Труды XXVIII научной конференции по радиофизике

СЕКЦИЯ
«ИНФОРМАЦИОННЫЕ СИСТЕМЫ. СРЕДСТВА, ТЕХНОЛОГИИ, БЕЗОПАСНОСТЬ»

Председатель – Л.Ю. Ротков, секретарь – А.А. Рябов.
Нижегородский государственный университет им. Н.И. Лобачевского.

СИСТЕМА ТЕСТОВ ДЛЯ ПРОВЕРКИ РЕАЛИЗАЦИИ ИЗОЛИРОВАННОЙ ПРОГРАММНОЙ СРЕДЫ

И.С. Болдырев[1)], А.А. Рябов[2)]

[1)] ООО «ТИС-Центр»
[2)] ННГУ им. Н.И. Лобачевского

Изолированная программная среда (ИПС) препятствует распространению вирусов и вредоносного программного обеспечения (ПО), блокирует выполнение несанкционированного программного обеспечения со стороны пользователей [1]. Настройка ИПС представляет собой процесс определения перечня исполняемых файлов, запуск которых разрешен для пользователя.

Важным этапом в разработке ПО является тестирование. Тестирование позволяет определить программы заданному функционалу и отсутствие конфликтов с другим программным обеспечением.

Разработка системы тестов для ИПС представляет собой актуальную задачу и является важным элементом информационной безопасности. Небольшое количество опубликованной информации о методах и процедурах тестирования механизма ИПС указывает на необходимость глубокого исследования в данной области.

Исследования проводились с использованием операционной системы Astra Linux, релиз «Смоленск».

Тестирование реализовано с использованием стратегии «черный ящик» с учетом ГОСТов [2-4].

Использовалась модель тестируемого объекта с разделением входных и выходных данных тестируемого объекта на разделы эквивалентности [5].

Модель синтаксиса представлена в виде ряда правил, где каждое правило определяет формат входного параметра в терминах «последовательностей», «итераций» или «выбора между» элементами синтаксиса [6].

Для реализации метода разделение на эквивалентные разделы и метода синтаксического тестирования разработан bash-скрипт, содержащий команды для выполнения следующих задач:

- создание ключа электронной подписи (ЭП);
- включение/выключение режима ИПС;
- подписание файлов произвольного типа с записью информации об ЭП в дополнительные атрибуты файла;
- выполнение тестов.

Разработанная система тестов включает в себя два теста. Протокол выполнения тестов отображается в журнале проведения испытаний.

Первый тест предназначен для проверки наличия информации об ЭП в дополнительных атрибутах файлов.

Второй тест предназначен для проверки корректности работы механизма ИПС в отладочном режиме. При этом производится проверка разрешения чтения содержимого подписанных файлов, а также проверка запрета чтения содержимого неподписанных файлов.

По окончании тестов производится контроль журнала проведения испытаний.

В разработанной системе тестов применяются методы эквивалентного разделения и синтаксического тестирования.

[1] Прокушев, Я.Е. Программно-аппаратные средства защиты информации: лабораторный практикум / Я.Е. Прокушев. – Санкт Петербург, 2017. 168 с.
[2] ГОСТ Р 56920-2016/ISO/IEC/IEEE 29119-1:2013 Системная и программная инженерия. Тестирование программного обеспечения. Часть 1. Понятия и определения – Москва: Стандартинформ, 2016. 54 с.
[3] ГОСТР56921-2016/ISO/IEC/IEEE29119-2:2013 Системная и программная инженерия. Тестирование программного обеспечения. Часть 2. Процессы тестированияопределения – Москва: Стандартинформ, 2016. 65 с.
[4] ГОСТР56922—2016/ISO/IEC/IEEE29119-3:2013 Системная и программная инженерия. Тестирование программного обеспечения. Часть 3. Документация тестирования – Москва: Стандартинформ, 2016. 114 с.
[5] Глоссарий терминов, используемых при тестировании программного обеспечения BS 7925-2, 1998.
[6] Международный стандарт ISO_IEC_IEEE 29119-4-2015 Разработка программного обеспечения и систем Тестирование программного обеспечения Часть 4: Методы тестирования. 2015. 150 с.

СРАВНЕНИЕ СЛОЖНОСТИ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАТЕЛЕЙ

А.А. Горбунов, Е.А. Макушев

ННГУ им. Н.И. Лобачевского

Одним из методов идентификации динамических систем является подход, основывающийся на определении базовых параметров входных и выходных сигналов данных систем [1]. Указанный подход может быть применен в частности при решении задач, связанных с получением сравнительных оценок сложности криптографических преобразователей (таких как шифраторы, дешифраторы) в криптосистемах (КС). При этом построение динамических математических моделей КС осуществляется путем структурной идентификации, опираясь только на имеющиеся в наличии открытые тексты, шифротексты и их практически измеряемые параметры [2].

Набор базовых параметров (БП), определяемых по текстовым последовательностям криптографических преобразователей, состоит из:

$$\text{БП} = \{q, n\}.$$

Базовый параметр q для текстовых последовательностей может быть интерпретирован как размерность их алфавита. Границы области поиска базового параметра q задаются, исходя из априорных сведений о модели идентифицируемой объекта. Величина базового параметра $n = n(q)$ должна обеспечивать нахождение такого минимального значения n, при котором идентифицируемый источник текста являлся бы непротиворечивым прогнозирующим оператором рассматриваемого порядка n его текстовой q-уровневой последовательности.

В настоящей работе осуществлялось экспериментальное определение базовых параметров шифротекстов, полученных при работе в различных режимах шифрования, таких КС как DES, AES, ChaCha20-Poly1305 [3]. Также было проведено сравнение сложностей источников данных текстов при различных значениях q размерности их алфавита. Количество символов M в исследуемых текстах соответствовало числу байт в файлах размером 1 Мбайт, полученных после работы указанных шифраторов. Значение каждого байта в зашифрованном файле рассматривалось как код отдельного символа шифротекста и подвергалось процедуре переквантования с целью получения величин размерности алфавита q = 16, 32, 64, 128, 256.

Полученные экспериментально значения базового параметра n для шифротекстов исследуемых криптографических преобразователей для различных значений базового параметра q представлены на следующих графиках. На рис. 1 отображено сравнение величин n для текстов, полученных после шифрования блочным шифром DES в различных режимах работы и после применения поточного шифра из семейства ChaCha20.

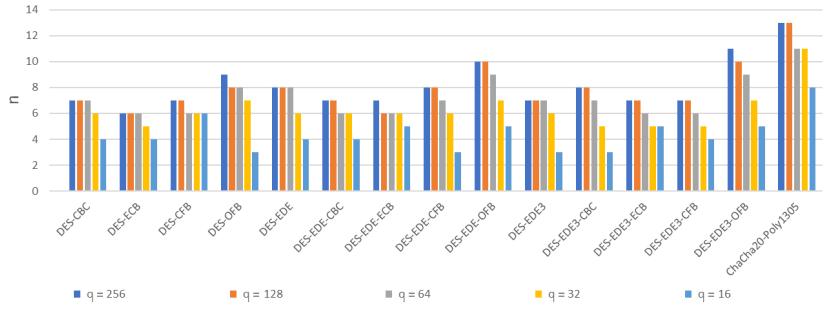

Рис. 1

Аналогично на рис. 2 отображено сравнение величин *n* для текстов, полученных после шифрования блочным шифром AES в различных режимах работы и после применения поточного шифра из семейства ChaCha20.

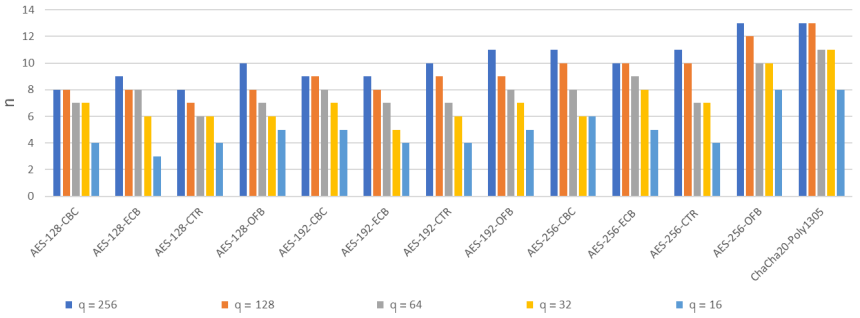

Рис. 2

Представленные результаты демонстрирует, что идентификация различий между шифрующими преобразователями на основе определения базовых параметров их текстовых последовательностей остается возможной при больших размерностях алфавита (например, при значениях $q = 128, 256$) и становится неудовлетворительной при сильном загрублении анализируемых данных (например, при значениях $q = 16, 32$).

[1] Кирьянов К.Г. Выбор оптимальных базовых параметров источников экспериментальных данных при их идентификации. // Труды III Международной конференции "Идентификация систем и задачи управления SICPRO'04". – М.: ИПУ РАН, 2004. С. 187.

[2] Горбунов А.А. Сравнение алгоритмов структурной идентификации источников данных на основе определения их базовых параметров. // Труды XIII научной

конференции по радиофизике. /Ред. С.М. Грач, А.В.Якимов. – Н. Новгород: Изд-во «ТАЛАМ», 2009, с. 225.
[3] Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на С. – М.: Диалектика, 2022.

ИСПОЛЬЗОВАНИЕ МЕТОДА СПЕКТРАЛЬНОГО АНАЛИЗА ДЛЯ ОБНАРУЖЕНИЯ СОСТЯЗАТЕЛЬНЫХ АТАК

М.В. Капралова, С.П. Никитенкова

ННГУ им. Н.И. Лобачевского

Состязательное машинное обучение — это область, изучающая класс атак на нейронные сети, целью которых является ухудшение точности классификаторов, получение ошибочного прогноза с высокой степенью достоверности.

В работе исследовалась возможность применения спектрального анализа как инструмента обнаружения состязательной атаки. Гипотеза заключается в существовании различий между спектрами исходного и соответствующего ему атакованного изображений. Для создания состязательного примера использовался Fast Gradient Sign Method (FGSM) [1]. Идея метода состоит в том, чтобы добавить небольшое количество шума на основе градиента функции потерь по отношению к входным данным. Эффективности FGSM заключается в его простоте.

Для проверки гипотезы использовалась предварительно обученная на наборе данных Microsoft Asirra [2] сверточная нейронная сеть (CNN). На вход обученной нейронной сети подавались произвольные изображения кошек и собак. Животные на изображениях были распознаны корректно с точностью выше 90% несмотря на то, что на некоторых изображениях животные имели схожий с фоном окрас.

Выполнялась итеративная генерация вредоносного возмущения FGSM-методом. Уже после первой итерации изображение с кошкой, имеющей схожий с фоном окрас, стало классифицироваться, как изображение с собакой с вероятностью 91,4%. Потребовалось две итерации для того, чтобы аналогичным образом стала ошибочно воспринимать изображение с собакой как изображение с кошкой с вероятностью 95,2%. При дальнейшем увеличении количества итераций уверенность нейросети в правильности ошибочного решения увеличилась и достигла 100%.

Изображение обычно трактуется как двумерный сигнал, заданный на плоскости. Спектральные свойства изображения можно проанализировать с помощью дискретного преобразования Фурье. Для дискретного двумерного сигнала $f(x, y)$, представляющего отдельные цветовые каналы изображения размера $M \times N$, дискретное преобразование Фурье $F(kx,ky)$ определяется как:

$$F(k_x, k_y) = \frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) exp\left(-i2\pi\left(\frac{k_x x}{M} + \frac{k_y y}{N}\right)\right),$$

где x, y – позиция пикселя, $f(x,y)$ – значение пикселя выбранного канала изображения, kx,ky – пространственная частота.

Значение F(kx,ky) комплексное. Используя формулу Эйлера F(kx,ky) можно представить как

$$F(k_x, k_y) = |F(k_x, k_x)| exp\left(i\varphi(k_x, k_y)\right),$$

где $|F(kx,ky)|$ – амплитуда, $\varphi\varphi(kx,ky)$ – фаза.

Спектр изображения показывает, насколько быстро/медленно изменяется контраст/цвет/значения пикселей в пространственных измерениях. В фурье-представлении

изображений спектральная амплитуда и фаза играют разные роли. Амплитуда представляет собой интенсивность различных частот в изображении. Фаза отвечает за выделение границ объектов на изображении [3, 4].

Было обнаружено, что состязательная атака на изображение сильнее всего изменила амплитуды низких и средних частот фурье-спектра изображения. Фазовый спектр изображения после атаки имел меньше всего изменений в области низких частот.

Спектр мощности изображения является важной характеристикой изображения и определяется как

$$P(k_x, k_y) = |F(k_x, k_x)|^2 .$$

После применения преобразования Фурье к изображению информация представлена в новой области, но по-прежнему содержит 2D-информацию. Размерность может быть уменьшена без существенной потери информации путем азимутального усреднения:

$$P(r) = \frac{1}{2\pi}\int_0^{2\pi} P(r,\theta)d\theta, \text{ где } r = \sqrt{\frac{4\left({k_x}^2+{k_y}^2\right)}{M^2+N^2}} \text{ и } \theta = atan2\left(k_x, k_y\right).$$

Азимутальное усреднение можно рассматривать как сжатие и усреднение схожих частотных компонент.

На рисунке показан график разности значений азимутально-усредненного спектра мощности исходного и соответствующего ему атакованного изображений. Из графика видно, что с увеличением пространственной частоты разность значений спектра мощности начинает расти.

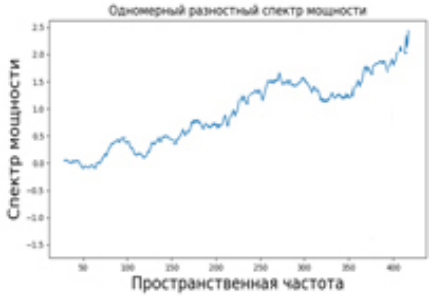

Рис.

Существенное различие в спектрах исходного и атакованного изображений доказывают справедливость выдвинутой гипотезы. Полученные результаты могут быть использованы для создания эффективных систем обнаружения состязательных атак.

[1] Goodfellow I.J., Shlens J., Szegedy C. // Explaining and harnessing adversarial examples. arXiv preprint arXiv:1412.6572. 2014.
[2] https://www.kaggle.com/c/dogs-vs-cats

[3] Juvells I. et al. The role of amplitude and phase of the Fourier transform in the digital image processing // Am. J. Phys. 1991. Vol. 59, No. 8. P. 8.
[4] Alieva T., Calvo M.L. Image reconstruction from amplitude-only and phase-only data in the fractional Fourier domain // Optics and Spectroscopy. 2003. Vol. 95. P. 110.

РАЗРАБОТКА ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ИДЕНТИФИКАЦИИ НЕМАРКИРОВАННЫХ ЭЛЕМЕНТОВ ПИТАНИЯ

А.А. Коротышева[1)], С.Н. Жуков[1)], Ю.С. Егоров[2)], А.Ю. Чекушева[2)]

[1)] ННГУ им. Н.И. Лобачевского
[2)] НГТУ

Одной из задач национального проекта «Экология» [1] является создание автоматизированных сортировочных линий, обладающих более высокой производительностью и безопасностью, чем ручная сортировка, что предопределяет актуальность разработки отечественной программно-аппаратной платформы для автоматической идентификации и сортировки опасных видов отходов, таких как химические источники тока (элементы питания или ЭП), в составе твёрдых коммунальных отходов.

Настоящая работа посвящена описанию разработки интеллектуальной системы идентификации немаркированных элементов питания в рамках такой платформы.

Для идентификации немаркированных элементов питания реализована обработка информации двух видов:

- цветное изображение *I* (от Image);
- рентгеновский снимок *R* (от Radiograph).

В основе этапов обработки изображений *I* и рентгеновских снимков *R* лежат нейронные сети (НС), обученные на подготовленных наборах данных, содержащих изображения и рентгеновские снимки ЭП разных типов.

Обобщенная схема идентификации ЭП представлена на рисунке.

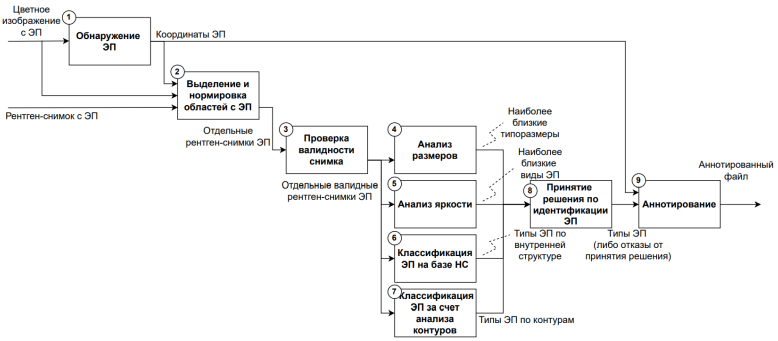

Рис.

В соответствии с разработанной схемой на основе обработки изображений *I* выполняются этапы:

1) Обнаружение ЭП;

На основе обработки изображений *I* совместно с рентгеновскими снимками *R* осуществляется:

2) Выделение и нормировка областей с ЭП;

8) Принятие решения по идентификации ЭП;

9) Аннотирование.

На основе обработки рентгеновских снимков *R* выполняются этапы:

3) Проверка валидности снимка;

4) Анализ размеров;

5) Анализ яркости;

6) Классификация ЭП на базе НС;

7) Классификация ЭП за счет анализа контуров.

Повышение достоверности идентификации ЭП осуществляется за счет применения двух каналов обработки изображений и рентгеновских снимков.

Таким образом, выделены следующие этапы обработки информации:

- Обнаружение ЭП − определение местоположений ЭП на входном изображении с помощью предобученной нейронной сети YOLO [2].
- Выделение и нормировка областей с ЭП − выделение областей по полученным координатам, и их нормировка путем вращения до вертикального положения ЭП. Получение фрагментов с выделенными областями из изображения.
- Проверка валидности снимка − оценка средней яркости фрагмента снимка.
- Анализ размеров − определение типоразмера ЭП [3] за счет оценки соотношения высоты и ширины фрагмента снимка.
- Анализ яркости − оценка средней яркости фрагмента снимка и сравнение с заранее определенными диапазонами яркости каждого типа ЭП.
- Классификация ЭП на базе НС − анализ фрагмента снимка сверточной нейронной сетью MobileNet2 [4].
- Классификация ЭП за счет анализа контуров − поиск границ на фрагменте снимка и выделение среди них прямых линий [5].
- Принятие решения по идентификации ЭП − агрегация полученных результатов идентификации ЭП от алгоритмов классификации и формирование итогового решения.
- Аннотирование − формирование файла с итоговым решением идентификации ЭП.

Если полученная достоверность результата классификации меньше заданного порога, на выходе интеллектуальной системы идентификации для немаркированных ЭП формируется отказ от приятия решения о типе ЭП.

Интеллектуальная система идентификации немаркированных ЭП на основе нейронных сетей является эффективным способом повышения качества линий сортировки ЭП [6]. Кроме того, применение системы возможно для проверки качества производства ЭП.

Описанная интеллектуальная система может быть дополнена другими новыми этапами обработки информации для увеличения количества классифицированных ЭП [7].

Работа выполнена при поддержке Фонда содействия развитию малых форм предприятий в научно-технической сфере (договор № 57ГС1ИИС12-D7/72200 от 21.12.2021).

[1] Национальный проект «Экология» [Электронный ресурс] :- Режим доступа: https://www.mnr.gov.ru/activity/np_ecology/ (дата обращения: 27.05.2024).

[2] Bochkovskiy A., Wang C.-Y., Mark Liao H.-Y. YOLOv4: Optimal Speed and Accuracy of Object Detection // Computer Vision and Pattern Recognition. 2020.
[3] ГОСТ Р МЭК 86-1-96. Батареи первичные. Часть 1. Общие положения. – М.: ИПК Издательство стандартов. 1997. 43 с.
[4] Sandler M., Howard A.G., Zhu M., Zhmoginov A., Chen L.-C. MobileNetV2: Inverted Residuals and Linear Bottlenecks // Computer Vision and Pattern Recognition. 2018. P. 4510.
[5] Canny J.A computational approach to edge detection // IEEE Transactions on Pattern Analysis and Machine Intelligence. 1986. PAMI-8(6). P. 679.
[6] Блатов Р.И., Вострякова Е.А., Москвин А.С., Чупров Д.А., Егоров Ю.С., Коротышева А.А., Милов В.Р., Дубов М.С., Кербенева А.Ю. Программа для ЭВМ «Прототип интеллектуальной системы идентификации немаркированных элементов питания с использованием методов машинного обучения» // Свидетельство об официальной регистрации программы для ЭВМ № 2022663863 от 20.07.2022 г.
[7] Коротышева А.А., Жуков С.Н. Разработка процедуры интеллектуальной идентификации объектов на основе анализа внутренней структуры // XXVIII Нижегородская сессия молодых ученых (гуманитарные, технические, естественные науки) : Статьи и тезисы молодых ученых, Нижний Новгород, 05–08 декабря 2023 года. – Нижний Новгород: Издательство "Перо", 2023. С. 255.

СРАВНЕНИЕ РАБОТЫ АЛГОРИТМОВ ВЫЯВЛЕНИЯ АНОМАЛИЙ В СЕТИ

Е.Н. Кривина, А.А. Рябов

ННГУ им. Н.И. Лобачевского

Обнаружение аномалий – это процесс выявления точек данных, сущностей или событий, которые выходят за пределы нормального диапазона, нахождение редких вещей или событий, которые по-разному отличаются от общей массы данных. Аномалия – это все, что отклоняется от стандартного или ожидаемого. Поэтому эту концепцию иногда называют обнаружением выбросов [1, 2].

На практике обнаружение аномалий часто используется для выявления подозрительных событий или плохих данных. Подозрительное событие может указывать на нарушение работы сети, мошенничество, преступление, болезнь. Аномалия также может быть результатом неисправности оборудования, поломки датчиков или отключения сети. Есть множество методов нахождения аномалий в данных, от статистических до применения алгоритмов машинного обучения.

Часто используемый набор методов – обучение с учителем, когда алгоритм обучается на помеченных данных. Метод контролируемого обучения основывается на существующих наборах данных с метками, которые называются обучающим набором, и путем сравнения с известными метками можно оценить прогнозируемый результат. Для принятия решения используется прошлый опыт, и для построения хорошо работающей модели всегда необходим высококачественный набор обучающих данных, однако удовлетворительный результат не гарантируется только набором данных, метод обучения является еще одним ключевым фактором в построении надежной модели. В обучении с учителем модель классификатора сначала создается путем обучения, после чего она может предсказывать дискретные или непрерывные выходы.

Популярными алгоритмами с обучением с учителем являются [3]:

- K-nearest neighbors (алгоритм K-ближайших соседей);
- Random forest (случайный лес);
- Gradient boosting (метод градиентного бустинга).

Для исследования взят набор данных UNSW-NB15, сетевые пакеты для которого искусственно создавались в лаборатории Cyber Range Lab UNSW Canberra для генерации гибрида обычных действий и атак [4-5]. Часть из этих данных была обработана и преобразована в тренировочный набор с 175000 записями. Этот набор включает 49 признаков с меткой, например, время жизни пакета, количество переданных байт, категорию атак.

Для набора составлена матрица корреляции признаков с метками. Одним из способов количественной оценки связи между переменными является использование коэффициента корреляции Пирсона, который является мерой линейной связи между переменными. На основе составленной матрицы были выбраны 9 численных признаков, которые являются наиболее важными для набора данных.

Для оценки работы алгоритмов использовались следующие метрики:

- Точность – доля объектов, названными классификатором положительными (выбросом) и при этом действительно являющимися положительными.
- Полнота – какую долю объектов положительного класса из всех объектов положительного класса нашёл алгоритм.

- F1-мера – среднее гармоническое двух метрик.

Обучение и тестирование работы алгоритмов по выявлению аномалий проводилось следующим образом:

1. Алгоритм обучался на наборе UNSW-NB15.
2. Для обучения с учителем набор разбивался в соотношении 1 к 2, где большая часть записей использовалась для обучения, меньшая для оценки работы алгоритма.

Результаты оценки работы алгоритмов приведены в таблице, где столбец 1 соответствует верному определению обычного действия, а столбец -1 – верному определению выброса. Общая оценка работы алгоритмов оценивается по метрике F1-мера. Значения F1-меры указаны в процентах.

Табл.

Название	Точность		Полнота		F1-мера
	1	-1	1	-1	
Градиентный бустинг	0,88	0,95	0,94	0,90	91,85
Алгоритм К-ближайших соседей	0,85	0,91	0,89	0,87	87,68
Случайный лес	0,90	0,95	0,94	0,91	92,26

Из таблицы видно, что алгоритм Случайный лес показал лучшие результаты.

Применение машинного обучения для выявления аномалий в сетевом трафике доказало свою эффективность как метод раннего обнаружения угроз.

[1] Hodge V.J., Austin J.A. // Artificial Intelligence Review. 2004. Vol. 22, No. 2. P. 39.
[2] Thwaini M.H. // Cukurova University Journal of Natural and Applied Sciences. 2022. Vol. 1. P. 34.
[3] Линдигрин А.Н. // Известия ТулГУ. Технические науки. 2019. № 12. С. 400.
[4] Nour M., Slay J. // Information Security Journal: A Global Perspective 2016. 2016. P. 1.
[5] Nour M. // Data Analytics and Decision Support for Cybersecurity: Trends, Methodologies and Applications. 2017. P. 127.

НОРМАТИВНО-ПРАВОВЫЕ И ТЕХНИЧЕСКИЕ АСПЕКТЫ ЗАЩИТЫ АСУ ТП

Р.Г. Нужный, Л.Ю. Ротков, В.А. Мокляков

ННГУ им. Н.И. Лобачевского

Технологическое производство в любой из сфер экономики и бизнеса на сегодняшний день не может обойтись без применения информационных технологий. Повышение эффективности производства и качества продукции предполагает среди прочего автоматизацию критических процессов, а вмешательство человеческого фактора сводят к минимуму, отдавая предпочтения отказоустойчивым высокопроизводительным системам АСУ ТП. Такой подход неизбежен и справедливо обоснован ввиду наличия опасностей, сопровождающих производство, связанное с нефтепереработкой, атомной энергетикой, космической отраслью, военной промышленностью, и другими сферами экономики. Глобальная автоматизация и информатизация производственных процессов также неизбежно увеличивает риски возникновения нештатных и кризисных ситуаций вследствие возникновения технических сбоев и отказов АСУ. Еще более опасным и внезапным фактором, влияющим на работоспособность АСУ, является недостаточная защищенность объектов КИИ от угроз информационной безопасности.

Стоит отметить, что далеко не во всех странах мира правительство разделяет ответственность по защите КИИ с их владельцами: Федеральным законом определена суть в обеспечении защиты и устойчивого функционировании КИИ при проведении в отношении ее компьютерных атак; Правительством Российской Федерации определен порядок категорирования объектов КИИ; Федеральными органами исполнительной власти и регуляторами разработаны обязательные к исполнению требования по защите таких объектов. При этом субъект КИИ избегает ответственности перед законом в случае возникновения наихудшего инцидента, повлекшего к возникновению негативных последствий, если им выполнены все обязательные требования по защите ОКИИ. В обязанности субъекта входит выявление критических процессов, нарушение которых принесет ущерб, и проведение инвентаризации всех ИС/ИТКС/АСУ. Далее составляется перечень объектов КИИ, и комиссией принимается решение о присвоении каждому из объектов КИИ одной из категории значимости, либо решение об отсутствии необходимости присвоения категории значимости, исходя из определения негативных последствий в случае компьютерного инцидента и подсчета значений показателей критериев значимости.

В данном процессе неизбежно возникают сложности в определении границ АСУ относительно других объектов КИИ: данная проблема ощутима на крупных предприятиях, осуществляющих в том числе химическое, металлургическое производство, производство в области машиностроения, топливно-энергетического комплекса и атомной энергии, где АСУ ТП представляет собой целостное решение, состоящие из систем автоматизированного управления и авторизированных устройств, выполняющие критические процессы, в том числе обеспечение промышленной безопасности. В такой ситуации стоит разделять АСУ ТП на составные части и каждую часть выделять как отдельный объект КИИ. Как правило такими составными частями являются:

- система диспетчерского управления и сбора данных (SCADA);
- система управления производством (MES);
- распределенная система управления (DCS);

- системы планирования (управления) ресурсами предприятия (ERP);
- система управления жизненным циклом продукции (PLM).

Другая проблема заключается в сложности оценки масштаба последствий в результате возникновения компьютерного инцидента на объектах, входящих в состав АСУ ТП. Такая сложность возникает даже после разделения АСУ ТП на отдельные объекты, т.к. они осуществляют один и тот же процесс и масштаб последствий схожий для каждого из объектов, что приводит к неточности расчетов значений показателей критериев значимости. Одним из вариантов решения такой проблемы является разбиение процесса на несколько параллельных процессов и (или) цепочек процессов. В результате появляется возможность в отдельности рассмотреть, является ли каждый процесс критическим, а также провести оценку масштаба последствий для каждого процесса, который является критическим, в отдельности.

Поскольку объекты КИИ очень разнообразны и специфичны, это делает очевидным невозможность их гарантированной защиты от всех возможных угроз. Субъект разрабатывает модель угроз нарушителя и безопасности информации на каждый объект КИИ, используя базовый, адаптивный и дополненный набор мер защиты в зависимости от актуальных угроз. В зависимости от специфики функционирования объекта и его размещения относительно границ КЗ, субъект по своему решению внедряет те или иные дополнительные меры защиты; создавая систему защиты значимого объекта КИИ, субъект также опирается на значения возможных рисков потери активов (информация, коммерческая тайна, оборудование, инфраструктура, и так далее). В зависимости от соотношения величины рисков и затрат на создание системы защиты объектов КИИ, субъект может внедрять современные решения по защите информации в тех уязвимых местах, где угроза атаки злоумышленником является наиболее актуальной. Для исключения воздействия извне контролируемой зоны субъекты стараются сделать объекты КИИ изолированными от внешних сетей связи; под внешними сетями в данном случае понимается не только «Интернет», но и, выделенная сеть смежного ведомства внутри единого предприятия, промышленной зоны, населенного пункта.

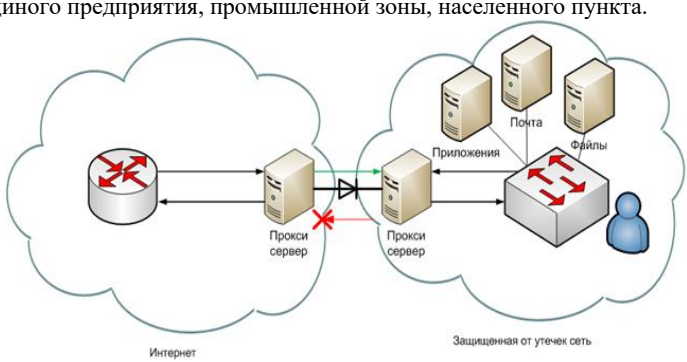

Рис. 1

Вместе с тем очень часто существует потребность передавать данные из сети связи с меньшим уровнем конфиденциальности в сети связи с более высоким уровнем конфиденциальности (рис. 1), другими словами, из открытой незащищенной сети в

систему в защищенном исполнении (АСЗИ). Так сложилось исторически, что система передачи данных с каждым годом становится все более универсальной средой для передачи самой различной информации как между конечными пользователями, так и между системными (служебными) устройствами. Чем больше универсальность, тем больше требований к этой системе. Также практически все современные инженерные системы имеют в своем составе встроенные компоненты для организации передачи разнородных данных (служебный "горизонтальный" трафик между устройствами, данные управления между центром управления и устройствами, мультимедийный трафик), имеющих непосредственное отношение к системам передачи данных [1].

Открытая сеть может быть источником сбора общедоступных данных, при этом данные могут быть соотнесены либо с самими собой, либо с другими наборами данных, и эта корреляция должна иметь гриф конфиденциальности. Иными словами, открытые данные могут и должны быть отнесены к конфиденциальным, в то же время как никакие конфиденциальные данные не должны выйти за пределы защищенного периметра. Угроза безопасности информации реализуется в результате образования канала реализации между источником угрозы и носителем (источником) информации, что создает необходимые условия для нарушения безопасности информации (деструктивного воздействия на нее или действия с ней). Для организации такого взаимодействия существуют сертифицированные решения, называемые однонаправленными шлюзами, или «Data Diode» (диод данных, рис. 2), и могут размещаться на канале передачи данных между двумя зонами с различными политиками информационной безопасности.

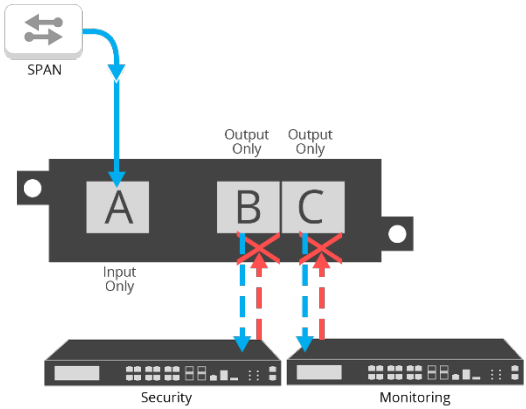

Рис. 2

Сетевые однонаправленные шлюзы – это специально разработанные аппаратные средства, которые позволяют «зеркалировать» сетевой трафик только в одном направлении [2]. Эту технологию теперь можно найти на уровне промышленного контроля для таких объектов, как атомные электростанции, производство электроэнергии и критически важные системы безопасности, такие как железнодорожные сети. Такая

конструкция позволяет создавать системы, недоступные для воздействия извне, но при этом допускающие сбор данных –например, телеметрии с промышленных датчиков. Обратная модель применения – получение защищённой сетью данных (например, обновлений) без возможности отправлять информацию за пределы периметра. Преимущество диодов данных над брандмауэрами заключается в том, что они устраняют фактор небрежного пользователя и разработчика. Поскольку диоды данных реализованы на аппаратном уровне, пользователи не могут неправильно настроить диод данных, и из-за его простоты маловероятно, что диод данных имеет скрытый недостаток конструкции, который позволит потоку данных вернуться в защищенный периметр.

К сожалению, такая организация взаимодействия между инфраструктурами различного уровня доступа всё равно не гарантирует защиту от утечки конфиденциальных данных с одной стороны и целостность и доступность с другой, поэтому требованиями к обеспечению защиты информации предусматривают в том числе использование граничных крипто-шлюзов, различного рода межсетевых экранов, систем обнаружения вторжений, антивирусную защиту, и так далее. Для обеспечения защиты информации используются в том числе анализаторы сетевых пакетов, устанавливаемые в информационной инфраструктуре в специально определенных точках захвата.

Если рассмотреть современную рабочую информационную инфраструктуру сложного объекта КИИ в разрезе уровней конфиденциальности составных сегментов, в ней обязательно будет присутствовать пересечение технологических процессов открытого и защищенного сегмента. Даже при условии организованного взаимодействия однонаправленной передачи данных между сегментами с разными уровнями конфиденциальности, на таких объектах необходимо обеспечивать дополнительные меры проверки отсутствия утечек данных, так как в результате инцидента ИБ данные с грифом конфиденциальности могут проникнуть в открытую сеть. Яркий и наиболее частый пример, когда нерадивый сотрудник использовал учтенный носитель секретной информации не по назначению, или в результате подключения этого носителя к машине, подключенной к открытой сети. То же самое может произойти, когда сотрудники не ознакомлены должным образом с политиками безопасности, подключают принесенный из дома USB-модем к защищенному локальному АРМ, обрабатывающему конфиденциальную информацию [3].

С учетом подобных инцидентов целесообразно дополнительно анализировать потоки однонаправленных данных между сегментами различного уровня конфиденциальности на предмет корреляции циркулирующих данных, для чего созданы и активно применяются системы обнаружения утечек информации (DLP-системы). Такие системы представляют из себя сложноорганизованную многоуровневую иерархию сбора и анализа данных, полученных в определенно выбранных точках захвата, при этом, чем сложнее инфраструктура объекта, тем сложнее и дороже DLP-система, ввиду увеличения количества обрабатываемых данных. Вместе с тем, большое количество циркулирующих данных требует быстроты и оперативности их обработки и анализа [4], и что немало важно отсутствия вмешательства в них, ведь, как известно, непрерывное и штатное функционирование объектов КИИ – есть основная цель организации таких объектов.

[1] Ищейнов В.Я. // Делопроизводство. 2022. №. 4. С. 97.

[2] https://www.anti-malware.ru/analytics/Market_Analysis/Data-Diodes
[3] https://www.securitylab.ru/contest/409633.php
[4] Плотников Л.М., Нужный Р.Г., Ротков Л.Ю., Мокляков В.А. // В Кн. Труды XXVII научной конференции по радиофизике (Нижний Новгород, 15—25 мая 2023 г.). – Нижний Новгород: ННГУ, 2023. С. 532.

МЕТОДЫ АУТЕНТИФИКАЦИИ, ПРИМЕНЯЕМЫЕ В IPSEC

А.А. Рябов, Е.А. Васильева

ННГУ им. Н.И. Лобачевского

Методы аутентификации в IPsec

IPsec – это семейство протоколов, обеспечивающих конфиденциальность и целостность данных при их передаче по публичной сети. Он используется для создания защищенных туннелей «точка-точка». Основу IPsec составляют протоколы IKE (Internet Key Exchange – протокол обмена ключами в сети Интернет), ESP (IP Encapsulating Security Payload – инкапсуляция защищенных данных IP) и AH (IP Authentication Header – аутентификационный заголовок IP). Все три протокола не зависят от конкретных криптографических алгоритмов, а описывают только общий набор методов и формат передачи данных.

AH и ESP используются для передачи пользовательских данных. Они гарантируют целостность сообщений и аутентифицируют их источник; кроме того, ESP еще обеспечивает конфиденциальность передаваемых данных.

Протокол IKE существует в двух версиях: IKEv1 и IKEv2. В статье рассматривается только IKEv1. По отношению к ESP и AH он выполняет вспомогательную функцию: стороны используют его для аутентифицированного обмена ключами по алгоритму Диффи-Хеллмана и согласования параметров защищенного соединения. Набор этих параметров вместе с выработанными ключами образует два однонаправленных логических соединения, называемых ассоциациями безопасности (англ. Security Association, SA). IKE согласует две пары SA: одну – для передачи своих данных и одну – для передачи пользовательских данных, поэтому работа IKE разделена на две части – фазы. Во время первой фазы протокол IKE согласует между сторонами ассоциации безопасности для передачи своих сообщений и таким образом создает защищенное соединение. Во второй фазе по этому защищенному соединению IKE согласует SA для работы ESP или AH. В результате второй фазы устанавливается защищенный туннель «точка-точка».

Аутентификация сторон происходит во время первой фазы, и существует четыре способа ее реализации [1]:

1) при помощи секретного ключа (англ. Pre-Shared Key, PSK);
2) при помощи электронной цифровой подписи (ЭП);
3) с использованием шифрования с открытым ключом (англ. Public Key Encryption, PKE);
4) с использованием переработанного режима шифрования с открытым ключом (англ. Revised Mode of Public Key Encryption, RPKE).

Аутентификация при помощи PSK является самой простой в настройке: каждому участнику соединения необходим только идентификатор другого участника и их общий PSK. Для работы данного варианта аутентификации не требуется установка и поддержка дополнительных систем. Очевидным недостатком является необходимость дополнительного защищенного канала для регулярного обновления PSK.

Остальные три варианта аутентификации в IKEv1 связаны с использованием криптографии с открытым ключом.

В варианте аутентификации при помощи ЭП каждая сторона формирует электронную подпись для имитовставки, охватывающей почти все сообщения 1-й фазы, и отправляет ее другой стороне. Другая сторона проверяет ЭП, и, если проверка завершается успешно, считается, что первая сторона прошла аутентификацию.

При аутентификации с использованием PKE каждая сторона использует открытый ключ другой стороны для зашифрования однократно используемого числа (англ. nonce) и своего идентификатора и затем отправляет их другой стороне. Другая сторона расшифровывает “nonce” своим закрытым ключом, формирует на его основе имитовставку для сообщений 1-й фазы и отправляет ее в ответном сообщении. При получении этого сообщения первая сторона тоже вычисляет имитовставку и сверяет свое значение со значением имитовставки, полученным от другой стороны. Эти значения совпадут только в том случае, когда другая сторона при формировании имитовставки использовала правильно расшифрованное значение “nonce”.

В варианте RPKE открытые ключи используются только для шифрования “nonce”, а для шифрования идентификаторов используется криптография с секретным ключом. С помощью шифрования с секретным ключом защищен и обмен ключами по алгоритму Диффи-Хеллмана, который в остальных вариантах аутентификации передается в открытом виде. Используемый секретный ключ вырабатывается на основе незашифрованного “nonce”. Это усложняет проведение атаки “человека посередине”.

Варианты аутентификации PKE и RPKE редко реализуются на практике [2].

PKI и сертификаты открытого ключа

Во всех вариантах аутентификации с использованием криптографии с открытым ключом проходящая аутентификацию сторона доказывает, что она является владельцем закрытого ключа: формирует с его помощью ЭП или расшифровывает сообщение от другой стороны. Другой стороне при этом необходимо знать открытый ключ аутентифицируемой стороны. Для этого она может использовать сертификат открытого ключа. Он содержит открытый ключ, идентификатор его владельца и сформированную для них электронную подпись доверенной третьей стороны, в роли которой обычно выступает центр сертификации (ЦС).

Центров сертификации может быть несколько, и в совокупности они образуют инфраструктуру открытых ключей (англ. Public Key Infrastructure, PKI). В целом, PKI является сложной системой, однако ее преимущества позволяют получить гибкий механизм управления ключами. Также, по сравнению с аутентификацией посредством PSK, добавление нового хоста в сеть IPsec не требует внесения изменений в настройки остальных хостов сети. Все это делает аутентификацию с использованием сертификатов наиболее часто используемой в сетях IPsec с большим количеством узлов.

При организации PKI необходимо учитывать много нюансов, касающихся безопасности связанной с PKI системы: ненадлежащее хранение закрытого ключа может привести к его компрометации и, если он принадлежит ЦС, изданию поддельных сертификатов и списков отозванных сертификатов; при утере закрытого ключа ЦС не сможет издавать списки отозванных сертификатов; недоступность или редкое обновление информации о статусе сертификатов снижает уровень доверия в системе; применение для подписи сертификатов нестойкого алгоритма цифровой подписи может привести к

использованию злоумышленниками уязвимостей в нем для издания поддельных сертификатов [3].

Для установления достоверности информации, содержащейся в сертификате, необходимо выполнять проверку цепочки сертификатов. Для этого можно использовать алгоритм, описанный в [3]. Критерием правильности выполнения проверки цепочки сертификатов в реализации служит совпадение результата проверки с результатом, который получается при использовании данного алгоритма.

От правильности и полноты реализации проверки цепочки сертификатов зависит безопасность передаваемых пользователем данных. Например, одним из шагов алгоритма [3] является проверка значения флага “cA”. Он входит в сертификаты ЦС, указывая на принадлежность содержащихся в них открытых ключей центрам сертификации, а следовательно – на то, что владельцы данных сертификатов вправе издавать сертификаты другим пользователям PKI. В сертификатах конечных пользователей данный флаг не должен быть установлен. Если программное обеспечение при проверке цепочки сертификатов пренебрегает проверкой данного флага, то возможна следующая атака [4]: злоумышленник получает у легитимного ЦС сертификат своего открытого ключа и, перехватывая подключение пользователя к сайту на этапе установления соединения, создает и подписывает своим ключом поддельный сертификат для этого сайта и отправляет его пользователю вместо настоящего. На стороне пользователя не проверяется флаг “cA” и сертификат злоумышленника признается действительным, поэтому злоумышленник может успешно перехватывать, расшифровывать и зашифровывать трафик между пользователем и сайтом.

Отсутствие выполнения проверки цепочки сертификатов или выполнение частичной проверки вместо полной является серьезной уязвимостью, и для ее обнаружения организации NIST [5] и BSI [6] разработали тесты и инструменты для их проведения. Задействованный в 2023 году для проверки российских средств ЭП инструмент NIST показал [7], что из трех средств ЭП только одно правильно выполняет проверку цепочки сертификатов, в двух других наблюдаются расхождения с ожидаемыми результатами в 10,5% и 6,5% тестов. Еще четыре средства ЭП не поддерживали зарубежные криптографические алгоритмы, и потому не участвовали в тестировании.

Проведение подобных тестов дает представление не только о правильности выполнения алгоритма в конкретной реализации, но и о функциональной совместимости данной реализации с другими.

Исходя из полученных в [7] результатов можно поставить задачу разработки системы тестов, в которой:

- тесты учитывают особенности функционирования PKI в конкретной области (в данном случае – IPsec);
- учитывается работа средств защиты информации с российскими криптографическими алгоритмами.

Таким образом, проблема создания системы тестов для аутентификации с использованием сертификатов в протоколе IKE является актуальной.

[1] Harkins D., Carrel, D. The Internet Key Exchange (IKE). RFC 2409. 1998.
[2] Frankel S., Kent K., Lewkowski R., Orebaugh A., Ritchey R., Sharma S. Guide to IPsec VPNs: Recommendations of the National Institute of Standards and Technology, Special

Publication (NIST SP) [электронный ресурс]. National Institute of Standards and Technology, Gaithersburg, MD. – 2005. Режим доступа: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=150393, свободный (дата обращения: 24.05.2024).
[3] Cooper D., Santesson S., Farrell S., Boeyen S., Housley R., Polk W. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280. 2008.
[4] Marlinspike M. More Tricks For Defeating SSL // DEFCON 17. 2009.
[5] Public Key Infrastructure Testing. X.509 Path Validation Test Suite. [электронный ресурс]. National Institute of Standards and Technology. Computer Security Resource Center. – 2016. Режим доступа: https://csrc.nist.gov/Projects/pki-testing/X-509-Path-Validation-Test-Suite, свободный (дата обращения: 24.05.2024).
[6] Certification Path Validation Test Tool. A test tool for checking X.509 certificate path validation. [электронный ресурс]. Federal Office for Information Security. Режим доступа: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Freie-Software/Certification-Path-Validation-Test-Tool/certification-path-validation-test-tool_node.html, свободный (дата обращения: 24.05.2024).
[7] Станкевич Т. PKI-TopGear: сравнительный тест средств электронной подписи // XXI международная конференция по проблематике инфраструктуры открытых ключей и электронной подписи. 2023.

ОПТИМИЗАЦИЯ ТОПОЛОГИИ РАЗМЕЩЕНИЯ ПУНКТОВ ПРИЕМА СИСТЕМЫ ОПРЕДЕЛЕНИЯ МЕСТОПОЛОЖЕНИЯ ИСТОЧНИКОВ РАДИОИЗЛУЧЕНИЙ

А.Э. Зотин, И.Н. Карельский, Л.Ю. Ротков

ННГУ им. Н.И. Лобачевского

При современных масштабах развития информационных радиотехнических систем различного назначения перспективной системой местоопределения источников радиоизлучения (ИРИ) может стать наземная пассивная двухпозиционная угломерно-разностно-дальномерная система (УРДС) [1]. Система состоит из двух пунктов приема сигналов ИРИ (ПП1, ПП2), разнесенных в пространстве на величину базы Б (рис. 1). Один из пунктов, например, ПП1, путем пеленгации определяет направления на ИРИ (β), а с помощью второго определяется расстояние (r), которое находится по формуле [1]:

$r = R^2 - Б^2/2(Б cos\beta - R)$, где $R = r - r_A = c(t_1 - t_2)$ – разность расстояний, определяемая по разности времен (t_1, t_2) в приходе сигнала, излученного ИРИ, на пункты приема ПП1 и ПП2, соответственно.

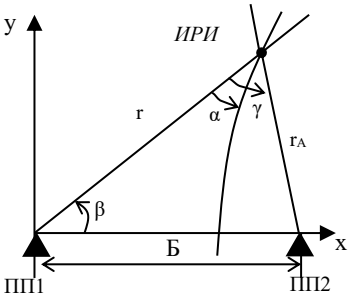

Рис. 1

Важной характеристикой УРДС, определяющей местоположение ИРИ, являются размеры *рабочей зоны системы* (РЗС), в которой среднеквадратическая ошибка (СКВО) измерения местоположения ИРИ не превышает максимально допустимую величину ($\sigma_{ири} \le \sigma_{ири\,max}$).

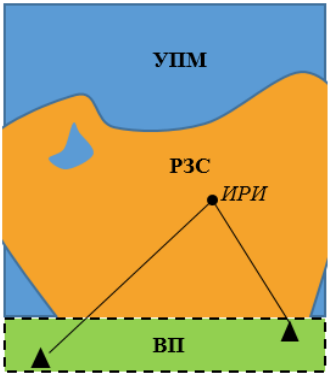

Рис. 2

РЗС находится в директивно установленной для системы *полосе местоопределения* (УПМ) (рис. 2). Обычно УПМ задается в виде границ (секторов или полос) относительно также директивно *выделенного участка пространства* (ВП), на котором должны быть размещены оба ПП.

СКВО $\sigma_{ири}$ для угломерно-разностно-дальномерного метода при некоррелированности измерений величин β и r зависит от ошибки определения линии положения (ЛП) постоянного пеленга на ИРИ $\sigma_{ЛП\beta}$ и ошибки определения ЛП постоянной разности дальностей до ИРИ $\sigma_{ЛПR}$, а также от угла α между двумя этими ЛП [2]:

$$\sigma_{ири} = \left(\sigma^2_{ЛП\beta} + \sigma^2_{ЛПR}\right)^{1/2} / sin\alpha \,.$$

СКВО $\sigma_{\text{ЛП}\beta}$ определяется СКВО пеленгатора σ_β и расстоянием r: $\sigma_{\text{ЛП}\beta} = r\sigma_\beta$, а СКВО $\sigma_{\text{ЛП}R}$ зависит от ошибки определения разности расстояний σ_R и угла γ под которым видна база системы (Б): $\sigma_{\text{ЛП}R} = \sigma_R / 2\sin\left(\frac{\gamma}{2}\right)$.

В УКВ диапазоне длин волн на размеры рабочей зоны УРДС существенное влияние оказывает рельеф земной поверхности в УПМ и ВП, на котором находятся ИРИ и ПП, так как дальность обнаружения ИРИ $R_{\text{обн}}$, в первую очередь наземных, ограничивается дальностью прямой видимости. Для её увеличения, требуется размещение ПП на высоких участках ВП. С другой стороны, ошибка местоопределения будет уменьшаться при увеличении базы (Б) (при углах α и γ близких к 90°), то есть, при размещении ПП ближе к краям ВП. Кроме того, на размещение ПП на некоторых участках ВП будут накладываться ограничения тактического и технического характера. Поэтому возникает потребность в оперативном адекватном определении мест расположения ПП с учетом противоречивых требований и объективных ограничений. Актуальность обозначенной задачи возрастает при относительно частой смене позиционного района применения УРДС.

В качестве *объекта исследования* рассматривается наземная двухпозиционная УРДС РТК, определяющая плоскостные координаты наземных ИРИ УКВ диапазона.

Целью исследования является разработка алгоритма определения оптимальных координат размещения ПП УРДС в новом позиционном районе, обеспечивающих максимальный размер РЗС при заданном ограничении на величину максимальной ошибки местоопределения с учетом рельефа земной поверхности и объективно установленных ограничений на размещение ПП.

РЗС рассматривается как суммарная зона обнаружения ИРИ каждым из ПП исходя из потенциальных (энергетических) дальностей обнаружения ИРИ ($R_э$) заданных техническими характеристиками ПП, и дальности прямой видимости ИРИ ($R_{\text{пв}}$), с учетом допустимых СКВО определения ЛП пеленга и ЛП разности дальностей.

В [3] и [4] предложен способ анализа дальности обнаружения $R_{\text{пв}}$ путем анализа и сравнения углов закрытия $\beta_{зi}$ и углов визирования цели (ИРИ) $\varepsilon_{цi}$. Углы закрытия определяются для каждого рассматриваемого направления приема ПП, а затем выбирается наибольший из них, который и будет углом закрытия на данном азимутальном направлении. Если $\beta_{зi} > \varepsilon_{цi}$, то выбирается $R_{\text{пв}} = R_з$, где $R_з$ – удаление фрагмента рельефа, препятствующего распространению ЭМВ. Если $\beta_{зi} \le \varepsilon_{цi}$, то $R_{\text{пв}}[\text{км}]$ можно рассчитать по формуле $R_{\text{пв}}[\text{км}] = 4{,}12\sqrt{|h_{\text{ИРИ}} - h_{\text{ПП}}|[\text{м}]}$, где $h_{\text{ИРИ}} = h_{\text{поз.ИРИ}} + h_{\text{ант ИРИ}}$ – абсолютная высота точки излучения ИРИ, с учетом высоты позиции $h_{\text{поз.ИРИ}}$ и высоты антенны $h_{\text{ант ИРИ}}$; $h_{\text{ПП}} = h_{\text{поз.ПП}} + h_{\text{ант ПП}}$ – абсолютная высота точки приема ПП, с учетом высоты позиции $h_{\text{поз.ПП}}$ и высоты антенны $h_{\text{ант ПП}}$.

Таким образом, при построении зон обнаружения ИРИ на возможных направлениях приема сигналов ПП необходимо определить дальность обнаружения сигналов ИРИ как минимальное из выше рассмотренных: $R_{\text{обн}} = min\{R_э, R_{\text{пв}}\}$. С этой целью необходимо иметь полную информацию о рельефе местности (абсолютных высотах) в местах возможного размещения ПП, ИРИ и на пути распространения ЭМВ: ПП-ИРИ. Данные о рельефе можно получить, например, путем отправки запросов сервису Google Map.

Алгоритм оптимизации. Под оптимизацией топологии размещения ПП УРДС будем понимать поиск ω — дискретного варианта размещения элементов системы, который обладает наилучшим значением показателя качества из заданного конечного количества вариантов $\Omega = \{\omega_1, \omega_2, \dots, \omega_n\}$, $\Omega \in Z_{\text{п}}$, область ВП. При этом под вариантом размещения, ω_i, $i = 1, \dots, n$, понимается совокупность векторов пространственных координат ПП системы $X_{\text{п}} = [x_{\text{п}1}, x_{\text{п}2}, \dots, x_{\text{п}m}]$, $Y_{\text{п}} = [y_{\text{п}1}, y_{\text{п}2}, \dots, y_{\text{п}m}]$, где m – число возможных вариантов размещения ПП, а показателем качества выступает площадь РЗС $S_{\Theta_{\text{р.}}}$. Таким образом, *целевой функцией в решаемой задаче является максимизация площади РЗС при заданных ограничениях:*

$$S_{\Theta_{\text{р.}}} = F(X_{\text{п}}, Y_{\text{п}}) \Rightarrow max.$$

Отмеченные выше ограничения на размещение ПП могут быть представлены в виде набора координат и линейных размеров, задающих области, в которых запрещено размещение пунктов приема сигналом системы местоопределения:

$$\Psi = \{(x_1, y_1, l_{x1}, l_{y1}), \dots, (x_n, y_n, l_{xn}, l_{yn})\},$$

где x_i, y_i – координаты центра прямоугольной области, l_{xi}, l_{yi} – расстояние от центра области до граней, составляющих прямоугольник, $\Psi \in Z_{\text{п}}$.

Зоны размещения пунктов системы и источников излучения можно представить в виде координатных матриц, содержащих соответственно $L_{\text{п}} = m_{\text{п}} * k_{\text{п}}$ и $L_{\text{ири}} = m_{\text{ири}} * k_{\text{ири}}$ элементов (m и k по осям x и y соответственно). Расстояние между элементами матриц Δ – шаг просмотра зон, выбираемый исходя из требуемой точности учета рельефа. Элементами этих матриц будут являться узлы координатной сетки соответствующих зон.

Алгоритм, используя метод полного перебора при анализе всех возможных комбинаций позиций ПП УРДС РТК в ВП, обеспечивает поиск наилучшего размещения для обеспечения наибольшей площади РЗС в пределах УПМ, учитывая заданные ограничения и критерии оптимизации. Этот подход, хотя и требует значительного времени на вычисления, позволяет учесть все возможные варианты и выбрать наилучшие.

Таким образом, в процессе анализа УПМ для каждого варианта размещения элементов системы строится РЗС на основании анализа ошибок определения МП. После этого проверяется возможность прямой видимости между точкой размещения ИРИ и каждым ПП. Если прямая видимость невозможна, то точки размещения ИРИ исключается из РЗС. Заключительным этапом алгоритма является выбор варианта размещения ПП, который обеспечивает наибольшую площадь РЗС.

На рис. 3 представлен результат оптимизации размещения ПП УРДС. В данном случае пункт системы, отвечающий за пеленгование и за определение времени прихода сигнала, алгоритм расположил справа. Рельеф местности данного района и полученные оптимальные позиции позволили получить РЗС площадью в 832 км^2. В сравнении с позициями, найденными без учета рельефа (рис. 4), наблюдается общее уменьшение площади, а также провалы в РЗС, связанные с невозможностью приема прямого сигнала из некоторых участков УПМ.

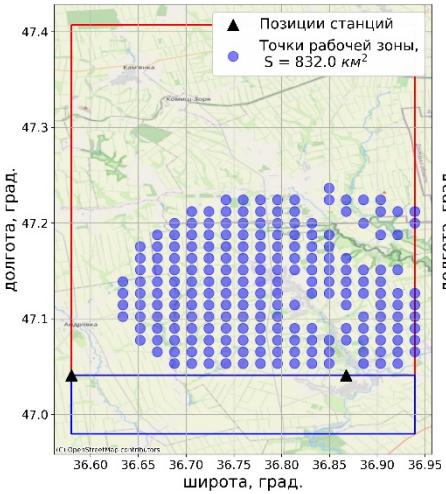

Рис. 3

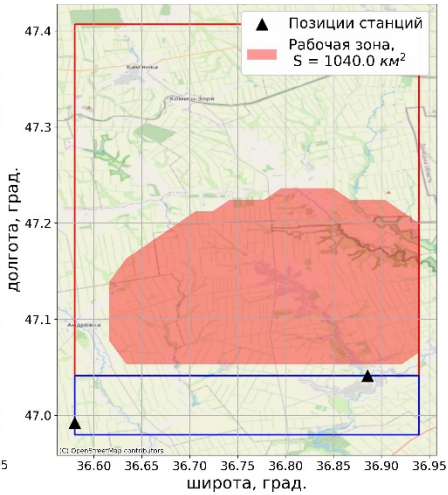

Рис.4

Из вышесказанного можно сделать следующие выводы:

1. Рельеф местности при размещении ПП УРДС в ВП существенно влияет на точность местоопределения ИРИ и размеры РЗС.

2. Разработанный алгоритм позволяет адекватно определять оптимальное размещение ПП УРДС и существенно сокращает время работы технического персонала по выбору позиций.

[1] Бердышев В.П., Гарин Е.Н., Фомин А.Н. Радиолокационные системы: учеб. / под общ. ред. В.П. Бердышева. – Красноярск: Сиб. федер. ун-т, 2011. 400 с.

[2] Дворников С.В., Саяпин В.Н., Симонов А.Н. Теоретические основы координатометрии источников радиоизлучений. // Учебное пособие. – СПб.: ВАС, 2007. 80 с.

[3] Беляев С.А., Экало А.В., Рубцов Е.А., Кудряков С.А. // Информатика и компьютерные технологии. 2022. №. 9 (28). С. 7.

[4] Чернышкова М.С. // Программные продукты, системы и алгоритмы. 2017. №. 2. С. 1.

Секция «Информационные системы.
Средства, технологии, безопасность»

Заседание секции проводилось 21 мая 2024 г.
Председатель – Л.Ю. Ротков, секретарь – А.А. Рябов.
Нижегородский государственный университет им. Н.И. Лобачевского