a.s.kollerov@ urfu.ru

ФАРТУШНЫЙ Андрей Владимирович, ассистент учебно-научного центра «Информационная безопасность» Институт радиоэлектроники и информационных технологий-РтФ Уральский федеральный университет им. первого Президента России Б.Н. Ельцина. Россия, 620002, г. Екатеринбург, ул. Мира, 19. E-mail: a.v.fartushnyi@urfu.ru

GIBILINDA Roman Vladimirovich, candidate of technical sciences, Associate Professor of Educational and Scientific Center "Information Security", Institute of Radio electronics and Information Technologies, Ural Federal University named after first President of Russia B.N. Yeltsin. 620002, Yekaterinburg, Mira str., 19. E-mail: r.v.gibilinda@urfu.ru.

KOLLEROV Andrey Sergeevich, candidate of technical sciences, Associate Professor, Associate Professor of Educational and Scientific Center "Information Security", Institute of Radio electronics and Information Technologies, Ural Federal University named after first President of Russia B.N. Yeltsin. 620002, Yekaterinburg, Mira str., 19. E-mail: a.s.kollerov@ urfu.ru.

FARTUSHNYI Andrey Vladimirovich, assistant of Educational and Scientific Center "Information Security", Institute of Radio electronics and Information Technologies, Ural Federal University named after first President of Russia B.N. Yeltsin. 620002, Yekaterinburg, Mira str., 19. E-mail: a.v.fartushnyi@ urfu.ru.

УДК 004.056 Вестник УрФО № 1(47) / 2023, с. 81–97

Голушко А.П., Жуков В.Г.

DOI: 10.14529/secur230108

ПРЕЦЕДЕНТНОЕ ОПРЕДЕЛЕНИЕ ПАРАМЕТРОВ КОНФИГУРИРОВАНИЯ, ОБЕСПЕЧИВАЮЩИХ РЕАЛИЗАЦИЮ МЕР ЗАЩИТЫ ИНФОРМАЦИИ

В статье рассматривается решение задачи определения параметров конфигурирования объектов информатизации и применяемых средств защиты, которые бы могли обеспечить противодействие компьютерным атакам. В качестве источника информации о сценариях проведения атак предлагается использовать результаты прецедентного анализа из базы знаний MITRE ATT&CK. Продемонстрирована возможность интеграции результатов прецедентного анализа информации о тактиках и техниках проведения атак организованными группами злоумышленников в процесс определения и настройки параметров конфигурирования и оценки эффективности реализуемых мер защиты с учетом существующих требований безопасности. Представлены результаты применения предлагаемого подхода на примере отдельно взятой тактики.

Ключевые слова: *защита информации, проектирование системы защиты информации, меры защиты информации, MITRE ATT&CK, эмуляция активности злоумышленника, Atomic Red Team.*

PRECEDENT DEFINITION OF CONFIGURATION PARAMETERS THAT ENSURE THE IMPLEMENTATION OF INFORMATION SECURITY MEASURES

The article is devoted to the scientific and practical problem of determining the configuration parameters of information infrastructure and its information security system, which could provide counteraction to modern methods of computer attacks. It is proposed to use MITRE ATT&CK matrices as a source of systemized analysis of computer attacks. The article presents the analysis results of systematized source applicability, advantages and limitations, an approach to integration into determining the of configuration parameters and evaluating the effectiveness of security system.

Keywords: *MITRE ATT&CK, FSTEC, information security system development, determination of security system configuration parameters, emulation of malicious activity, Atomic Red Team.*

1. Введение

При проектировании системы защиты информации перед специалистами ставится задача определения параметров настройки программного обеспечения, включая программное обеспечение средств защиты, обеспечивающих выполнение требований безопасности и нейтрализацию актуальных угроз. Наряду с требования нормативно-методических документов применяются существующие рекомендации – лучшие практики конфигурирования.

Однако набор параметров конфигурирования должен не только соответствовать требованиям нормативных документов и лучшим практикам, но также обеспечивать противодействие современным методам компьютерных атак. При внедрении системы защиты и проведении оценки соответствия эффективность системы защиты должна подтверждаться.

Основная сложность для владельцев информационных систем, лицензиатов ФСТЭК России и ФСБ России, осуществляющих проектирование и внедрение систем защиты, заключается в необходимости определять конфигурации, опираясь не только на знания о структурно-функциональных характеристиках системы, применяемых информационных технологиях и потенциально возможных угрозах безопасности, но опираясь также и на реальные прецеденты атак, наиболее объективно определяющие ландшафт угроз, условия их реализации и эффективные меры противодействия действиям злоумышленников.

Актуальность решаемой задачи обусловлена необходимостью единства подхода к обеспечению информационной безопасности – внедрению знаний о методах совершения атак, об активности преступных групп и используемых злоумышленниками инструментах – на всех этапах создания системы защиты: от оценки актуальных угроз и формирования требований до проектирования и внедрения системы защиты.

В результате, на этапе проектирования системы защиты должно определяться кон-

кретное содержание реализуемых мер защиты для предотвращения реализации современных компьютерных атак, а также должны обеспечиваться методы и средства оценки эффективности принятых мер.

2. Описание текущего подхода к процессу конфигурирования программного обеспечения и средств защиты информации

2.1 Описание текущего подхода

В рамках данной работы рассматривается подход к созданию системы защиты информации (далее – СЗИ), осуществляемый в соответствии с требованиями законодательства РФ [1–7].

В процесс создания СЗИ входят в т.ч. следующие мероприятия:

– определение угроз безопасности информации (далее – УБИ), реализация которых может привести к нарушению безопасности информации, и разработку на их основе модели угроз (этап – формирование требований к защите информации);

– определение требований к СЗИ (этап – формирование требований к защите информации);

– проектирование СЗИ (этап – разработка системы защиты информации).

Параметры конфигурирования определяются при проектировании СЗИ и фиксируются в проектной и/или эксплуатационной документации.

При определении требований к параметрам конфигурирования программного обеспечения (далее – ПО) и средств защиты информации (далее – СрЗИ) основными источниками, как правило, являются:

– эксплуатационная документация на ПО, программно-технические средства и СрЗИ;

– рекомендации разработчиков и исследовательских центров (CIS Benchmarks [10]);

– формуляры СрЗИ;

– нормативно-методические документы, например, «Меры защиты информации в государственных информационных системах» [8];

– структурно-функциональные характеристики информационной системы (далее – ИС);

– сведения об уязвимостях и способах реализации УБИ в соответствии с Банком данных угроз безопасности ФСТЭК России (далее – БДУ ФСТЭК России) [11] и региональными или отраслевыми нормативно-правовыми актами;

– международные базы данных об уязвимостях в ПО, например, CVE [12] и др.

На этапе проектирования СЗИ перед специалистами ставится задача определить такие состав и содержание мер защиты (в том числе параметры конфигурации), которое позволит выполнить минимально предъявляемые требования и обеспечить нейтрализацию актуальных УБИ.

На практике специалистам приходится применять «экспертный подход» для определения параметров конфигурации, которые бы могли обеспечить нейтрализацию актуальных УБИ. Такой подход заключается в необходимости поиска информации во внешних источниках и руководстве собственным профессиональным опытом. Меры защиты в большей степени реализуются путем определения параметров в соответствии с лучшими практиками, например, [10] и требованиями регулятора, например, [8]. При этом отсутствует единый методологический подход к проведению контроля на предмет, позволяют ли эти параметры в действительности блокировать современные УБИ.

Дополнительно необходимо отметить, что в связи с применением СрЗИ уровня узла сети, частично или полностью заменяющих стандартные средства операционных систем, при проектировании СЗИ преимущественно осуществляется выбор конфигураций СрЗИ, в то время как штатные средства операционных систем могут оставаться с настройками «по умолчанию» или с теми параметрами, которые применяются для задач системного администрирования.

2.2 Пример определения параметров конфигурации

Для того, чтобы наглядно продемонстрировать возможные результаты интеграции систематизированных сведений о мерах противодействия современным техникам компьютерных атак (далее – КА) в процесс определения параметров конфигурирования, предлагается рассмотреть пример определения параметров конфигурации для некоторой произвольной ИС.

Для рассмотрения были выбраны меры защиты из нескольких групп в соответствии с документом [4], для каждой из которых приведены сведения о выбранных параметрах конфигурирования и потенциально нейтрализуемых УБИ (табл. 1).

При определении параметров конфигурирования специалистами используются ис-

Таблица 1

Выбор параметров конфигурации системы защиты

№ п/п	Меры защиты информации[1]	Параметры конфигурирования	Внутренние документы, отражающие состав и содержание мер защиты в ИС	Нейтрализуемые УБИ[2]
1	ИАФ.1 Идентификация и аутентификация пользователей, ИАФ.3 Управление идентификаторами, ИАФ.4 Управление средствами аутентификации	– Максимальный период неактивности до блокировки экрана: 15 минут; – Количество неудачных попыток аутентификации: от 3 до 10 попыток; – Минимальная длина: не менее 6-8 символов; – Требования к сложности пароля: наличие строчных, прописных букв, цифр и символов – Срок действия пароля: не более 180/120/90/60 дней	Описание технологического процесса обработки информации Положение по идентификации и аутентификации	УБИ.008 Угроза восстановления аутентификационной информации УБИ.100 Угроза обхода некорректно настроенных механизмов аутентификации
2	УПД.2 Реализация необходимых методов, типов и правил разграничения доступа, УПД.4 Разделение полномочий пользователей, администраторов, УПД.5 Назначение минимально необходимых прав и привилегий	– Контроль отсутствия административных прав у учетных записей пользователей на уровне системного и прикладного ПО – Назначение необходимых прав на файлы и каталоги – Назначение необходимых прав в прикладном ПО для обеспечения выполнения трудовых обязанностей	Матрица разграничения прав доступа Инструкции администратора ИБ, системного администратора, пользователей	УБИ.006 Угроза внедрения кода или данных УБИ.028 Угроза использования альтернативных путей доступа к ресурсам
3	ОПС.1 Определение запускаемых компонентов ПО, настройка параметров запуска, ОПС.2 Управление установкой компонентов ПО, определение компонентов, подлежащих установке	Настройка защищенной программной среды: – Прикладное ПО и его компоненты, которым разрешен запуск (например, Microsoft Office и средства чтения pdf документов в пользовательском сегменте, СУБД Postgree SQL, веб-сервер Nginx, docker-контейнеры в серверном сегменте) – Запрет запуска исполняемых файлов . exe и скриптов (.bat, PowerShell)	Перечень ПО и его компонентов, разрешенных к установке в ИС	УБИ.178 Угроза несанкционированного использования системных и сетевых утилит УБИ.188 Угроза подмены программного обеспечения

[1] Состав мер защиты информации формируется на этапе формирования требований к системе защиты информации и фиксируется в Техническом задании на создание системы защиты информации.

[2] В соответствии с требованиями законодательства РФ в качестве основного источника сведений об УБИ применяется БДУ ФСТЭК России, дополнительно могут применяться иные источники.

точники, которые предоставляют отдельно сведения о нейтрализуемых УБИ и уязвимостях [11, 12], требованиях к мерам защиты [8] и рекомендациях по настройке параметров ПО [10].

3. Выбор систематизированного источника информации о методах современных компьютерных атак для интеграции

На текущий момент становится важным интегрировать знания о проведенных КА по всему миру в процесс создания СЗИ, поскольку эти сведения формируют реальный ландшафт актуальных УБИ и могут служить источником эффективных мер противодействия действиям злоумышленников.

Это направление развития высоко оценивается и методически поддерживается регулятором. Такой практико-ориентированный подход теперь должен применяться на этапе разработки модели угроз в соответствии с новой методикой оценки угроз безопасности, утвержденной ФСТЭК России [9].

Согласно данной методики оценка актуальности угроз осуществляется посредством построения возможных сценариев их реализации. Сценарии реализации УБИ формируются из состава тактик и техник действий злоумышленников, которые были определены в результате апостериорного анализа инцидентов информационной безопасности. Проектируемая СЗИ должна обеспечить блокирование техник из состава актуальных сценариев реализации УБИ.

Совместными усилиями различных организаций в течение нескольких лет собирались и систематизировались знания о мерах противодействия актуальным УБИ, которые могут быть интегрированы в существующий процесс проектирования СЗИ в целях повышения их эффективности против современных КА.

Так, например, центр компьютерной безопасности Австралии (Australian Cyber Security Centre) выпускает рекомендации по конфигурированию операционных систем, веб-ресурсов и иных компонентов ИС [13], в т.ч. определяет меры, внедрение которых направлено на минимизацию рисков возникновения инцидентов в разных организациях [14].

В качестве основного источника для выбора безопасных конфигураций ПО серверов, рабочих станций и сетевого оборудования часто выступают рекомендации CIS Benchmarks [10].

Однако наиболее подходящим с точки зрения единства методологического подхода источником информации о мерах противодействия современным КА является систематизированная база знаний о тактиках и техниках действий злоумышленников Adversarial Tactics, Techniques & Common Knowledge (далее – ATT&CK), разработанная компанией MITRE [15].

ATT&CK представляет собой постоянно растущий систематизированный ресурс информации о результатах апостериорного анализа поведения злоумышленников при совершении КА. Общая структура MITRE ATT&CK представлена на рис. 1.

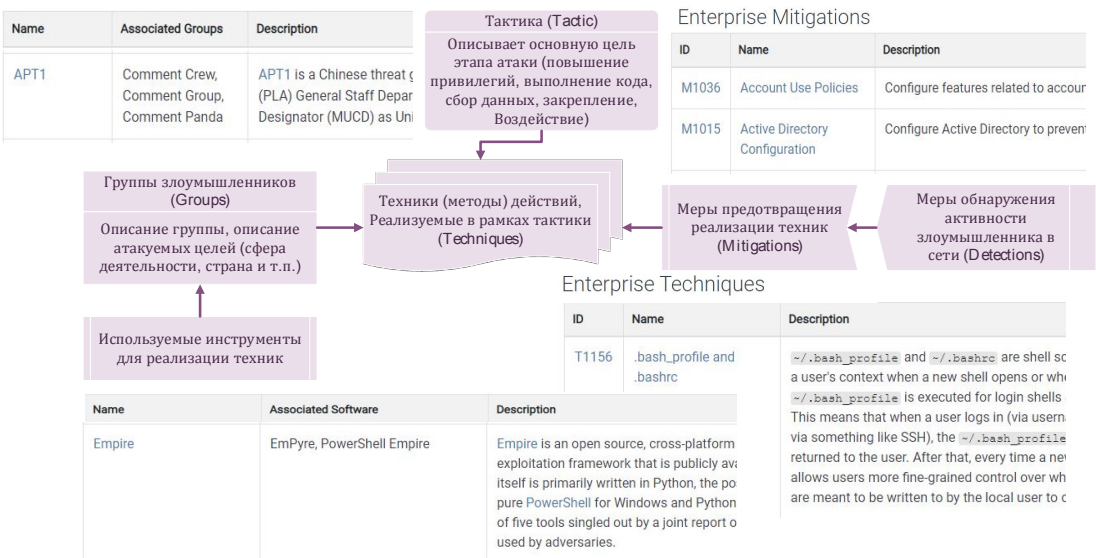


Рис. 1. Структура базы знаний MITRE ATT&CK

В рамках настоящей работы наибольший интерес представляют сведения о возможных мерах защиты и предотвращения возможности реализации техник (Mitigations).

В состав мер противодействия техникам, описанных в категории ATT&CK Enterprise, входит более сорока мер. Каждая мера имеет ссылки на нейтрализуемые с ее применением техники и соответственно суб-техники.

4. Анализ применимости ATT&CK к задаче определения конфигурации системы защиты информации

Представленные в ATT&CK Enterprise меры противодействия техникам могут быть соотнесены с мерами защиты, определяемыми в соответствии с требованиями документов [4–8]. Пример частичного сравнения мер защиты из [4] и [15] представлен в табл. 2.

Таблица 2

Соотнесение мер противодействия техникам КА и мер защиты, определяемых нормативно-методическими документами

№ п/п	Меры защиты ФСТЭК России	ATT&CK Mitigations
1	ИАФ.1 Идентификация и аутентификация пользователей, ИАФ.3 Управление идентификаторами ИАФ.4 Управление средствами аутентификации	M1032 Multi-factor Authentication M1027 Password Policies M1043 Credential Access Protection M1028 Operating System Configuration
2	УПД.1 Управление учетными записями, УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой), типов (чтение, запись, выполнение) и правил разграничения доступа УПД.4 Разделение полномочий УПД.5 Назначение минимально необходимых прав и привилегий УПД.11 Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	M1026 Privileged Account Management M1022 Restrict File and Directory Permissions M1024 Restrict Registry Permissions M1052 User Account Control M1018 User Account Management M1015 Active Directory Configuration M1028 Operating System Configuration M1054 Software Configuration
3	УПД.3 Управление информационными потоками между устройствами, сегментами ИС, а также иными ИС	M1037 Filter Network Traffic
4	ОПС.1 Определение запускаемых компонентов ПО, настройка параметров запуска, ОПС.2 Управление установкой компонентов ПО, определение компонентов, подлежащих установке ОПС.3 Установка только разрешенного к использованию ПО и его компонентов	M1038 Execution Prevention M1033 Limit Software Installation
5	АН3.1 Выявление, анализ уязвимостей и оперативное устранение АН3.2 Контроль установки обновлений ПО, АН3.3 Контроль работоспособности, параметров настройки и правильности функционирования ПО и СрЗИ	M1051 Update Software M1054 Software Configuration M1016 Vulnerability Scanning M1050 Exploit Protection M1015 Active Directory Configuration M1028 Operating System Configuration M1054 Software Configuration
6	СОВ.1 Обнаружение вторжений	M1031 Network Intrusion Prevention
7	ЗИС.17 Разбиение ИС на сегменты	M1030 Network Segmentation
8	ОДТ.4 Периодическое резервное копирование информации ОДТ.5 Обеспечение возможности восстановления информации с резервных носителей	M1053 Data Backup
9	УПД.17 Обеспечение доверенной загрузки средств вычислительной техники	M1046 Boot Integrity
10	ОЦЛ.1 Контроль целостности ПО, включая ПО СрЗИ	M1025 Privileged Process Integrity M1045 Code Signing

Чтобы подтвердить, что сведения, представленные в базе ATT&CK допустимо считать достаточно информативными для их интеграции в процесс определения параметров настройки ПО и СрЗИ необходимо провести дополнительный анализ уровня детализации состава и содержания мер противодействия техникам ATT&CK.

Для того, чтобы оценить рекомендации о мерах противодействия, в качестве примера рассмотрим несколько техник из состава тактики Lateral Movement. Сведения приведены в табл. 3.

Таблица 3 дополнена столбцом, содержащим сведения о мерах защиты согласно документу [4]. Требования к реализации обозна-

Таблица 3

Анализ уровня детализации представленных сведений о мерах противодействия техникам действий злоумышленников

№ п/п	Техника действий злоумышленника (ATT&CK)	Содержание угрозы	Меры противодействия по MITRE ATT&CK	Меры детектирования действий в сети	Меры защиты по приказам ФСТЭК России
1	T1077-Windows Admin Shares	Скрытые сетевые папки предоставляют возможность удаленного копирования файлов. Примеры: C$, ADMIN$, IPC$ Получение учетных данных администратора позволяет через SMB/RPC создавать назначенные задания, запуск служб и использовать WMI	(M1027) Внедрение парольной политики: создание сложных и уникальных паролей, использование разных паролей на учетных записях локального администратора, (M1026) запрет удаленного входа в систему встроенной учетной записи локального администратора (M1038) Ограничение с применением Software Restriction Policies возможности запуска ПО, которое может быть использовано для эксплуатации SMB и Admin Shares	Централизованный сбор и хранение журналов использования учетных данных для входа в системы Отслеживание действий удаленных пользователей, которые подключаются к Admin Shares, отслеживание инструментов и команд, которые используются для подключения к общим сетевым ресурсам, или осуществляют поиск удаленных систем	ИАФ.1, Идентификация и аутентификация пользователей, ИАФ.3 Управление идентификаторами ИАФ.4 Управление средствами аутентификации ОПС.1 Определение запускаемых компонентов ПО, настройка параметров запуска, ОПС.2 Управление установкой компонентов ПО, определение компонентов, подлежащих установке
2	T1028-Windows Remote Management	Реализуется путем возможности удаленного взаимодействия с машиной через службу WinRM с применением PowerShell или иных программ	(M1042) отключить службу WinRM (M1030) внедрение физической и/или логической сегментации сети. Внедрение DMZ для размещения интернет-сервисов (M1026) в случае если служба WinRM необходима, дефолтные настройки скорректировать - произвести настройку учетных записей, рабочих станций и серверов для разграничения прав доступа	Мониторинг использования WinRM – процессов и действий, выполняемых службой WinRM Соотнесение событий WinRM с другими связанными событиями.	УПД.1 Управление учетными записями пользователей, УПД.2 Реализация необходимых методов, типов и правил разграничения доступа ЗИС.17 Разбиение ИС на сегменты и обеспечение защиты периметров сегментов ИС

ченных мер приведены в документе [8] и включают в себя в т.ч. требования:

– ИАФ.1 (О) При доступе в ИС должна осуществляться идентификация и аутентификация пользователей и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей;

– ИАФ.1 (У.3) должна обеспечиваться многофакторная (двухфакторная) аутентификация для локального/удаленного доступа в систему с правами привилегированных учетных записей (администраторов);

– ИАФ.3 (О) формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство;

– ИАФ.3 (У.2) оператором должно быть обеспечено блокирование идентификатора пользователя через период времени неиспользования не более 90/45 дней;

– ИАФ.3 (У.3) оператором должно быть обеспечено использование различной аутентификационной информации (различных средств аутентификации) пользователя для входа в ИС и доступа к прикладному (специальному) ПО;

– ИАФ.4 (О) изменение аутентификационной информации, заданных их производителями и (или) используемых при внедрении СЗИ;

– ИАФ.4 (О) установление характеристик пароля: а) задание минимальной сложности пароля с определяемыми оператором требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов; б) задание минимального количества измененных символов при создании новых паролей; в) задание максимального времени действия пароля; г) задание минимального времени действия пароля;

– УПД.1 (О) предоставление пользователям прав доступа к объектам доступа ИС, основываясь на задачах, решаемых пользователями;

– УПД.2 (У.1) в ИС правила разграничения доступа должны обеспечивать управление доступом субъектов при входе; (У.2) управление доступом субъектов к техническим средствам, устройствам, внешним устройствам; (У.3, У.4) управление доступом субъектов к объектам, создаваемым общесистемным, прикладным и специальным ПО.

В составе перечисленных требований, например, содержатся требования к паролям и однозначной идентификации пользователей, в т.ч. привилегированных, что коррелирует с мерами противодействия M1026 и M1027 из состава ATT&CK. Однако дополнительные рекомендации по предотвращению реализации атак на конкретные используемые технологии (в примере из таблицы – Windows Admin Shares, WinRM service) дополняют имеющиеся требования и могут быть внедрены при проектировании СЗИ.

Таким образом могут быть сделаны выводы, что сведения, представленные в матрице Enterprise MITRE ATT&CK, дополняют содержание мер защиты практическими рекомендациями, позволяющими определить необходимые параметры конфигурирования.

По результатам проведенного анализа, предлагается подход к интеграции знаний о мерах противодействия техникам КА в процесс определения параметров настройки ПО, включая ПО СрЗИ.

5. Описание предлагаемого подхода к интеграции знаний о мерах противодействия техникам компьютерных атак в процесс определения параметров конфигурирования системы защиты информации

Предлагаемый подход основывается на основных этапах создания (проектирования) СЗИ, которые осуществляются в соответствии с [1–7].

Интеграцию знаний о тактиках и техниках действий злоумышленников предлагается осуществлять после того, как определены минимальные требования к составу мер защиты в соответствии с [4–8].

Область действия подхода охватывает процесс определения параметров конфигурирования системного и прикладного ПО ИС и ПО СрЗИ.

Предлагаемый подход включает в себя следующие этапы:

1. Из общего состава мер защиты осуществляется выбор одной меры или группы мер, для которой необходимо определить минимальные требования по настройке и дополнительные рекомендации по противодействию техникам КА.

2. Определяются параметры настройки в соответствии с требованиями нормативно-методических документов (если требованиями предусмотрены конкретные значения параметров).

3. Осуществляется выбор категории мер противодействия (Mitigations) из состава MITRE ATT&CK, сопоставимой или соответ-

ствующей мерам защиты, выбранным на этапе 1.

4. Для выбранных на этапе 3 категорий мер противодействия к рассмотрению принимаются представленные в MITRE ATT&CK более детализированные рекомендации.

5. Далее во внешних источниках осуществляется поиск конкретных практических рекомендаций для реализации рекомендуемой меры противодействия (в случае если ATT&CK не содержит достаточных сведений по практической реализации). После получения конкретных параметров настройки, которые могут быть внедрены в состав проектируемой СЗИ, данные параметры включаются в итоговый перечень.

6. Дополнительно может осуществляться выбор мер детектирования (обнаружения) активности злоумышленника, реализующего технику. В качестве источника правил обнаружения может использоваться репозиторий аналитик обнаружения, также разработанный компанией MITRE – Cyber Analytic Repository (CAR) [16].

7. Проделанные этапы необходимо провести поочередно для всех мер защиты информации.

Далее рассмотрим пример применения предлагаемого подхода, продемонстрированный на рис. 2.

Пример иллюстрирует следующий порядок действий для каждого этапа подхода:

1. (1 этап) Рассматривается ИС, в отношении которой определен третий класс защищенности (для ИС, классифицированной в соответствии с документом [4]). Выбраны меры защиты ИАФ.1, ИАФ.4, УПД.1.

2. (2 этап) К выбранным мерам предъяв-

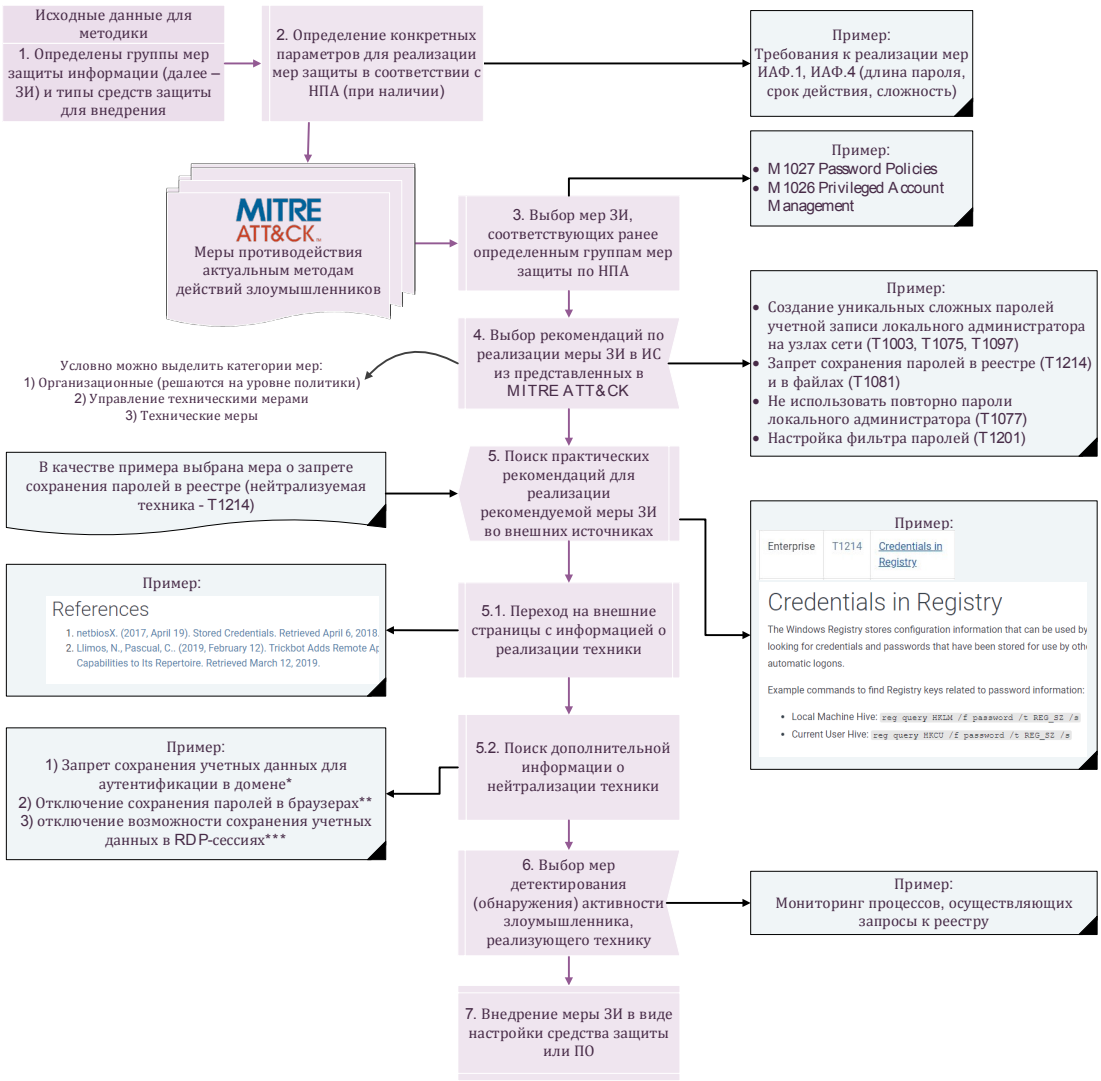


Рис. 2. Пример работы по предлагаемому подходу

ляются следующие требования для установленного класса защищенности: длина пароля должна составлять не менее 6 символов, алфавит пароля не менее 60 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток, блокировка в случае достижения установленного максимального количества неуспешных попыток аутентификации от 5 до 30 минут, срок действия пароля должен составлять не более 120 суток [8].

3. (3 этап) Наиболее подходящими категориями мер противодействия на странице Mitigations являются M1027 Password Policies (парольная политика) и M1026 Privileged Account Management (управление привилегированными пользователями).

Примечание: в примере рассматривается только несколько категорий мер противодействия из общего состава сопоставимых мер.

4. (4 этап) Для категорий M1026 и M1027 были выбраны следующие рекомендации по реализации мер противодействия:

– создание уникальных сложных паролей учетной записи локального администратора на узлах сети (T1003, T1075, T1097);

– запрет сохранения паролей в реестре (T1214) и в файлах (T1081);

– запрет повторного использования пароля локального администратора (T1077);

– настройка фильтра паролей (T1201).

Для дальнейшей демонстрации примера выбрана одна мера из перечисленных выше – запрет сохранения паролей в реестре (нейтрализуемая техника T1214).

5. (5 этап) Изучены сведения о технике действий злоумышленника T1214 Credentials in Registry. Суть реализации техники заключается в возможности осуществления запросов к реестру для перечисления учетных данных, хранимых в нем. После выполнения техники будет отображен любой раздел реестра, содержащий слово «пароль». В результате поиска дополнительной информации были определены рекомендуемые действия для фактической реализации меры защиты:

– настройка сохранения паролей ОС для аутентификации в домене [17];

– не разрешать хранение паролей или учетных данных для сетевой проверки подлинности в RDP-сессиях в соответствии с [18] и [19];

– блокировка сохранения паролей в браузерах на уровне групповых политик домена, например, [20] и [21].

6. (6 этап) Для рассматриваемой техники действий злоумышленника T1214 Credentials in Registry рекомендуется внедрить мониторинг приложений, которые могут быть использованы для запросов к реестру, например, Reg. Также рекомендуется сбор параметров команд, которые могут указывать на поиск учетных данных. В качестве источника для создания правил в SIEM-системе предлагается использовать репозиторий аналитик безопасности CAR [16]. Аналитики содержат в себе описание правил для внедрения в системы управления событиями безопасности и способы их тестирования [22].

7. Проделанные этапы повторяются для всех остальных мер защиты. Кроме того, необходимо учесть, что не все меры на этапе 4 были включены в настоящий пример и они также должны быть проработаны с учетом структурно-функциональных характеристик ИС.

6. Тестирование предлагаемого подхода интеграции знаний о мерах противодействия техникам современных компьютерных атак в существующий процесс проектирования системы защиты.

Для оценки качественных изменений в составе и содержании параметров настройки применим предлагаемый подход к примеру, из табл. 1.

Результаты проделанной работы представлены в табл. 4.

В табл. 4 рекомендации по конфигурированию системы защиты приведены не в полном объеме, но в составе достаточном для демонстрации результатов и составления выводов о применимости предлагаемого подхода. Приведенные рекомендации по конфигурированию указаны преимущественно для ОС Windows. При этом из состава Enterprise Mitigations также могут быть определены меры противодействия техникам для ОС семейства Linux.

Основная сложность при внедрении предлагаемого подхода заключается в необходимости поиска дополнительных сведений о практической реализации мер противодействия техникам действий злоумышленников. Однако формат ресурса ATT&CK требует определенного уровня универсальности приводимых в нем рекомендаций по предотвращению КА, что обуславливает высокоуровневость большинства мер противодействия.

7. Оценка эффективности принятых мер защиты, направленных на противодействие реализации современных угроз безопасности.

По результатам интеграции знаний о мерах противодействия техникам действий злоумышленников в процесс проектирования СЗИ необходимо определить дальнейшие действия по оценке эффективности принятых мер защиты против реализации УБИ. В частности, в ходе работы будут определены конкретные техники, блокирование которых

Таблица 4

Изменения в составе параметров конфигурирования по результатам интеграции предлагаемого подхода

№ п/п	Меры защиты	Параметры конфигурирования, принятые до интеграции знаний о мерах противодействия	Рекомендуемые дополнительные параметры конфигурирования для внедрения	Рекомендуемые дополнительные организационные меры	Нейтрализуемые УБИ и техники действий злоумышленников
1	ИАФ.1, ИАФ.3, ИАФ.4	– Максимальный период неактивности до блокировки экрана: 15 минут; – Количество неудачных попыток аутентификации: от 3 до 10 попыток; – Минимальная длина: не менее 6-8 символов; – Требования к сложности пароля: наличие строчных, прописных букв, цифр и символов – Срок действия пароля: не более 180/120/90/60 дней	– Двукратный сброс пароля учетной записи KRBTGT для деактивации билетов Kerberos (M1015) – Установка сложных паролей длиной более 25 символов для системных учетных записей (M1027); – Включение компонента Windows Defender Credential Guard в Windows 10 (M1043) – Ограничить число учетных записей, для которых разрешено кеширование паролей через параметр HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\cachedlogonscountvalue (M1028) – Настройка через GPO: Computer Configuration > [Policies] > Administrative Templates > SCM: Pass the Hash Mitigations: Apply UAC restrictions to local accounts on network logons (M1028) – не разрешать хранение паролей или учетных данных для сетевой проверки подлинности в RDP-сессиях (M1027) – блокировка сохранения паролей в браузерах на уровне групповых политик домена (M1027)	– Создание сложных и уникальных паролей, использование разных паролей на учетных записях локального администратора (M1027) – Создание различных учетных записей для администрирования и иных задач в ИС (M1027) – Запрет хранения паролей в файлах (M1027) – Установление требования по смене паролей по умолчанию при установке нового оборудования или ПО (M1027)	– УБИ.008 Угроза восстановления аутентификационной информации – УБИ.100 Угроза обхода некорректно настроенных механизмов аутентификации – T1003.005 OS Credential Dumping: Cached Domain Credentials – T1550.002 Use Alternate Authentication Material: Pass the Hash – T1021.002 Remote Services: SMB/Windows Admin Shares – T1558 Steal or Forge Kerberos Tickets T1552 Unsecured Credentials – T1547.008 Boot or Logon Autostart Execution: LSASS Driver

Окончание таблицы 4

2	УПД.2, УПД.4, УПД.5	– Контроль отсутствия административных прав у учетных записей пользователей на уровне системного и прикладного ПО – Назначение необходимых прав на файлы и каталоги, – Назначение необходимых прав в прикладном ПО для обеспечения выполнения трудовых обязанностей	– Замена учетной записи SYSTEM при создании задач, запускаемых по расписанию, на авторизуемую учетную запись через GPO или ключ реестра расположенный по пути HKLM\SYSTEM\CurrentControlSet\Control\Lsa\SubmitControl (M1026) – Запрет входа по RDP для учетной записи локального администратора (M1026) – Настройка фильтров WMI и групп безопасности для ограничения возможности изменения параметров GPO только отдельными учетными записями администраторов (M1026) – Ограничить права на создание logon-скриптов, разрешить только для тех учетных записей администраторов, которым эта функция необходима (M1022) – Задать максимальное время в течение которого может быть активна RDP-сессия и таймауты для проверки состояния (M1028)	– Переодический контроль состава назначенных прав у доменных и локальных учетных записей с целью выявления несанкционированных изменений (M1026)	– УБИ.006 Угроза внедрения кода или данных – УБИ.028 Угроза использования альтернативных путей доступа к ресурсам – T1053 Scheduled Task/Job – T1021.001 Remote Services: Remote Desktop Protocol – T1484 Domain Policy Modification – T1037 Boot or Logon Initialization Scripts – T1563.002 Remote Service Session Hijacking: RDP Hijacking
3	ОПС.1, ОПС.2	Настройка защищенной программной среды: – Прикладное ПО и его компоненты, которым разрешен запуск (например, Microsoft Office и средства чтения pdf документов в пользовательском сегменте, СУБД Postgree SQL, веб-сервер Nginx, docker-контейнеры в серверном сегменте) – Запрет запуска исполняемых файлов .exe и скриптов (.bat, PowerShell)	– В настройках application control запретить возможность запуска двоичных файлов, которые могут быть использованы злоумышленником и их функционирование в ИС не требуется (например, hh.exe, .cpl, CMSTP.exe, InstallUtil.exe, mshta.exe, Odbcconf.exe, Regasm.exe, verclsid.exe, msxsl.exe) (M1038)	–	– УБИ.178 Угроза несанкционированного использования системных и сетевых утилит – УБИ.188 Угроза подмены программного обеспечения – T1218 Signed Binary Proxy Execution – T1220 XSL Script Processing

должно быть обеспечено выбранными конфигурациями системного и прикладного ПО, а также СрЗИ.

В решении задачи оценки эффективности принятых мер защиты может быть применен метод эмуляции активности злоумышленника (adversary emulation), суть которого заключается в попытке успешно реализовать последовательность актуальных для защищаемой инфраструктуры техник из состава ATT&CK.

В качестве программного инструмента для эмуляции можно использовать набор тестов Atomic Red Team [23], который представляет собой свободно-распространяемый ресурс, в котором разработчики своевременно отражают изменения, происходящие в ATT&CK.

Тесты Atomic Red Team содержат в себе инструкции по реализации большинства техник действий злоумышленников. При работе с тестами может потребоваться корректировка приведенных инструкций в связи с возможной разницей в версиях программного обеспечения. Например, в разных версиях PowerShell потребуется использовать разный синтаксис команд.

В качестве примера осуществим эмуляцию техники T1550.002 Use Alternate Authentication Material: Pass the Hash. Суть техники заключается в том, что с помощью хэша пароля злоумышленник может действовать в скомпрометированной системе как будто обладает полными учетными данными [24].

Необходимо скачать и запустить утилиту Mimikatz [25] с использованием хэша пароля доменного администратора, который может быть получен путем реализации техники T1003 OS Credential Dumping. В результате будет запущена командная строка с правами администратора, что дает злоумышленнику неограниченные права в системе (рис. 3).

Утилита Mimikatz имеет широкий функционал и соответственно с применением техники Pass The Hash злоумышленником могут быть достигнуты и другие результаты.

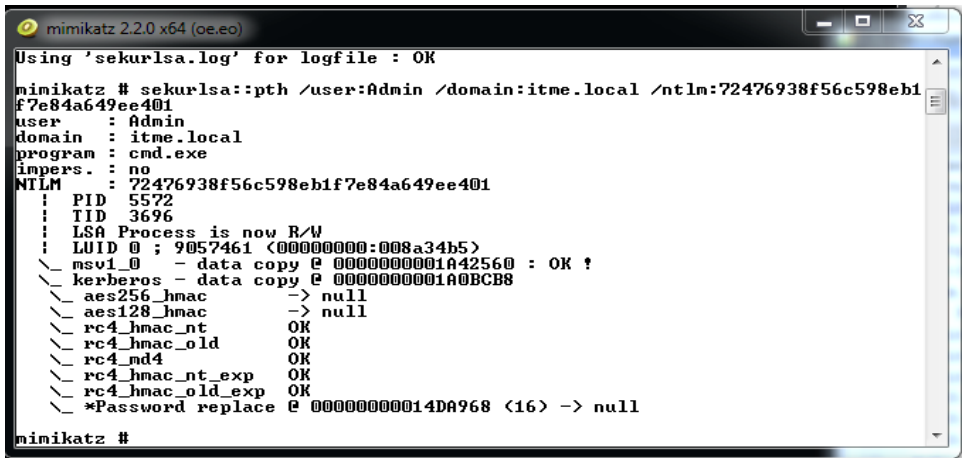


Рис. 3. Эмуляция техники с применением утилиты Mimikatz

Рекомендуемые параметры конфигурирования ИС для противодействия обозначенным техникам частично приведены в таблице 4. При этом необходимо учитывать, что рекомендации в составе ATT&CK Enterprise Mitigations не могут в ряде случаев обеспечить полную блокировку техники, но скорее направлены за увеличение времени и сложности в ее реализации злоумышленником. Это связано, как правило, с особенностями реализации архитектуры операционных систем, в которых многие функции не могут быть полностью отключены или перенастроены так чтобы реализация техники стала невозможна.

Тем не менее, предложенные к внедрению конфигурации выполняют целевую задачу по противодействию техникам действий злоумышленников и рекомендуются для интеграции в состав проектируемой системы защиты.

В результате интеграции знаний о мерах противодействия техникам действий злоумышленников специалистам предоставляется не только возможность выбора безопасных конфигураций для предотвращения реализации УБИ, но также механизм и инструменты для оценки реальной практической защищенности от них.

8. Заключение

Таким образом, в рамках работы был представлен подход по интеграции знаний о мерах противодействия КА в существующий процесс проектирования СЗИ, направленный на нейтрализацию УБИ и, в частности, техник действий злоумышленников через которые эти угрозы могут быть реализованы.

Предлагаемый подход развивает вопрос интеграции знаний о техниках КА, основывающийся на новой методике оценки УБИ, утвержденной ФСТЭК России [10].

Поэтому предлагаемый в рамках настоящей работы подход является одним из этапов развивающегося в России комплексного процесса защиты информации, выстраиваемого с учетом систематизированных и широко применяемых знаний о тактиках и техниках действий злоумышленников.

Литература

1. ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования: национальный стандарт Российской Федерации: издание официальное: утвержден и введен в действие Постановлением Госстандарта России от 30 июня 2000 г. 175-ст. – М.: Стандартинформ, 2022. – Текст: непосредственный.

2. ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы: межгосударственный стандарт: издание официальное: утвержден и введен в действие Постановлением Государственного комитета СССР по стандартам от 24.03.89 № 661. – М.: Стандартинформ, 2022. – Текст: непосредственный.

3. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения: национальный стандарт Российской Федерации: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 28 января 2014 г. № 3-ст. – М.: Стандартинформ, 2022. – Текст: непосредственный.

4. Российская Федерация. Законы. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России от 11.02.2013 № 17. –URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (дата обращения: 14.09.2022). – Текст: электронный.

5. Российская Федерация. Законы. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: приказ ФСТЭК России от 18.02.2013 № 21. – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения: 14.09.2022). – Текст: электронный.

6. Российская Федерация. Законы. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: приказ ФСТЭК России от 25.12.2017 № 239 – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (дата обращения: 14.09.2022). – Текст: электронный.

7. ГОСТ Р 57580.1-2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер: национальный стандарт Российской Федерации: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 08.08.2017 г. № 822-ст. – М.: Стандартинформ, 2020. – Текст: непосредственный.

8. Российская Федерация. Законы. Методический документ Меры защиты информации в государственных информационных системах: утвержден ФСТЭК России 11.02.2014 – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument (дата обращения: 14.09.2022). – Текст: электронный.

9. Российская Федерация. Законы. Методический документ. Методика оценки угроз безопасности информации: утвержден ФСТЭК России 5.02.2021 – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2022-g (дата обращения: 16.09.2022). – Текст: электронный.

10. Center for Internet Security. CIS Benchmarks. – URL: https://www.cisecurity.org/cis-benchmarks/ (дата обращения: 12.09.2022). – Текст: электронный.

11. Банк данных угроз безопасности информации ФСТЭК России. – URL: https://bdu.fstec.ru/threat (дата обращения: 14.09.2022). – Текст: электронный.

12. MITRE CVE. – URL: https://cve.mitre.org/ (дата обращения: 15.09.2022). – Текст: электронный.

13. Australian Cyber Security Centre. View all publications. – URL: https://www.cyber.gov.au/acsc/view-all-content/publications (дата обращения: 12.09.2022). – Текст: электронный.

14. Australian Cyber Security Centre. Strategies to Mitigate Cyber Security Incidents – Mitigation Details. February 2017. – URL: https://www.cyber.gov.au/sites/default/files/2021-10/PROTECT%20-%20Strategies%20to%20Mitigate%20Cyber%20Security%20Incidents%20%E2%80%93%20Mitigation%20Details%20%28February%202017%29.pdf (дата обращения: 12.09.2022). – Текст: электронный.

15. MITRE ATT&CK. – URL: https://attack.mitre.org/ (дата обращения: 12.09.2022). – Текст: электронный.

16. Full Analytic List. – URL: https://car.MITRE.org/wiki/Full_Analytic_List (дата обращения: 16.09.2022). – Текст: электронный.

17. Network access: Do not allow storage of passwords and credentials for network authentication. – URL: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-do-not-allow-storage-of-passwords-and-credentials-for-network-authentication (дата обращения: 16.09.2022). – Текст: электронный.

18. Passwords must not be saved in the Remote Desktop Client. – URL: https://www.stigviewer.com/stig/windows_10/2015-11-30/finding/V-63729 (дата обращения: 16.09.2022). – Текст: электронный.

19. Cached Credentials: Important Facts That You Cannot Miss. – URL: https://cqureacademy.com/blog/windows-internals/cached-credentials-important-facts (дата обращения: 16.09.2022). – Текст: электронный.

20. Disable Browser Password Saving via Group Policy. – URL: https://support.practiceprotect.com/knowledge-base/disable-browser-password-saving-via-group-policy/ (дата обращения: 16.09.2022). – Текст: электронный.

21. Disabling the option to save a password on Internet Explorer. – URL: https://searchsecurity.techtarget.com/answer/Disabling-the-option-to-save-a-password-on-Internet-Explorer (дата обращения: 16.09.2022). – Текст: электронный.

22. CAR-2013-03-001: Reg.exe called from Command Shell. – URL: https://car.MITRE.org/analytics/CAR-2013-03-001/ (дата обращения: 16.09.2022). – Текст: электронный.

23. Atomic-red-team. – URL: https://github.com/redcanaryco/atomic-red-team (дата обращения: 16.09.2022). – Текст: электронный.

24. T1550.002 – Pass the Hash. – URL: https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1550.002/T1550.002.md (дата обращения: 16.09.2022). – Текст: электронный.

25. Mimikatz. – URL: https://github.com/gentilkiwi/mimikatz (дата обращения: 16.09.2022). – Текст: электронный.

References

1. GOST R 51624-2000. Zashchita informatsii. Avtomatizirovannyye si-stemy v zashchishchennom ispolnenii. Obshchiye trebovaniya: natsional'nyy stan-dart Rossiyskoy Federatsii: izdaniye ofitsial'noye: utverzhden i vveden v deystviye Postanovleniyem Gosstandarta Rossii ot 30 iyunya 2000 g. 175-st. – M.: Standartinform, 2022. – Tekst: neposredstvennyy.

2. GOST 34.602-89. Informatsionnaya tekhnologiya. Kompleks standar-tov na avtomatizirovannyye sistemy. Tekhnicheskoye zadaniye na sozdaniye avto-matizirovannoy sistemy: mezhgosudarstvennyy standart: izdaniye ofitsial'-noye: utverzhden i vveden v deystviye Postanovleniyem Gosudarstvennogo komi-teta SSSR po standartam ot 24.03.89 № 661. – M.: Standartinform, 2022. – Tekst: neposredstvennyy.

3. GOST R 51583-2014. Zashchita informatsii. Poryadok sozdaniya avto-matizirovannykh sistem v zashchishchennom ispolnenii. Obshchiye polozheniya: natsional'nyy standart Rossiyskoy Federatsii: izdaniye ofitsial'noye: utverzhden i vveden v deystviye Prikazom Federal'nogo agentstva po tekhnicheskomu regulirovaniyu i metrologii ot 28 yanvarya 2014 g. № 3-st. – M.: Standartinform, 2022. – Tekst: neposredstvennyy.

4. Rossiyskaya Federatsiya. Zakony. Ob utverzhdenii trebovaniy o za-shchite informatsii, ne sostavlyayushchey gosudarstvennuyu taynu, soderzhashcheysya v gosudarstvennykh informatsionnykh sistemakh: prikaz FSTEK Rossii ot 11.02.2013 № 17. –URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (data obrashcheniya: 14.09.2022). – Tekst: elektronnyy.

5. Rossiyskaya Federatsiya. Zakony. Ob utverzhdenii sostava i soderzha-niya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti per-sonal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh perso-nal'nykh dannykh: prikaz FSTEK Rossii ot 18.02.2013 № 21. – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (data obrashcheniya: 14.09.2022). – Tekst: elektronnyy.

6. Rossiyskaya Federatsiya. Zakony. Ob utverzhdenii Trebovaniy po obespecheniyu bezopasnosti znachimykh ob"yektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii: prikaz FSTEK Rossii ot 25.12.2017 № 239 – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (data obrashcheniya: 14.09.2022). – Tekst: elektronnyy.

7. GOST R 57580.1-2017. Bezopasnost' finansovykh (bankovskikh) ope-ratsiy. Zashchita informatsii finansovykh organizatsiy. Bazovyy sostav orga-nizatsionnykh i tekhnicheskikh mer: natsional'nyy standart Rossiyskoy Fede-ratsii: izdaniye ofitsial'noye: utverzhden i vveden v deystviye Prikazom Fe-deral'nogo agentstva po tekhnicheskomu regulirovaniyu i metrologii ot 08.08.2017 g. № 822-st. – M.: Standartinform, 2020. – Tekst: neposred-stvennyy.

8. Rossiyskaya Federatsiya. Zakony. Metodicheskiy dokument Mery za-shchity informatsii v gosudarstvennykh informatsionnykh sistemakh: utverzhden FSTEK Rossii 11.02.2014 – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument (data obrashcheniya: 14.09.2022). – Tekst: elektronnyy.

9. Rossiyskaya Federatsiya. Zakony. Metodicheskiy dokument. Metodika otsenki ugroz bezopasnosti informatsii: utverzhden FSTEK Rossii 5.02.2021 – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2022-g (data obra-shcheniya: 16.09.2022). – Tekst: elektronnyy.

10. Center for Internet Security. CIS Benchmarks, available at: https://www.cisecurity.org/cis-benchmarks/ (accessed: 12.09.2022).

11. Bank dannykh ugroz bezopasnosti informatsii FSTEK Rossii. – URL: https://bdu.fstec.ru/threat (data obrashcheniya: 14.09.2022). – Tekst: elek-tronnyy.

12. MITRE CVE, available at: https://cve.mitre.org/ (accessed: 15.09.2022).

13. Australian Cyber Security Centre. View all publications, available at: https://www.cyber.gov.au/acsc/view-all-content/publications (accessed: 12.09.2022).

14. Australian Cyber Security Centre. Strategies to Mitigate Cyber Security Incidents – Mitigation Details. February 2017, available at: https://www.cyber.gov.au/sites/default/files/2021-10/PROTECT%20-%20Strategies%20to%20Mitigate%20Cyber%20Security%20Incidents%20%E2%80%93%20Mitigation%20Details%20%28February%202017%29.pdf (accessed: 12.09.2022).

15. MITRE ATT&CK, available at: https://attack.mitre.org/ (accessed: 12.09.2022).

16. Full Analytic List, available at: https://car.MITRE.org/wiki/Full_Analytic_List (accessed: 16.09.2022).

17. Network access: Do not allow storage of passwords and credentials for network authentication, available at: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-do-not-allow-storage-of-passwords-and-credentials-for-network-authentication (accessed: 16.09.2022).

18. Passwords must not be saved in the Remote Desktop Client, available at: https://www.stigviewer.com/stig/windows_10/2015-11-30/finding/V-63729 (accessed: 16.09.2022).

19. Cached Credentials: Important Facts That You Cannot Miss, available at: https://cqureacademy.com/blog/windows-internals/cached-credentials-important-facts (accessed: 16.09.2022).

20. Disable Browser Password Saving via Group Policy, available at: https://support.practiceprotect.com/knowledge-base/disable-browser-password-saving-via-group-policy/ (accessed: 16.09.2022).

21. Disabling the option to save a password on Internet Explorer, available at: https://searchsecurity.techtarget.com/answer/Disabling-the-option-to-save-a-password-on-Internet-Explorer (accessed: 16.09.2022).

22. CAR-2013-03-001: Reg.exe called from Command Shell, available at: https://car.MITRE.org/analytics/CAR-2013-03-001/ (accessed: 16.09.2022).

23. Atomic-red-team, available at: https://github.com/redcanaryco/atomic-red-team (accessed: 16.09.2022).

24. T1550.002 – Pass the Hash, available at: https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1550.002/T1550.002.md (accessed: 16.09.2022).

25. Mimikatz, available at: https://github.com/gentilkiwi/mimikatz (accessed: 16.09.2022).

ГОЛУШКО Анна Павловна, аспирант, кафедра безопасности информационных технологий, ФГБОУ ВО «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева». Россия, 660037, Красноярский край, г. Красноярск, пр. имени газеты «Красноярский рабочий», д. 31. E-mail: golushko.ap@yandex.ru

ЖУКОВ Вадим Геннадьевич, кандидат технических наук, доцент кафедры безопасности информационных технологий, ФГБОУ ВО «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева». Россия, 660037, Красноярский край, г. Красноярск, пр. имени газеты «Красноярский рабочий», д. 31. E-mail: zhukov@sibsau.ru

GOLUSHKO Anna Pavlovna, Postgraduate student, Information Technologies Security Department, Reshetnev Siberian State University of Science and Technology. 660037, Krasnoyarsk Territory, Krasnoyarsk, avenue named after the newspaper "Krasnoyarsky Rabochiy", 31. E-mail: golushko.ap@yandex.ru.

ZHUKOV Vadim Gennadievich, Candidate of Technical Sciences, Associate Professor of the Department of Information Technology Security, Reshetnev Siberian State University of Science and Technology. 660037, Krasnoyarsk Territory, Krasnoyarsk, avenue named after the newspaper "Krasnoyarsky Rabochiy", 31. E-mail: zhukov@sibsau.ru

УДК 004.043 Вестник УрФО № 1(47) / 2023, с. 98–101

Гончаренко Ю.Ю.

DOI: 10.14529/secur230109

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН ДЛЯ ПРОВЕРКИ ПОДЛИННОСТИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ И ФАЙЛОВ

В данной статье предложено решение на основе распределенной децентрализованной технологии блокчейн для проверки подлинности электронной документации, проанализирована целесообразность использования и преимущества его внедрения.

На сегодняшний день проблема обеспечения подлинности электронных документов, особенно в их долговременной перспективе, является актуальной задачей, обеспечивающей безопасность обмена электронными данными за счет установления достоверности происхождения документа и целостности передаваемой информации.

В целях создания надежного верификационного центра для электронных документов и файлов было разработано веб-приложение, основанное на технологии блокчейн.

Ключевые слова: *блокчейн, электронный документ, верификация, веб-приложение.*

Goncharenko Y.Y.

USING BLOCKCHAIN TECHNOLOGY TO VERIFY THE AUTHENTICITY OF ELECTRONIC DOCUMENTS AND FILES

In this article, a solution based on distributed decentralized blockchain technology for verifying the authenticity of electronic documentation is proposed, the expediency of using it and the advantages of its implementation are analyzed.

To date, the problem of ensuring the authenticity of electronic documents, especially in their long-term perspective, is an urgent task that ensures the security of electronic data exchange by establishing the authenticity of the origin of the document and the integrity of the transmitted information.

In order to create a reliable verification center for electronic documents and files, a web application based on blockchain technology was developed.

Keywords: *blockchain, electronic document, verification, web application.*

Введение

В настоящее время во всём мире стремительно растет объем документооборота, что значительно расширяет спектр возможностей для злоумышленников по воздействию на какого-либо пользователя, например, таких, как кража данных, подделка документов и авторства и прочее. Это огромная проблема для широкой аудитории и еще большая проблема для предприятия с большим объемом циркулирующих данных [1].

Решением данной проблемы может быть внедрение технологии блокчейн в систему электронного документооборота, т. к. именно она способна защитить данные и сделать их аудит более прозрачным. Стремительность роста использования данной технологии и расширение спектра ее возможного применения позволяет не только обеспечить повышение информационной безопасности данных, но также и повысить уровень оказываемых услуг, предоставляя пользователям большое количество возможностей своего использования [2].

Таким образом, наличие специализированного средства подтверждения подлинности электронных документов и файлов, обусловленное необходимостью обеспечения целостности данных внутри них, является актуальной разработкой в сфере защиты информации. Такой подход к защите информации не позволит видоизменять передаваемые данные, поэтому информация в конечном виде будет полностью соответствовать сведениям, предоставленным и подтвержденным отправителем в изначальном виде [3].

Основная часть

Согласно п.11.1 ст.2 ФЗ «Об информации, информационных технологиях и о защите информации», электронный документ – это «документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах» [4].

При работе с электронными документами большое внимание уделяется гарантии их подлинности, для чего в системе электронного документооборота должны быть предусмотрены механизмы, гарантирующие защищённое хранение конфиденциальных документов, предотвращение несанкционированных изменений документов, копирование их содержимого [5]. Конечно, одним из распространенных способов подтвердить неизменность данных в документе и идентифицировать лицо, его подписавшее, является электронная подпись [6].

Но наличие проблем, связанных с ее использованием, не дают гарантий безопасности [7], поэтому в целях создания надежного верификационного центра для электронных документов и файлов было разработано веб-приложение, основанное на технологии блокчейн. Для написания более адаптивного и расширяемого приложения, было принято решение разделить его на логику взаимодействия пользователя с программным интерфейсом и на сам механизм блокчейна в серверной части приложения. Такая архитектура позволяет написать множество реализаций сценариев взаимодействия пользователя с API системой, например, мобильное приложение (рис. 1).

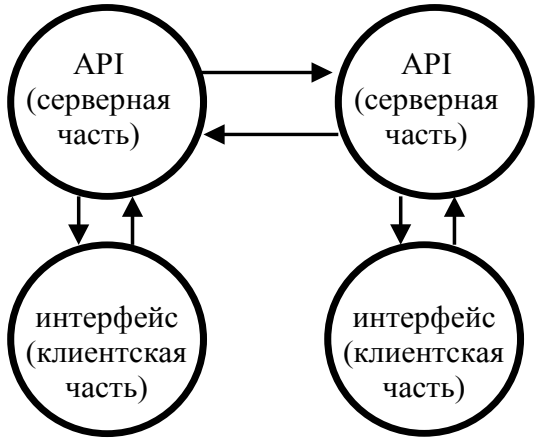


Рис. 1. Логика взаимодействия частей приложения

Основная идея заключается в возможности зарегистрированного пользователя загрузить в систему блокчейн хеш-сумму от документа (рис. 2).

После загрузки файла во временное хранилище веб-приложения происходит перевод файла в формат Base64. К полученной строке символов применяется функция хеширования SHA-256, а ее результат заносится в массив ожидающих транзакций. В свою очередь, пользователю выводится уведомление о добавлении хеш-суммы в блок цепочки блокчейн (рис. 3).

Для добавления нового блока, подтверждения транзакций и верификации единой версии реестра во всех его копиях нахождение консенсуса в системе осуществляется на

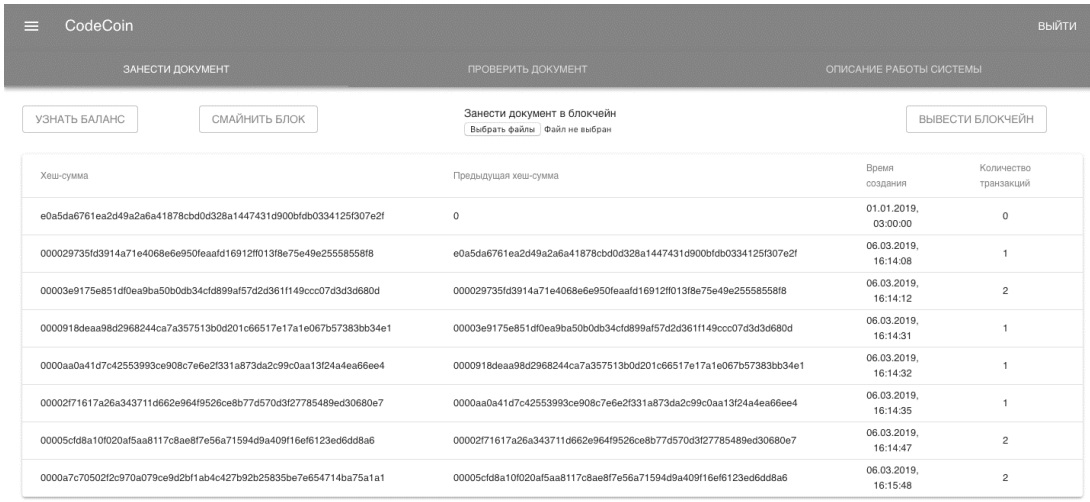


Рис. 2. Главная страница приложения

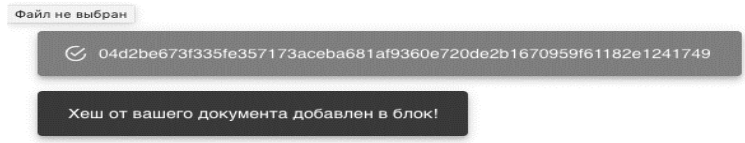


Рис. 3. Уведомление о добавлении в блок и хеш-сумма

основе алгоритма консенсуса Proof of Work (доказательство работы) [8]. Поэтому для закрытия блока и внесения его в цепочку необходимо подобрать такое число (nonce), при котором хеш-сумма от всего блока начиналась бы на «0000». Узлу, нашедшему требуемую хеш-сумму, начисляется 100 единиц (codecoin). При добавлении большого числа пользователей возможно увеличение количества нулей, что способствует росту вычислительной сложности закрытия блока.

После закрытия блока, пользователь всегда сможет удостоверится в том, что его документ был занесен в систему или, что он остался неизмененным. Для этого необходимо указать логин участника, создавшего документ, и ввести от него хеш-сумму. Если документ был зарегистрирован, то система покажет соответствующее уведомление, и есть возможность проверить целостность файла (рис. 4). Пользователь может повторно получить хеш-сумму от файла и проверить, зарегистрирован ли он.

В дальнейшем усовершенствовании системы для занесения документа будет требоваться небольшая сумма «codecoin», как оплата вычислительной мощности узлов, которые просчитывают хеш-функции. Уже на данный момент у зарегистрированных пользователей существуют кошельки с балансами, а также возможность передачи внутренней валюты другим пользователям (рис. 5).

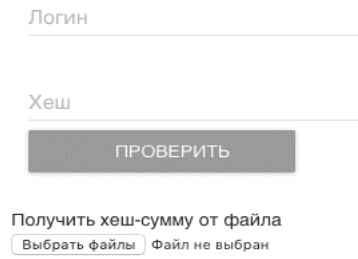


Рис. 4. Проверка файла

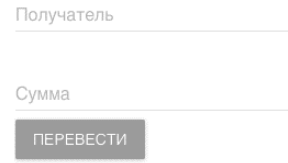


Рис. 5. Перевод codecoin

Выводы

Таким образом, разработанное веб-приложение, основанное на технологии блокчейн, представляет собой надежный верификационный центр для электронных документов и файлов, одним из преимуществ которого является отсутствие потребности хранить электронные копии документов на централизованном сервере, что в первую очередь исключает возможность получения доступа к ним злоумышленникам.

Данное приложение может быть использовано для упрощения взаимодействия между пользователями системы электронного документооборота, имеющими основание не доверять друг другу в вопросах подлинности совместно используемых данных.

Литература

1. Blockchain Usage: List Of 20+ Blockchain Technology Use Cases. – URL: https://101blockchains.com/blockchain-usage/ (дата обращение: 30.01.2023).

2. Гончаренко, Ю.Ю. Программный модуль для контроля и ведения электронного документооборота на основе технологии блокчейн / Ю.Ю. Гончаренко, Д.А. Арзамасцев // Научный результат. Информационные технологии. – Т.5, №3, 2020. – С. 32–40.

3. Гончаренко, Ю.Ю. Качественная оценка методик разработки автоматизированных средств / Ю.Ю. Гончаренко, Г.С. Погуляй, В.В. Пелись, М.Г. Щербаченко // Энергетические установки и технологии, 2022. – Т. 8. № 2. С. 79–86.

4. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями). – URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращение: 30.01.2023).

5. Электронная подпись: что и зачем нужно настроить? – URL: https://docsvision.com/info-centr/articles/elektronnaya-podpis.html (дата обращение: 30.01.2023).

6. Федеральный закон от 06.04.2011 N 63-ФЗ (ред. от 28.12.2022) «Об электронной подписи». – URL: https://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращение: 30.01.2023).

7. Проблемы использования электронной цифровой подписи. – URL: https://studbooks.net/2431093/informatika/problemy_ispolzovaniya_elektronnoy_tsifrovoy_podpisi (дата обращение: 30.01.2023).

8. Что такое алгоритм Proof-of-Work (PoW)? – URL: https://forklog.com/cryptorium/chto-takoe-proof-of-work-i-proof-of-stake (дата обращение: 30.01.2023).

References

1. Blockchain Usage: List Of 20+ Blockchain Technology Use Cases. – Available at: https://101blockchains.com/blockchain-usage/ (accessed 30 January 2023).

2. Goncharenko, YU.YU. Programmnyy modul' dlya kontrolya i vedeniya elektronnogo dokumentooborota na osnove tekhnologii blokcheyn / YU.YU. Goncharenko, D.A. Arzamastsev // Nauchnyy rezul'tat. Informatsionnyye tekhnologii. – T.5, №3, 2020. – S. 32–40.

3. Goncharenko, YU.YU. Kachestvennaya otsenka metodik razrabotki avtomatizirovannykh sredstv / YU.YU. Goncharenko, G.S. Pogulyay, V.V. Pelis', M.G. Shcherbachenko // Energeticheskiye ustanovki i tekhnologii, 2022. – T. 8. № 2. S. 79–86.

4. Federal'nyy zakon ot 27 iyulya 2006 g. N 149-FZ "Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii" (s izmeneniyami i dopolneniyami). – URL: https://www.consultant.ru/document/cons_doc_ LAW_61798/ (data obrashcheniye: 30.01.2023).

5. Elektronnaya podpis': chto i zachem nuzhno nastroit'? – URL: https://docsvision.com/info-centr/articles/elektronnaya-podpis.html (data obrashcheniye: 30.01.2023).

6. Federal'nyy zakon ot 06.04.2011 N 63-FZ (red. ot 28.12.2022) "Ob elektronnoy podpisi". – URL: https://www.consultant.ru/document/cons_doc_ LAW_112701/ (data obrashcheniye: 30.01.2023).

7. Problemy ispol'zovaniya elektronnoy tsifrovoy podpisi. – URL: https://studbooks.net/2431093/informatika/problemy_ispolzovaniya_elektronnoy_tsifrovoy_podpisi (data obrashcheniye: 30.01.2023).

8. CHto takoe algoritm Proof-of-Work (PoW)? Available at: https://forklog.com/cryptorium/chto-takoe-proof-of-work-i-proof-of-stake (accessed 30 January 2023).

ГОНЧАРЕНКО Юлия Юрьевна, доктор технических наук, доцент, профессор кафедры «Информационная безопасность», Федеральное государственное автономное образовательное учреждение высшего образования «Севастопольский государственный университет». Россия, 299053, г. Севастополь, ул. Университетская, 33. E-mail: luliay1985@mail.ru

GONCHARENKO Yuliya Юрьевна, Doctor of Technical Sciences, Associate Professor, Professor of the Department of Information Security, Federal State Autonomous Educational Institution of Higher Education "Sevastopol State University". 299053, Sevastopol, Universitetskaya Street, 33. E-mail: luliay1985@mail.ru

УДК 004.056.52 Вестник УрФО № 1(47) / 2023, с. 102–111

Копытов П.Д., Королёв И.Д., Кулиш О.А., Степанцов С.В.

DOI: 10.14529/secur230110

ПОСТРОЕНИЕ ФОРМАЛЬНЫХ МОДЕЛЕЙ РАСПРОСТРАНЕНИЯ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ ПО ТЕХНИЧЕСКИМ КАНАЛАМ УТЕЧКИ ИНФОРМАЦИИ ДЛЯ ОБЪЕКТОВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ ОТ ТЕХНИЧЕСКИХ СРЕДСТВ РАЗВЕДКИ

В статье рассматривается построение формальной модели для расчёта контрольных точек как возможных установленных технических средств разведки в двухмерном пространстве с дальнейшим переходом в трехмерное евклидово пространство и построение новой обновленной модели.

Ключевые слова: *формальная модель, побочные электромагнитные излучения, средства технические разведки, эффективность защиты, теория Фибоначчи, системы координат, Платоновы тела.*

CONSTRUCTION OF FORMAL MODELS FOR PROPAGATION OF SIDE ELECTROMAGNETIC EMISSIONS THROUGH TECHNICAL CHANNELS OF INFORMATION LEAKAGE FOR COMPUTER EQUIPMENT FROM INTELLIGENCE TECHNICAL TOOLS

The article discusses the construction of a formal model for calculating control points as possible established technical means of reconnaissance in two-dimensional space with a further transition to three-dimensional Euclidean space and the construction of a new updated model.

Keywords: *formal model, spurious electromagnetic radiation, technical intelligence means, protection efficiency, Fibonacci theory, coordinate systems, Platonic Solids.*

Одной из наиболее возможных угроз перехвата информации от объектов вычислительной техники (далее - ОВТ) считается утечка за счёт канала побочных электромагнитных излучений (далее - ПЭМИ), создаваемых техническими средствами. ПЭМИ существуют в диапазоне частот от единицы Гц до полутора ГГц и способны распространять фоновый сигнал, который возможно перехватить за счёт средств технической разведки (далее - СТР). Наиболее опасными источниками ПЭМИ являются дисплеи, проводные линии связи, накопители на магнитных дисках, видеокарты, выходные порты: HDMI, DVI, VGA, слоты PCI Express. Защита информации, обрабатываемой техническими средствами, осуществляется с применением пассивных и активных методов и средств, а также организационными мероприятиями перед вводом ОВТ в эксплуатацию.

При выявлении технических каналов утечки информации СВТ необходимо рассматривать как систему, включающую основные технические средства и системы (ОТСС), непосредственно участвующие в обработке конфиденциальной информации, и вспомогательные технические средства, и системы (ВТСС), не участвующие в обработке конфиденциальной информации, но находящиеся в зоне электромагнитного поля, создаваемого СВТ.

Оценка угрозы утечки информации, вызванной побочными излучениями основных технических средств, производится путём сравнения радиусов зон потенциального перехвата опасных сигналов с размерами контролируемых зон организации. Различают 2 вида зон вокруг систем вычислительной техники:

1. Зона с радиусом R_1 – пространство вокруг ОТСС, в пределах которого не допускается размещение ВТСС, через которое может происходить утечка информации за пределы контролируемой зоны;

2. Зона с радиусом R_2 , в пределах которой уровень сигнала, излучаемого ОТСС, превышает норматив. $R_2 > R_1$, так как в качестве средства перехвата используется специаль-

ный приёмник с существенно более высокими характеристиками, чем ВТСС.

Информация, содержащаяся в информационных параметрах радиосигналов, защищена вне пределов контролируемой зоны, если $R_{з2} < D_{кз}$, а $R_{з1}$ меньше расстояния между ОТСС и ВТСС, где $D_{кз}$ – расстояние от ОТСС до границы контролируемой зоны [21].

Выявление опасных сигналов из общей совокупности сигналов и измерение их уровня проводится при специально организованных тестовых режимах технических средств, при которых длительность и амплитуда информационных импульсов остаются теми же, что и в рабочем режиме, но используется периодическая импульсная последовательность. Данное требование связано с тем, что в принятых методиках расчёта результатов специальных исследований значения полосы суммирования частотных составляющих и тактовая частота информационных импульсов должны быть константами.

В данной статье рассматриваются формальные модели, которые будут повышать точность расчётов при определении защищенности ОВТ обеспечивая защиту информации от утечки по техническим каналам утечки информации (далее – ТКУИ) за счёт каналов ПЭМИ.

Из существующих предпосылок к возникновению утечки информации путём ПЭМИ следует рассматривать модель в больших масштабах с расширенным пространством вокруг СВТ за счёт модификации существующих моделей с переходом в область сферического трёхмерного пространства. В связи с этим необходимость создания модели, построенной на сферической поверхности с учётом слепых зон и равномерным распределением точек по данной поверхности сильно возрастает.

Математическая постановка задачи в двухмерной системе отсчёта

Для описания процесса распределения точек в двухмерном пространстве за единицу измерения взят единичный квадрат, подходящий под размеры помещения в здании.

Для получения равномерного распределения точек по секторам используем метод используемый при построении кубатурных формул:

Узлы – точки пересечения линии широты и долготы, разобьём на три группы по четыре узла в каждой группе. Первую группу узлов образуют точки пересечения окружности с центром в начале. Первую группу узлов образуют точки пересечения окружности с центром в начале координат и радиусом $\alpha > 0$ с осями координат. Вторую группу узлов составляют точки пересечения окружности тем же центром и радиусом $b\sqrt{2} > 0$ с диагоналями квадрата. Третья группа узлов образуется, как вторая, при этом радиус окружности берется равным $c\sqrt{2} > 0$. Коэффициенты для узлов одной и той же группы считаем одинаковыми и равными соответственно A, B и C для узлов первой, второй и третьей групп. Выбор узлов каждой группы согласован с симметрией квадрата. При совмещениях квадрата с самим собой точки любой группы переходят в точки той же группы (рис. 1). [1].

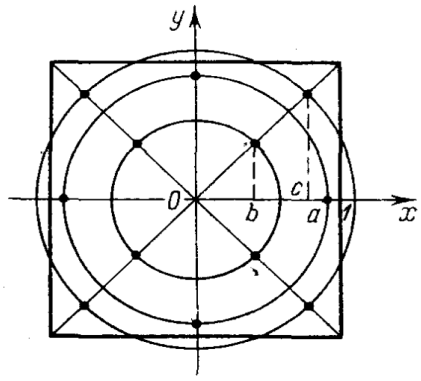


Рис. 1. Элемент равномерного разбиения 12-ти точек [1]

Область системы: прямоугольник $[x_0, x_1] \times [y_0, y_1]$

Элемент-разбиения: квадрат $[-1,1] \times [-1,1]$

Переход на мастер-элемент: $\xi(x,y) = 2\frac{x-x_0}{x_1-x_0} - 1$

$\eta(x,y) = 2\frac{y-y_0}{y_1-y_0} - 1;$

Переход с мастер-элемента:

$$x(\xi,\eta) = \frac{(x_1 - x_0)(\xi + 1)}{2} + x_0$$

$$y(\xi,\eta) = \frac{(y_1 - y_0)(\eta + 1)}{2} + y_0$$ [12].

Исходя из рис. 2 видно, что модель построения точек разбита на 4 сектора. Распространение сигнала ПЭМИ от ОВТ расположенного в центре происходит на 360 градусов. При делении полной окружности (на количество равномерно построенных точек по формуле Гаусса получим:

$$\frac{360}{12} = 30$$

Данное значение показывает оптимальный угол в для измерения секторов направлений ПЭМИ.

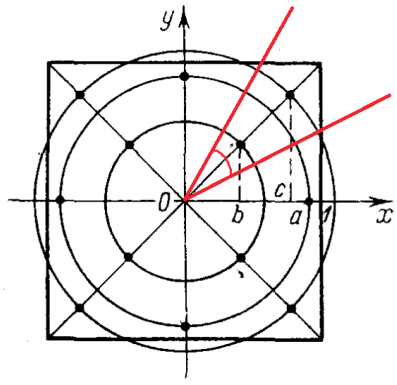


Рис. 2. Элемент с указанием угла в $\alpha = 30^0$

При данном разбиении окружности в области которой распространяется сигнал в каждом секторе 30^0 для повышения эффективности защиты необходимо ввести такие обозначения как открытый и закрытый участок траектории. Данный аспект будет учитывать использование окон, дверей и других открытых участков, за пределы которых распространение значения ПЭМИ будет выше и может выйти за пределы КЗ. Экспериментально установлено, что для повышения уровня защищенности необходимо в секторе с расположением 2 контрольных точек одну из них вывести за пределы КЗ, другую же разместить на границе КЗ. Такое распределение обеспечит высокую степень защиты по всему периметру КЗ, а точка за пределами КЗ будет показателем того распространяется ли сигнал от ОВТ за допустимые границы или нет.

На данном этапе была рассмотрена двухмерная формальная модель построения защиты информации на ОВТ от СТР. При анализе и оценки эффективности защиты, а также при нарастающем числе угроз снятия информации, сканировании местности и других способах получения закрытых данных с использованием БПЛА, была разработана методика подсчёта сферических координат КЗ. При изучении и выявлении упущений первой методики в лабораторных и специальных исследованиях были выведены не все области распространения сигнала ЭМИ. Так при 2-ух мерной модели области контроля распространения сигнала были выявлены слепые (неконтролируемые) зоны, что влечёт за собой утечку информации. Исходя из этого создаётся технический канал утечки информации на объектах без активных средств защиты, при этом возникает возможность применения БПЛА с доставкой измерительной аппаратуры (антенн) на крыши сооружения (здания). Расчёт защищенности ОВТ проводится в горизонтальной плоскости (на расстоянии КЗ – нормы выполняются), но в верхней области распространения возможно нахождение СТР и каналы утечки информации, которые в методике не учитываются. Первичная методика свидетельствует о том, что, хотя и существует устоявшийся способ проведения подсчёта контрольных точек, но вместе с тем имеются существенные особенности, которые должны быть учтены и разработаны в новой методике, которая будет учитывать 3-ех мерное распространение сигнала ЭМИ и обеспечивать более надежный уровень защищенности технических каналов утечки информации.

Математическая постановка задачи в трехмерной системе отсчёта

Используя метод оценки защищённости (эффективности защиты) от СТР была разработана методика двухмерного подсчёта контрольных точек на плоскости области контроля распространения сигнала с последующим переходом на трехмерную (сферическую) модель для повышения уровня защиты ОВТ. При построении математического аппарата воспользуемся сеткой Фибоначчи (для трехмерных систем координат) и методом неопределённых параметров (для двухмерных систем координат), с последующим описанием взаимосвязи между данными моделями.

Основным опасным участком направления ПЭМИ в нашей задаче являются верхние границы сферической поверхности. Для упрощения задачи подсчёта контрольных точек за основу возьмем геометрическую фигуру – икосаэдр (геодезический купол), являющаяся ровным делением полной сферы.

Для разбиения сферы был использован вписанный в сферу икосаэдр, который был разбит на 105 (граней) равносторонних треугольников с 61 контрольной точкой (вершиной). Этот процесс разбиения можно продолжать до достижения требуемой точности. На рис. 3 показано разбиение поверхности сферы с помощью вписанного в сферу икосаэдра.

Была построена модель разбиения сферы в соответствии с рассмотренной методикой.

Рассмотрев икосаэдр (геодезический купол) внимательно, становится заметно, что структура построения геодезической сетки не является хаотичной, а представляет собой

строгую математическую модель. Эта модель берет свое начало из геометрии Платоновых тел.

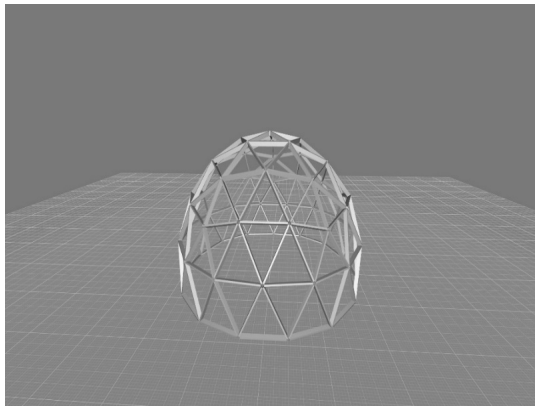


Рис. 3. Икосаэдр

Частота триангуляции

Для расчета геокупола требуется понимать, что такое «частота триангуляции». Это понятие подразумевает плотность разбивки купола на треугольники. Т.е. один и тот же купол можно «описать» разным количеством треугольников. Например, для менее плотной разбивки потребуется меньше треугольников, но с большей длиной ребра и форма будет более угловатой. Для более плотной разбивки потребуется большее количество треугольников с меньшей длиной ребра, но форма получится боле ровной и близкой к сферической. Для определения частоты деления для множества треугольников введём обозначение частоты латинской буквой «V». Число значения частоты равняется количеству «рядов».

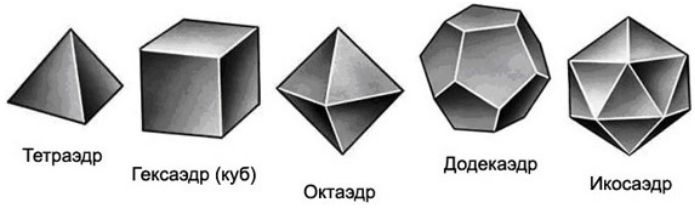


Рис. 4. Платоновы тела

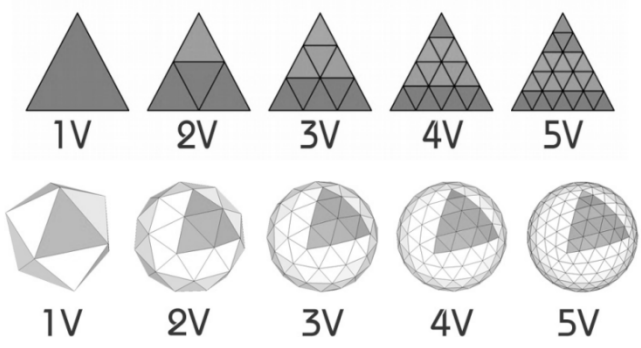


Рис. 5. Разбиение купола на треугольники

Сечение сферы

Следующий параметр, который следует знать при расчете геодезического купола – это значение сечения сферы. Если рассматривать сферу как целое, можно поделить её на различное количество частей. Удобнее всего купол разбить по «рядам». У куполов с разной частотой триангуляции «V» – разное количество «рядов», поэтому сечение для них всегда индивидуальное.

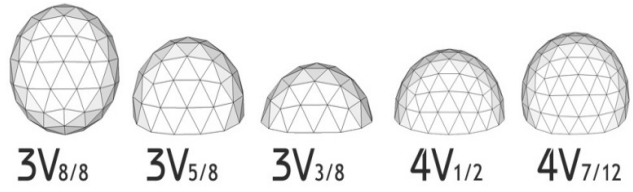


Рис. 6. Сечение сферы

Равномерное распределение точек на поверхности сферы имеет значение для большого числа математических задач.

Особый интерес к равномерному распределению точек на поверхности сферы может быть объяснен, с одной стороны, геометрическими свойствами поверхности – свойствами центральной симметрии, с другой стороны, тем, что при моделировании многих объектов в окружающем нас мире удобно использовать именно сферическую (купольную) конструкцию как геометрический объект.

В зависимости от числа точек, которые необходимо распределить на поверхности сферы, и от дополнительных ограничений и условий, могут быть рассмотрены различные подходы к решению данной частной задачи:

1. Создание генератора случайных точек, сферические координаты которых удовлетворяют заданным условиям и ограничениям. Этот подход может оказаться наиболее адекватным в случаях с достаточно большим количеством точек.

2. Использование правильных многогранников (тел Платона) и дальнейшая аппроксимация сферы на их основе. Однако необходимо сказать, что тел Платона для трехмерного пространства только пять: тетраэдр, октаэдр, гексаэдр, додекаэдр, икосаэдр;

3. Использование метода золотого сечения сетки Фибоначчи наложения на поверхность сферы равномерное распределение точек.

4. Путём трехмерного моделирования используя платформы 3D моделей.

Представим две различные модели, построенные за счёт различных методик математического описания и с использованием наложения равномерности распределения точек на поверхность сферы:

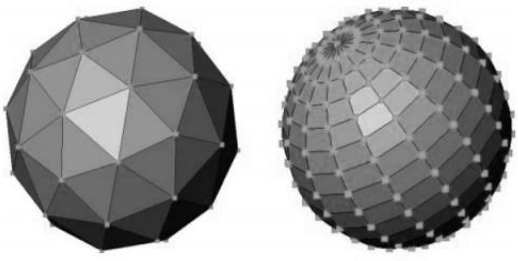


Рис. 7. Представление сферы

Заполнение буфера вершин

Так при использовании совокупности методов возможности более оптимального распределения показал вариант сетки Фибоначчи, который использует систему треугольников. Это объясняется тем, что треугольник — простейший и, следовательно, наиболее фундаментальный элемент поверхности. Каждый треугольник определяется всего лишь тремя точками — вершинами в углах треугольника.

Дуги и другие изогнутые поверхности намного сложнее. Треугольники являются фундаментальными элементами поверхности по той причине, что любую фигуру с прямыми гранями (квадрат, прямоугольник, многоугольник и др.) можно расчленить на набор треугольников. Так же данная абстракция используется в программном обеспечении любого современного графического оборудования при задачах распределения точек на сферических поверхностях.

Вершина — это объект данных, представляющий точку в трехмерном пространстве. Большинство систем трехмерной графики функционируют путем конструирования сложных поверхностей и объектов на основе многих тысяч крошечных треугольников. Каждый треугольник определен тремя точками, причем каждая точка является вершиной треугольника [3].

Так же необходимо отметить, что при классическом построении за счёт прямоугольников использование узлов координатной сетки на сфере – то есть точек пересечения линий широт и долгот не дает равномерного распределения точек на сфере. Визуальный анализ (Рис. 7) показывает, что узлы пересечения широт и долгот сгущаются при приближении к полюсам. [3], [4], [11]

Преимущество метода Фибоначчи по распределению точек на поверхности сферы в сравнении с другими методами заключается в том, что при использовании аппаратуры проверки состояния ЭМИ область распространения сигнала на сфере представляет круг, для оптимального захвата сигнала требуется идентичная геометрическая фигура, которая будет гарантировать отсутствие слепых зон на сферической поверхности. Такой фигурой является шестигранник, который в свою очередь состоит из шести равнозначных треугольников, построенных в сфере таким образом, чтобы минимизировать расстояние между всеми контрольными точками.

В литературе встречается два схожих определения множества точек сферической сетки Фибоначчи. Исходное определено строго для N, равного одному из членов ряда Фибоначчи, и хорошо изучено в теории чисел.

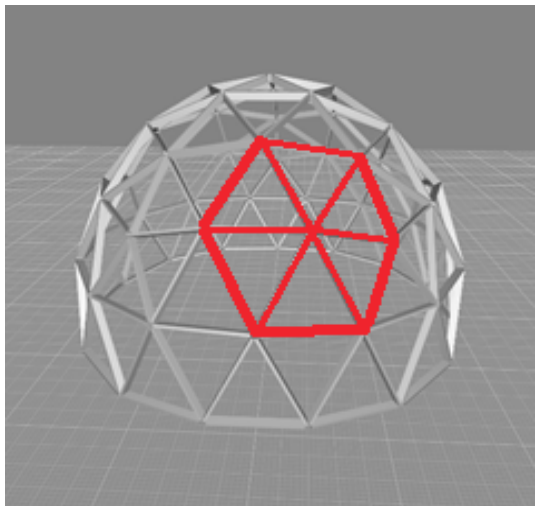


Рис. 8. Выборка необходимого элемента

$$t_i = \left(\frac{i}{F_m}, \frac{i\,F_m - 1}{F_m}\right) \quad \text{при } 0 \le i \le N - 1$$

Второе определение обобщает формулу до произвольного количества N и используется в вычислениях чаще:

$$t_i = \left(\frac{i}{N}, \frac{i}{\varphi}\right) \quad \text{при } 0 \le i \le N$$

где

$$\phi = \frac{\sum 1\sqrt{5}}{2} = \lim_{n\to\infty}\left(\frac{F_{n+1}}{F_n}\right)$$ [12].

Требуется создать регулярное покрытие сферы треугольниками, близкими по размеру и форме. В качестве эталона примем сетку Фибоначчи. Вначале рассмотрим алгоритм построения сетки в базовом сферическом треугольнике. Затем уделим внимание различным способам разделения сферы на базовые сферические треугольники. Наконец, представим пример создания треугольной сетки на основе икосаэдра.

По приведенным значениям определяется средняя точка, которая разделяет треугольник точного решения на четыре треугольника. На следующем этапе находятся координаты еще трех точек, которые хотя и не являются точным разбиением сферы, однако достаточно близки к нему. При дальнейшем продолжении разбиения равномерность существенно ухудшается, хотя если продолжать рекурсивную процедуру только с новым поколением точек, она остается, сравнимая с другими алгоритмами.

Генерация сетки в сферическом треугольнике

Процедуру создания на некоторой поверхности сетки треугольников обычно называют триангуляцией. В качестве базы для создания сетки используем некоторый сферический треугольник, заданный координатами своих вершин.

Метод бисекции

Назовём бисекцией операцию деления исходного треугольника на четыре треугольника нового поколения (рис.9). Собственно, термин «бисекция» относится к делению сторон пополам.

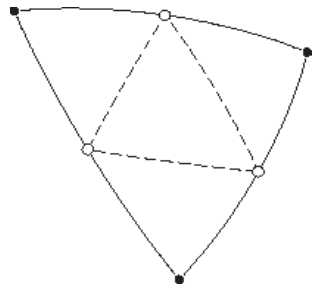


Рис. 9. Бисекция сферического треугольника

В середины рёбер вставляются новые вершины (белые точки на рисунках), которые соединяются новыми рёбрами (пунктирные линии), образующими новые треугольники. Следующее поколение получается очередной бисекцией.

Метод трисекции

Можно сразу провести разделение сферического треугольника на 9 треугольников, применяя трисекцию (рис. 10).[2].

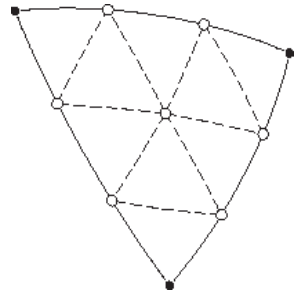


Рис. 10. Трисекция сферического треугольника

В терминах геометрии на сфере задача вставки точек в стороны треугольников решается последовательным решением обратной и прямой геодезических задач. Однако в данном случае гораздо проще использовать векторную алгебру. Пусть концы стороны заданы векторами a и b; тогда средняя точка f вычисляется как их нормированная сумма:

$$f = \frac{a + b}{|a + b|}$$

Для получения значений координат точек следует использовать соотношения:

– *Преобразования сферических координат в декартовы:*

$$x = \cos\varphi \cos\lambda$$
$$y = \cos\varphi \sin\lambda$$
$$z = \sin\varphi$$

– *Преобразования декартовых координат в сферические:*

$$\lambda = arctg\frac{y}{x}$$
$$\varphi = arctg\frac{z}{\sqrt{x^2 + y^2}}$$ [2], [9].

Рассматривая исходные данные которые имеются в модели двухмерного пространства и применяя к ним математический аппарат теории Фибоначчи построим взаимосвязь с описанием перехода от двухмерной системы координат в трехмерную. Исходный единичный квадрат дает возможность произвести переход решения задачи в другую плоскость для дальнейшего построения более сложной модели. Для этого используем цилиндрическую равновеликую проекцию:

$$(x, y) \rightarrow (\theta, \phi): (cos^{-1}(2x - 1)\pi/2, 2\pi y)$$

$$(\theta, \phi) \rightarrow (x, y, z): (cos\theta cos\phi, cos\theta sin\phi, sin\theta)$$

[12].

Перенос из единичного квадрата на поверхность сферы выполняется проекцией с сохранением площади.

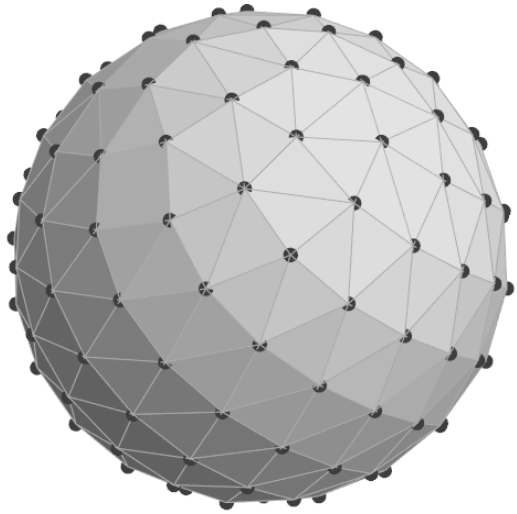


Рис. 11. Представление сетки Фибоначчи наложенной на сферу [4], [5], [6], [12]

Расположение точек в интервалах (по правилу средней точки в квадратурной формуле Гаусса)

Сферические множества Фибоначчи глобально не являются наилучшим распределением сэмплов на сфере (потому что их решения не совпадают с решениями для платоновых тел при (n=4,6,8,12,20), однако они обладают превосходными свойствами семплирования и очень легки в построении по сравнению с другими, более сложными схемами сферического семплирования.

Вывод

Проведя анализ уровня защищенности ОВТ на территории КЗ были выявлены технические каналы утечки информации в верхней области распространения сигнала ПЭМИ. По данной проблеме были проведены специальные исследования, по результату которых разработаны формальные модели в двухмерной и трехмерной системе отчёта. Данные модели имеют общий математический аппарат теории Фибоначчи, позволяющий простроить оптимальное распространение точек в геометрической области решения задачи, а также доказать безопасность системы, опираясь на объективные доказуемые математические постулаты. Так, большее распределение контрольных точек даёт большую эффективность защиты ОВТ от СТР, и тем самым выше вероятность обнаружения возможной утечки по каналу ПЭМИ.

Литература

1. Мысовских И.П. Интерполяционные кубатурные формулы // Главная редакция физико-математической литературы издательства «Наука», 1981. – 336 с.

2. Милосердов Е.П. Разбиение сферы на равномерные участки // Журнал естественнонаучных исследований Том 5, № 4, 2021 – 59 с.

3. https://professorweb.ru/my/Silverlight/base/level6/6_1.php Основы трёхмерного моделирования.

4. Johann S. Brauchart a, b, 1, 2, Peter J. Grabner b,3 Distributing many points on spheres: minimal energy and designs.

5. D.P. Hardin, T. Michaels and E.B. Saff Comparison of Popular Point Configurationson .

6. Копытов Н.П. Равномерное распределение точек на поверхностях и его применение в исследованиях структурнонеоднородных сред. Диссертация на соискание ученой степени кандидата физико-математических наук.

7. Paul Leopardi. Distributing points on the sphere: Partitions, separation, quadrature and energy. The University of New South Wales School of Mathematics and Statistics Department of Applied Mathematics.

8. E.B. Saff and A.B.J Kuijlaars Distributing Many Points on a Sphere.

9. А.В. Скворцов Триангуляция Делоне и её применение. – Томск: Изд-во Том. ун-та, 2002. – 128 с.

10. Василенко С.Л. Золотые купола в задаче конусной упаковки евклидового пространства.

11. Степанов Н.Н. Сферическая тригонометрия. Государственное издательство технико-теоретической литературы. – Ленинград, 1948 г., Москва.

12. https://habr.com/ru/post/460643/ Равномерное распределение точек на сфере.

13. Баранова, Е.К. Информационная безопасность и защита информации: учебное пособие / Е.К. Баранова, А.В. Бабаш. – М.: Риор, 2018. – 400 с.

14. Мельников, В.П. Защита информации: Учебник / В.П. Мельников. – М.: Академия, 2019. – 320 с.

15. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. – М.: ГЛТ, 2016. – 280 с.

16. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. – М.: Гелиос АРВ, 2017. – 336 с.

17. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. – М.: ДМК, 2017. – 702 с.

18. Хорев, П.Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. – М.: Форум, 2018. – 352 с.

19. Ярочкин, В.И. Информационная безопасность: учебник для вузов / В.И. Ярочкин. – М.: Акад. Проект, 2018. – 544 с.

20. Марков С.В., Барагузина В.В., Бердников С.М., Степанцов С.В., Способ выявления и обнаружения несущей частоты информативного сигнала при сканировании объектов разной яркости и контрастности // Труды XXIV Всероссийской научно-практической конференции РАРАН. В 7-ми томах.01-04 апреля 2021, Санкт-Петербург, 2021, Том 4, С. 347–352.

21. Д.В. Кислицын, Разработка измерительного комплекса для оценки защищённости технических средств от утечки информации по каналу побочных электромагнитных излучений и наводок. Пермский государственный национальный исследовательский университет, 614990, Пермь, Букирева, 15.

References

1. Mysovskikh I.P. Interpolyatsionnyye kubaturnyye formuly // Glavnaya redaktsiya fiziko-matematicheskoy literatury izdatel'stva "Nauka", 1981. – 336 c.

2. Miloserdov Ye.P. Razbiyeniye sfery na ravnomernyye uchastki // Zhurnal yestestvennonauchnykh issledovaniy Tom 5, № 4, 2021 – 59 s.

3. https://professorweb.ru/my/Silverlight/base/level6/6_1.php Osnovy trokhmernogo modelirovaniya.

4. Johann S. Brauchart a, b, 1, 2, Peter J. Grabner b,3 Distributing many points on spheres: minimal energy and designs.

5. D.P. Hardin, T. Michaels and E.B. Saff Comparison of Popular Point Configurationson .

6. Kopytov N.P. Ravnomernoye raspredeleniye tochek na poverkhnostyakh i yego primeneniye v issledovaniyakh strukturnoneodnorodnykh sred. Dissertatsiya na soiskaniye uchenoy stepeni kandidata fiziko-matematicheskikh nauk.

7. Paul Leopardi. Distributing points on the sphere: Partitions, separation, quadrature and energy. The University of New South Wales School of Mathematics and Statistics Department of Applied Mathematics.

8. E.B. Saff and A.B.J Kuijlaars Distributing Many Points on a Sphere.

9. A.V. Skvortsov Triangulyatsiya Delone i yeyo primeneniye. – Tomsk: Izd-vo Tom. un-ta, 2002. – 128 c.

10. Vasilenko S.L. Zolotyye kupola v zadache konusnoy upakovki yevklidovogo prostranstva.

11. Stepanov N.N. Sfericheskaya trigonometriya. Gosudarstvennoye izdatel'stvo tekhniko-teoreticheskoy literatury. – Leningrad, 1948g., Moskva.

12. https://habr.com/ru/post/460643/ Ravnomernoye raspredeleniye tochek na sfere.

13. Baranova, Ye.K. Informatsionnaya bezopasnost' i zashchita informatsii: Uchebnoye posobiye / Ye.K. Baranova, A.V. Babash. – M.: Rior, 2018. – 400 c. 14. Mel'nikov, V.P. Zashchita informatsii: Uchebnik / V.P. Mel'nikov. – M.: Akademiya, 2019. – 320 c.

15. Malyuk, A.A. Informatsionnaya bezopasnost': kontseptual'nyye i metodologicheskiye osnovy zashchity informatsii / A.A. Malyuk. – M.: GLT, 2016. – 280 c.

16. Chipiga, A.F. Informatsionnaya bezopasnost' avtomatizirovannykh sistem / A.F. Chipiga. – M.: Gelios ARV, 2017. – 336 c.

17. Shan'gin, V.F. Informatsionnaya bezopasnost' i zashchita informatsii / V.F. Shan'gin. – M.: DMK, 2017. – 702 c.

18. Khorev, P.B. Programmno-apparatnaya zashchita informatsii: Uchebnoye posobiye / P.B. Khorev. – M.: Forum, 2018. – 352 c.

19. Yarochkin, V.I. Informatsionnaya bezopasnost': Uchebnik dlya vuzov / V.I. Yarochkin. – M.: Akad. Proyekt, 2018. – 544 c.

20. Markov S.V., Baraguzina V.V., Berdnikov S.M., Stepantsov S.V., sposob vyyavleniya i obnaruzheniya nesushchey chastoty informativnogo signala pri skanirovanii ob"yektov raznoy yarkosti i kontrastnosti // Trudy XXIV Vserossiyskoy nauchno-prakticheskoy konferentsii RARAN. V 7-mi tomakh.01-04 aprelya 2021, Sankt-Peterburg, 2021, Tom 4, S. 347–352.

21. D.V. Kislitsyn, Razrabotka izmeritel'nogo kompleksa dlya otsenki zashchishchonnosti tekhnicheskikh sredstv ot utechki informatsii po kanalu pobochnykh elektromagnitnykh izlucheniy i navodok. Permskiy gosudarstvennyy natsional'nyy issledovatel'skiy universitet, 614990, Perm', Bukireva, 15.

КОПЫТОВ Павел Дмитриевич, инженер, 4-й государственный центральный межвидовой полигон МО РФ. Россия, 416540, г. Знаменск, ул. Ленина, дом 11. E-mail: zaharov0896@gmail.com

КОРОЛЁВ Игорь Дмитриевич, доктор технических наук, профессор, Краснодарское высшее военное училище имени генерала армии С. М. Штеменко. Россия, 350005 г. Краснодар, ул. Грибоедова, 18, микрорайон 9-й километр. E-mail: pi_korolev@mail.ru

КУЛИШ Ольга Александровна, кандидат физико-математических наук, доцент, Краснодарское высшее военное училище имени генерала армии С. М. Штеменко. Россия, 350005 г. Краснодар, ул. Грибоедова, 18, микрорайон 9-й километр. E-mail: culish_olga@mail.ru

СТЕПАНЦОВ Сергей Валерьевич, преподаватель кафедры МиИ, Астраханский государственный университет им. В.Н. Татищева. Россия, 414056, г. Астрахань, ул. Татищева, 20а. E-mail: stepantsov.sergey@asu.edu.ru

KOPYTOV Pavel Dmitrievich, engineer, 4th State Central Interspecific landfill of the Ministry of Defense of the Russian Federation. 416540, Znamensk, Lenin St., house 11. E-mail: zaharov0896@gmail.com

KOROLEV Igor Dmitrievich, Doctor of Technical Sciences, Professor, Krasnodar Higher Military School named after Army General S. M. Shtemenko. 350005 g. Krasnodar, Griboyedov str., 18, microdistrict 9th kilometer. E-mail: pi_korolev@mail.ru

KULISH Olga Aleksandrovna, Associate Professor Candidate of Physical and Mathematical Sciences, Krasnodar Higher Military School named after General of the Army S. M. Shtemenko. 350005 g. Krasnodar, Griboyedov str., 18, microdistrict 9th kilometer. E-mail: culish_olga@mail.ru

STEPANTSOV Sergey Valeryevich, lecturer of the Department of MI, Astrakhan State University named after V.N. Tatishchev. 414056, Astrakhan, Tatishcheva str., 20a. E-mail: stepantsov.sergey@asu.edu.ru

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

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

ВЕСТНИК УрФО
Безопасность в информационной сфере № 1(47) / 2023
Подписано в печать 17.03.2023. Дата выхода в свет 21.03.2023.
Формат 70×108 1/16. Печать цифровая. Усл.-печ. л. 9,8. Тираж 50 экз.
Заказ 43/105.
Цена свободная.

Отпечатано в типографии Издательского центра ФГАОУ ВО "ЮУрГУ (НИУ)".
454080, г. Челябинск, пр. им. В. И. Ленина, 76, ЮУрГУ, Издательский центр.

Bulletin of the Ural Federal District
Security in the Sphere of Information No. 1(47) / 2023
Signed to print March 17, 2023. Date of publication of the 21.03.2023.
Format 70×108 1/16. Screen printing. Conventional printed sheet 9,8. Circulation – 50 issues.
Order 43/105.
Open price.

Printed in the printing house of the Publishing Center of FGAOU VO "SUSU (NIU)".
SUSU, Publishing Center, 76, Lenina Str., Chelyabinsk, 454080