ИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ»

Вестник СибГУТИ Том 16, № 3, 2022

Выпускается ежеквартально, выходит с 2007 г.

Учредитель –
федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»

Адрес редакции и издателя

630102, г. Новосибирск, ул. Кирова, д. 86 e-mail: vestnik@sibguti.ru

Информация о журнале доступна в сети Internet по адресу https://vestnik.sibsutis.ru/jour.

Журнал включён в Перечень ВАК российских рецензируемых научных журналов, в которых должны быть опубликованы основные научные результаты диссертаций на соискание учёных степеней доктора и кандидата наук.

Журнал зарегистрирован Федеральной службой по надзору за соблюдением законодательства в сфере массовых коммуникаций и охране культурного наследия, свидетельство о регистрации ПИ № ФС77-25835 от 29.09.2006. ISSN 1998-6920. Подписной индекс в каталоге «Урал-Пресс» – 82519.

Дата выхода в свет 06.10.2022. Отпускная (редакционная) цена 750 руб.
Отпечатано в издательском центре СибГУТИ по адресу: 630102, г. Новосибирск, ул. Кирова, д. 86.
Бумага офсетная, формат А4. Тираж 300 экз.

СОДЕРЖАНИЕ

УДК 004.056.5:378.3
DOI: 10.55648/1998-6920-2022-16-3-3-13

Особенности формирования вектора современных сетевых атак

И. А. Ветров, В. В. Подтопельный

Рассмотрены проблемы, возникающие при постановке задачи определения вектора сетевой атаки в корпоративной информационной сети. Приведены и охарактеризованы разновидности методик, упрощающих построение вектора сетевой атаки, применяемых при анализе надежности информационных систем, рассмотрена их пригодность для различных процедур определения параметров вектора. При построении вектора сетевой атаки определяется специфика проявления параметра времени как характеристики, указывающей на более эффективный путь распространения компрометации. Формирование вектора рассматривается с учетом специфики многоуровневой организации сетей. Определяется специфика упрощенной модели вычисления вектора, которая включает процедуры, ориентированные на различные подходы.

Ключевые слова: вектор сетевой атаки, информационная система, корпоративная информационная сеть, уязвимость.

1. Введение

Для построения вектора атаки в Российской Федерации применяются несколько руководящих документов, последний из которых принят в 2021 году – «Методика оценки угроз безопасности информации» (далее – Методика). Приведенная в нём методика предлагает использовать при определении тактики злоумышленника массивы данных о признаках угроз, об уязвимостях, а затем, ориентируясь на экспертное мнение, формировать векторы атак с возможностью заимствования различных, в том числе зарубежных, способов описания сценариев реализации угрозы (CAPEC, ATT&CK, OWASP, STIX, WASC и др.) [1]. В данном документе при построении вектора предполагается учитывать угрозы, потенциал возможных нарушителей (уровень их квалификации, наличие средств атаки, а также предложено рассмотреть аспекты целеполагания нарушителей).

Приведённая методика направлена на рассмотрение в качестве целевого объекта распределенных информационных систем, построенных на клиентско-серверной архитектуре, но при этом не исключается рассмотрение локальных систем (они не предполагают применения сетевых технологий для поддержи работоспособности системных и пользовательских компонентов). Очевидно, что типы информационных систем и специфика поиска уязвимостей в этих информационных системах должны быть учтены при построении векторов атак по требованиям рассматриваемого методического документа. Однако в самой методике хотя и используются понятия риск (фактически подразумевается прогноз возможных действий злоумышленника), угроза, специфика классификации признакового пространства сетевых атак не учитывается, а построение последовательности тактик основано на экспертной оценке, которая зачастую неточна из-за субъективности оценок экспертов. Кроме того, сам предложенный способ описания вектора атаки не подразумевает формального учёта вероятностных показателей путей достижения цели злоумышленником (вероятность достижения цели злоумышленником

одним из путей предполагает наличие наиболее эффективного – быстрого и гарантированного – способа эксплуатации актуальных уязвимостей). Соответственно, для более точного построения сценария атаки, предложенную Методику требуется дополнить простыми (то есть не вызывающими затруднения при применении на производстве при построении модели угроз) формальными способами определения последовательности вредоносных воздействий (тактик).

2. Проблемная область формирования вектора атаки

Вектор атаки должен учитывать возможность возникновения нового направления атакующих воздействий или нового сценария реализации угрозы. Таким образом, вектор, построенный с учетом факторов, изменяющих направление атаки (в том числе с применением средств защиты), будет включать некоторое количество сегментов вектора, описываемых как состояния с признаками компрометации, признаками эксплуатации уязвимостей (несанкционированного доступа (НСД) на одном узле, на множестве узлов) [2]. Подобный способ формирования вектора выгоден при реализации аудита многоуровневых систем, поскольку в этом случае будут учитываться все особенности используемых при обработке информации технологий, особенности средств защиты. Продолжение вектора или определение нового направления вектора будет зависеть от меры успешности предыдущих атакующих последовательностей. При описании вектора в Методике предлагается использовать мнение экспертов, которые должны участвовать в обсуждении проблем безопасности и оценивании способов реализации различных угроз.

При сегментировании подсистем оцениваемых АИС и, соответственно, при использовании процедур поиска угроз и уязвимостей может проявиться проблема несогласованности оценок различных групп экспертов, занимающихся анализом своих профильных подсистем и компонентов технологически различающихся уровней одной информационной системы, что затрудняет определение направления вектора атаки при множестве данных о состоянии безопасности.

Некоторые сетевые параметры могут определяться как маркеры атаки только тогда, когда они используются совместно с другими маркерами или при определенных условиях их (маркеров) проявления. При этом их фиксация может указывать на простую ошибку передачи данных в сети. Таким образом, само выявление сигнатурных маркеров в некоторых случаях не гарантирует того, что выстроенный вектор атаки соответствует реалиям атакующих воздействий. Более того, повышается вероятность получения ошибочных сетевых пакетов при работе в сетях большого масштаба, а также при некорректной настройке маршрутизирующих устройств. Допустим, в векторе атак сегментов и уровней АСУТП признаки атаки следующие: запрос к закрытым портам сетевых служб; ошибочная последовательность флагов TCP при открытии соединения или в ходе соединения, множественная попытка открытий соединений в ограниченный период времени, неправильные контрольные суммы пакетов транспортных протоколов, IP-адрес сетевого узла назначения совпадает с IP-адресом источника, последовательный опрос портов. Последний параметр нельзя отнести к явным признакам атаки, так как он зависит от периодичности нагрузок на трафик [4]. Более того, сетевые атаки в своей сигнатурной последовательности могут включать больший массив признаков нормального трафика по сравнению с однозначно маркирующими класс атаки признаками или включать признаки других атак, что приводит к путанице при их классификации (рис. 1). Стандартно к параметрам, которые однозначно (явно) маркируют присутствие вредоносной активности или ошибочная интерпретация которых наименее вероятна, можно отнести:

1. Наборы флагов, которые не соответствуют стандарту соединения по TCP-протоколу (RFC-793).

2. Наличие в TCP-пакете порта узла-источника, равного 0 (нельзя использовать нулевой порт).

3. Несоответствие указанных контрольных сумм пакетов их оригинальным суммам.

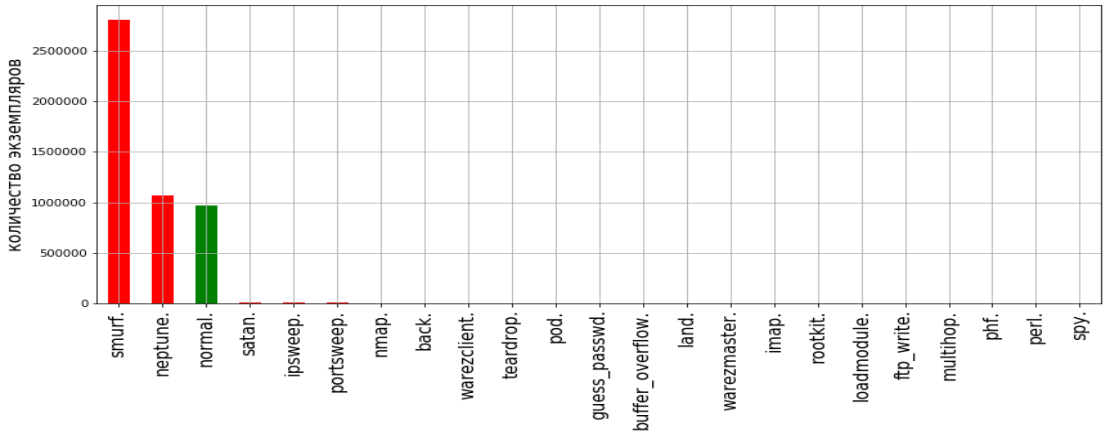

Рис. 1. Гистограмма распределения экземпляров данных

Таким образом, среди маркеров сетевых атак, позволяющих создать признаковое пространство, можно выделить два типа: явные и косвенные. Очевидно, что не все косвенные маркеры можно игнорировать. Однако при намеренном учете в правилах всех косвенных признаков вероятность ошибки при определении атаки будет возрастать. Соответственно, первоначально требуется при построении вектора атаки учитывать однозначно интерпретируемые признаки вредоносный действий. Общее представление о признаках, позволяющих различать классы атак на транспортном уровне OSI, приведено в табл. 1.

Таблица 1. Факторы (признаки), позволяющие различать векторы атак, которые распространяются параллельно в одной сетевой инфраструктуре

Данные, которые постоянно встречаются при анализе	Уникальные данные, которые следует учитывать в отдельных случаях
1. Количество принятых сетевых пакетов. 2. Число TCP-пакетов с ACK-флагом. 3. Число TCP-пакетов с SYN- флагом. 4. Число TCP-пакетов с FIN- флагом. 5. Время жизни сетевого пакета (TTL). 6. Число ICMP-пакетов. 7. Общее количество пакетов TCP. 8. IP-адреса сетевых узлов. 9. Длина сетевого пакета.	1. Число ICMP-ответов без ICMP-запросов. 2. Количество запросов с неправильными комбинациями флагов. 3. IP-адрес и MAC-адрес в ARP-reply. 4. Запросы к закрытым портам. 5. Пакеты опроса портов. 6. TCP-пакеты с портом источника 0. 7. Количество открытий соединений. 8. Число полуоткрытых соединений. 9. Число UDP-пакетов.

Чтобы снизить большое количество ложных срабатываний систем обнаружения вторжений (СОВ), требуется математическими методами скорректировать формируемый вектор атаки. На рис. 1 видно, что большая часть признаков атак имеет малый масштаб фиксации по сравнению с первыми атаками на диаграмме (показано красным цветом). Соответственно, при эксплуатации системы обнаружения вторжений плохо интерпретируемые сетевые атаки (с малым пулом данных) сложно распознавать с большой достоверностью при поведенческом и эвристическом анализе. При этом СОВ остаётся работоспособной и может отсеивать большой массив других атак [5].

Одним из способов построения вектора атаки является использование графа компрометации. В данном графе ребрами обозначаются соответствующие переходы (при эксплуатации уязвимостей) между состояниями компрометации следующих типов: зондирование, взлом, проникновение, эскалация, нанесение ущерба. Граф предполагает изменение направления

атаки в зависимости от наличия или отсутствия информации об уязвимостях системы и средств их эксплуатации. Показатель успешности атаки определяется по формуле [6]:

$$T = t_1 \cdot P_1 + P_2 \cdot (1 - P_1) \cdot t_2 + (1 - P_1) \cdot (1 - P_2) \cdot t_3, \quad (1)$$

где t_1 – ожидаемое время успешного завершения атаки при известности уязвимостей и средств их эксплуатации (обычно 1 день);

t_2 – ожидаемое время завершения атаки при неизвестности уязвимостей;

P_1 – вероятность успешного завершения атаки при известности уязвимостей и средств их эксплуатации;

P_2 – вероятность успешного завершения атаки при неизвестности уязвимостей [6].

Поскольку при рассмотрении корпоративных информационных систем (КИС) выделяются множества различных параллельно и последовательно связанных объектов, векторы атак необходимо представить при учете сегментированных подсистем, классифицируемых по специфике их функционального предназначения. Таким образом, выстраивается последовательность вероятностей проявления вредоносных воздействий, ассоциированных с конкретными элементами КИС. Это позволит локализовать узкие места в проекте КИС или определить при предварительном анализе область нахождения причины сбоев [7].

Другой подход к формированию предполагает формирование вектора на основе переходов в логическом отображении сетевой инфраструктуры организации исследуемых систем (топологический принцип), его можно привести в виде набора элементов нескольких множеств (элементы имеют различные взаимосвязи), которые и следует учитывать при разработке модели компрометации (рис. 2). Выделяются следующие типы множеств [8]:

– множество объектов узлов (U);

– множество потенциальных угроз проявления аномалий (A);

– множество средств ИБ, модифицирующих вектор атак (R).

При этом наборы векторов аномалий будут включать каждую ветку направленного графа распространения, вершинами которого будут являться элементы описанных множеств.

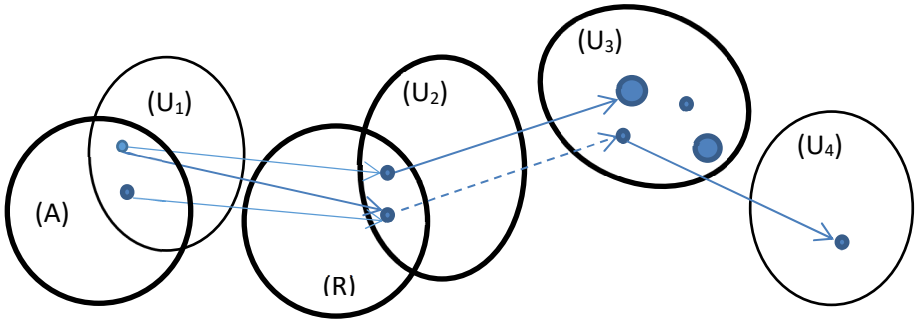

Рис. 2. Граф распространения вектора атаки со множествами сетевых узлов-вершин с учетом времени и альтернативного пути

Оба подхода не позволяют достоверно отобразить вектор развертываемой атаки с учетом всех особенностей. В первом случае применение топологических характеристик необязательно, а во втором случае не предполагается вычисление вероятностей переходов от одного узла к другому. Соответственно, требуется рассмотреть и совместить подходы, представляющие граф компрометации, то есть вектор атаки, как фиксацию признаков присутствия угрозы (состояния небезопасности на последовательности узлов) и граф компрометации как набор этапов, каждый из которых указывает на продвижение злоумышленника к цели своей атаки с определённой скорость (временем достижения состояния компрометации).

3. Построение вектора и определение скорости его распространения

Для построения вектора есть последовательность состояний, которые реализуются в виде последовательно фиксируемых признаков атаки на сетевых узлах с учетом времени фиксации признаков. Модернизированный граф с учетом времени и состояний компрометации формируется в контексте массива сходных атакующих воздействий (атаки со множеством способов реализации), при этом в каждом случае предполагается различная скорость достижения целей злоумышленника, что влияет на приоритет ветви вектора при выборе сценария атаки, а значит, позволяет определить его актуальность. Таким образом, ключевым параметром в описании вектора является время достижения некоторого компрометированного состояния, выраженного в виде ранее неактивного однозначно интерпретируемого признака атаки (набора признаков атаки). Описание этого признака – нетривиальная задача. Допустим, при анализе вектора сетевой разведки описание параметра времени компрометации резко осложняется неравномерной зависимостью скорости сканирования от количества портов тестируемого сетевого узла. В табл. 2 можно увидеть сильный разброс значений времени отклика при полуоткрытом SYN-сканировании с помощью утилиты Nmap. На показатели сканирования могут влиять следующие факторы [5]:

- показатель загрузки трафика в сети в период сканирования;
- пропускная способность сетевого интерфейса;
- количество Nmap-пакетов в сети в заданный период времени.

Таблица 2. Результаты полуоткрытого SYN-сканирования

№ раунда (эксперимента)	число портов	среднее значение, с.	1 скан.	2 скан.	3 скан.	4 скан.	5 скан.	6 скан.	7 скан.	8 скан.	9 скан.
1	1	0.63	0.63	0.65	0.62	0.62	0.63	0.64	0.61	0.63	0.65
2	10	1.82	1.82	1.82	1.80	1.83	1.86	1.82	1.82	1.80	1.79
3	100	2.05	2.04	2.06	2.05	2.04	2.07	2.05	2.05	2.04	2.04
4	250	2.37	2.43	2.40	2.30	2.25	2.40	2.40	2.32	2.41	2.43
5	500	5.45	6.21	6.20	6.20	3.16	6.19	3.11	3.14	3.14	11.71
6	750	7.83	9.20	8.61	8.60	8.00	7.81	7.69	7.82	4.10	8.60
7	1000	19.91	33.71	11.89	9.49	11.11	11.12	9.49	35.37	21.80	35.25
8	1500	27.54	14.23	16.53	16.75	34.12	14.21	16.52	49.80	45.27	40.45
9	2000	54.58	18.32	90.14	41.97	37.50	71.81	13.21	74.13	84.42	59.74

Присутствует смешение параметров-признаков угроз, и часть из представленных признаков с учетом фиксации времени их проявления становится белым шумом, если система не ориентирована четко дифференцировать векторы с учетом вредоносных операций (действий злоумышленника). Фиксируемые признаки можно представить в виде случайной дискретной последовательности длиной n отсчетов:

$$Y = [y_1, y_2, y_3, \ldots, y_n]. \tag{2}$$

Можно вероятностно описать с помощью многомерной плотности распределения вероятностей (a):

$$a(y_1, y_2, y_3, \ldots, y_n) = a(y_1) \cdot a(y_2 \mid y_1) \cdot a(y_3 \mid y_1, y_2) \cdot \ldots \cdot a(y_n \mid y_1, \ldots, y_{n-1}). \tag{3}$$

Но очевидно, что все параметры, фиксируемые подобным образом, будут независимыми между собой, что в рамках поля фиксируемых признаков будет смешение ложных признаков (рис. 3) и признаков отслеживаемой атаки (выделен на рис. 3 оранжевым цветом).

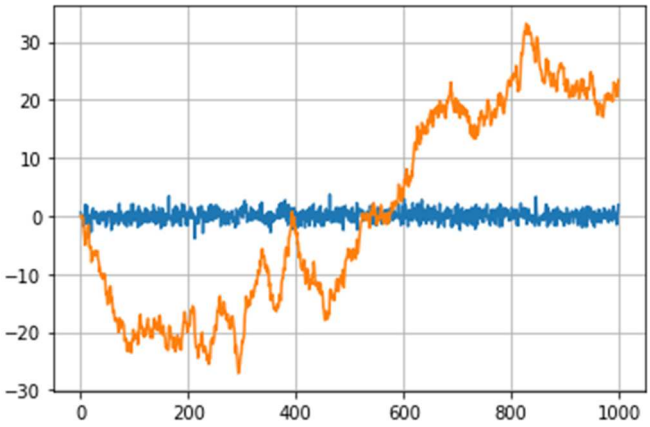

Рис. 3. Множества признаков вектора атаки

Тогда для того, чтобы представить связь признаков вредоносных воздействий (как фиксации состояния компрометации) при распространении вектора атаки, требуется условные распределения вероятности сделать зависимыми только от предыдущего момента их фиксации:

$$a(y_3 \mid y_1, y_2) = a(y_3 \mid y_2);$$
$$a(y_4 \mid y_1, y_2, y_3) = a(y_4 \mid y_3);$$
$$a(y_n \mid y_1, \ldots, y_{n-1}) = a(y_n \mid y_{n-1}).$$

Далее, классифицируя признаки атаки, все случайные последовательности, которые соответствуют правилу, выраженному в марковской последовательности, можно выразить следующим образом [9]:

$$a(y_1, \ldots, y_n) = a(y_1) \prod_{i=2}^{n} a(y_i \mid y_{i-1}),\ y_i = y_{i-1} + \xi_i, \tag{4}$$

где показатель y_{i-1} – предшествующее скомпрометированное состояние сетевого узла с фиксированным признаком атаки;

ξ_i – случайное изменение как величина нормальной плотности распределения вероятностей с нулевым математическим ожиданием и дисперсией σ_ξ^2.

Таким образом, типовой вектор атаки (то есть определение направления) можно наложить на сетевую топологию (требуется учитывать свёртки графа, если несколько признаков последовательно фиксируется на одном узле), чтобы получить последовательность и прогноз следующего шага нарушителя с учетом времени переходов от одного локализованного состояния компрометации к другому. Соответственно, можем определить все условные плотности распределения вероятностей переходов следующим образом:

$$a(y_i \mid y_{i-1}) = \frac{1}{\sigma_\xi \sqrt{2\pi a}} \cdot \exp\left(-\frac{\sigma_\xi}{2\sigma_\xi^2} \right), \tag{5}$$

Таким образом, можно произвести прогнозирование изменения вектора атаки и, соответственно, построить алгоритм ее реализации.

Формируемый вектор будет состоять из вершин, фиксируемых при переходах систем из одного состояния компрометации в типологически отличное следующие. Для коррекции роста дисперсии не требуется дополнительных вычислений, так как количество переходов в графе для корпоративных сетей мало и, соответственно, разброс величин (вероятностей отклонения вектора атаки) мал. При рассмотрении версий атакующих воздействий с учетом возможностей злоумышленника (два дополнительных варианта развития событий по графу компрометации) можно использовать типы этапов графа компрометации, при этом вычисляя время атаки с применением марковских последовательностей.

Тогда возникает пять основных множеств признаков при расчете временных показателей по числу типов переходов в графе компрометации (множество признаков состояний зондирования, взлома, проникновения, эскалации, нанесения ущерба) или десять в соответствии с типовыми тактиками Методики (множество признаков успешной реализации массива техник, принадлежащих к классам последовательно примененных тактик), что в итоге можно использовать при настройке средств защиты, ориентированных на определенные методы воздействия нарушителя. Для масштабных интернет-топологий с большим количеством узлов или состояний компрометации требуется скорректировать величину дисперсии, применив авторегрессии 1-го порядка (нужно добавить случайную величину с дисперсией).

Используя векторные марковские последовательности можно рассмотреть два типа векторов:

1. Первый тип с учетом состояний компонентов сети (по графу, по Методике) и времени, затрачиваемого на достижения этих состояний (t_i). При этом компоненты объединены по множеству типов воздействия и наличию признаков атаки (y_i). И для каждой из координат состояния компрометации можно записать модель:

$$\begin{cases} y_i = y_{i-1} + \xi_{ti} \\ t_i = t_{i-1} + \xi_{ti} \end{cases}. \quad (6)$$

На рисунках ниже изображены примеры векторов атаки с учетом состояний компрометации (рис. 4) и с учетом фиксации признаков проявления тактик злоумышленника (рис. 5). Вектор включает в свой состав порядок действий (фиксацию из признаков), характерный для следующих типов атакующих воздействий:

1. Сетевая разведка (сканирование Nmap, сниффинг).
2. ARP-спуфинг.
3. Перехват сеанса.

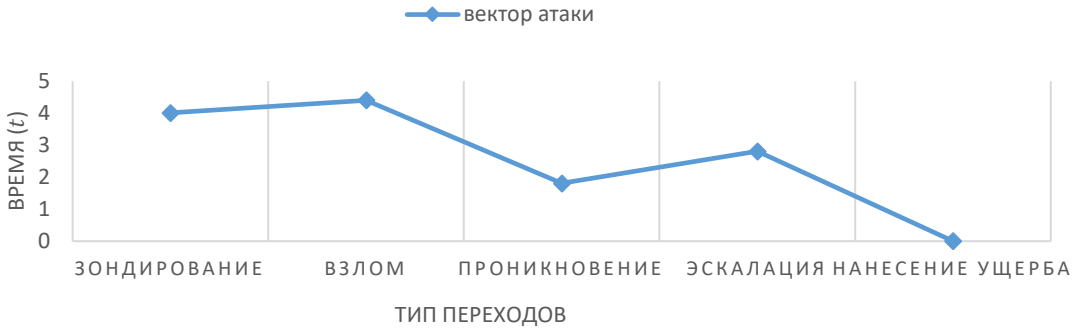

Рис. 4. Пример вектора атаки по числу типов переходов в графе компрометации

Рис. 5. Пример вектора атаки по числу типов тактик

2. Второй тип с учётом топологии сети. Для второго случая предлагается система координат, в которой учитывается уровень VLAN y_i (уровень агрегации сетевых пакетов и возможность воздействия на целевые сетевые узлы), последовательно связанные сетевые узлы (h_i), время фиксации признака угрозы (t_i). Принципы формирования координатной плоскости могут быть разными, предлагаются по степени приближения к ядру инфраструктуры и посегментно.

Для каждой из координат можно записать модель:

$$\begin{cases} y_i = y_{i-1} + \xi_{yi} \\ h_i = h_{i-1} + \xi_{hi} \\ t_i = t_{i-1} + \xi_{ti} \end{cases}. \quad (7)$$

Далее можно представить в векторно-матричной форме для первого и второго случая.

Для первого случая:

$$\begin{bmatrix} y_i \\ t_i \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} y_{i-1} \\ t_{i-1} \end{bmatrix} \begin{bmatrix} \xi_{hi} \\ \xi_{xi} \end{bmatrix}. \quad (8)$$

Для второго случая:

$$\begin{bmatrix} y_i \\ h_i \\ t_i \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} y_{i-1} \\ h_{i-1} \\ t_{i-1} \end{bmatrix} \begin{bmatrix} \xi_{hi} \\ \xi_{xi} \\ \xi_{xi} \end{bmatrix}. \quad (9)$$

Тогда изменения координат в векторе атаки, а следовательно, и его направление в топологии сети, динамика изменения состояний систем (g_{yi}) по матрице определяются следующим образом (применяется для вычисления каждой координаты):

$$\begin{cases} y_i = y_{i-1} + \xi_{hi} \\ g_{yi} = g_{yi-1} + \xi_{xi} \end{cases}. \quad (10)$$

Наиболее приоритетный вектор будет определяться высокой скоростью достижения цели, то есть наименьшим количеством времени, затраченным на преодоления всех вершин графа конкретной атаки (атаки, характеризуемой связанным набором признаков, комбинацией признаков как маркеров состояний компрометации), и, соответственно, общим количеством времени, затраченным на реализацию вектора атаки.

4. Заключение

Таким образом, при определении вектора атаки в дополнение к методикам, изложенным в методических документах ФСТЭК, а также к теории применения графа компрометации можно использовать векторные марковские последовательности. Их применение представлено в двух подходах, один из которых позволяет рассматривать в двумерном представлении переходы между состояниями компрометации с прогнозированием этих переходов (это дает возможность определить степень достижения цели злоумышленником посредством фиксации актуального состояния компрометации в одной из типовых зон), а второй подход позволяет рассмотреть переходы между компрометируемыми узлами или состояниями этих узлов (также с возможностью прогнозирования последующих состояний). При этом учитывается специфика перемещения фиксации актуальных действий нарушителя внутри или между различными зонами, сегментами сети. Применение одного из приведенных способов рассмотрения вектора атаки позволяет с большей точностью формировать сценарии атаки при анализе угроз информационной безопасности сетевой инфраструктуры. Совмещение этих подходов в дальнейшем предполагает рассмотрение кортежа нескольких разнотипных признаков (в *n*-мерном пространстве), что затруднит визуализацию результатов, но позволить более точно прогнозировать степень повышения опасности при реализации сценария атаки.

Литература

1. Методика оценки угроз безопасности информации // Методический документ ФСТЭК России: утв. ФСТЭК России России 5 февраля 2021 г.
2. ГОСТ Р 56546-2015 Национальный стандарт российской федерации. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. М.: Стандартинформ, 2018.
3. *Горбачев И. Е., Глухов А. П.* Моделирование процессов нарушения информационной безопасности критической инфраструктуры // Труды СПИИРАН. 2015. Вып. 1 (38). С. 112–135.
4. *Котенко И. В.* Многоагентные технологии анализа уязвимостей и обнаружения вторжений в компьютерных сетях // Новости искусственного интеллекта. 2004. № 1. С. 56–72.
5. *Щеглов А. Ю.* Защита компьютерной информации от несанкционированного доступа. СПб.: Наука и Техника, 2004. 384 с.
6. *Галатенко В. А.* Управление рисками: обзор употребительных подходов (часть 2) // Jet Info. 2018. № 12.
7. *Астахов А.* Введение в аудит информационной безопасности // GlobalTrust Solutions [Электронный ресурс]. 2018. URL: `http://globaltrust.ru` (дата обращения: 29.01.2018).
8. *Аверченков В. И., Рытов М. Ю., Гайнулин Т. Р* Оптимизация выбора состава средств инженерно-технической защиты информации на основе модели Клементса–Хоффмана // Вестник Брянского государственного технического университета. 2008. № 1 (17).

9. Марковские процессы в дискретном времени: [сайт]. URL: https://propproprogs.ru/dsp/markovskie-processy-v-diskretnom-vremeni.

Статья поступила в редакцию 15.05.2022.

Ветров Игорь Анатольевич
к.т.н., доцент, образовательно-научный кластер «Институт высоких технологий», Балтийский федеральный университет им. И. Канта (236041, Калининград, ул. Александра Невского, 14), e-mail: vetrov.gosha2009@yandex.ru.

Подтопельный Владислав Владимирович
старший преподаватель, Институт цифровых технологий ФГБОУ ВО «КГТУ» (236022, Калининград, Советский пр., 1), e-mail: ionpvv@mail.ru.

Vector formation features of modern network attacks

Vetrov Igor Anatolyevich
Candidate of Technical Sciences, Associate Professor, Institute of Physical and Mathematical Sciences and Information Technologies, I. Kant Baltic Federal University (14 Alexander Nevsky Str., Kaliningrad, 236041), vetrov.gosha2009@yandex.ru.

Podtopelny Vladislav Vladimirovich
senior lecturer, Institute of Digital Technologies of KSTU (236022, Sovetsky ave., 1, Kaliningrad, Kaliningrad region), ionpvv@mail.ru.

The problems that arise when setting tasks for determining the vector of a network attack in a corporate information network are considered. The varieties of various techniques that simplify the construction of a network attack vector used in the analysis of the reliability of information systems are presented and characterized. The suitability for various procedures for determining vector parameters is considered. When constructing a network attack vector, the specificity of the manifestation of the time parameter was determined as a characteristic indicating a more effective way of spreading compromise. The formation of the vector is considered taking into account the specifics of the networks multilevel organization. The specifics of the simplified vector calculation model including procedures focused on various approaches are determined.

Keywords: vectors of network attack, information systems, corporate information network, vulnerability.

References

1. *Metodika otsenki ugroz bezopasnosti informatsii Metodicheskii dokument FSTEK Rossii: utv. FSTEK Rossii 5 fevralya 2021*. [Methodology for assessing threats to information security Methodological document of the FSTEC of Russia]. Moscow, 2021.
2. *GOST R 56546-2015 Natsional'nyi standart rossiiskoi federatsii. Zashchita informatsii. Uyazvimosti informatsionnykh sistem. Klassifikatsiya uyazvimostei informatsionnykh system* [National Standard of the Russian Federation. Data protection. Vulnerabilities of information systems. Classification of vulnerabilities of information systems]. Moscow, Standartinform, 2018.
3. Gorbachev I. E., Glukhov A. P. Modelirovanie protsessov narusheniya informatsionnoi bezopasnosti kriticheskoi infrastruktury [Modeling the processes of violation of information security of critical infrastructure]. *Trudy SPIIRAN*, Moscow, 2015, iss. 1(38), pp. 112 – 135.

4. Kotenko I. V. Mnogoagentnye tekhnologii analiza uyazvimostei i obnaruzheniya vtorzhenii v komp'yuternykh setyakh [Multi-agent technologies for vulnerability analysis and intrusion detection in computer networks]. *Novosti iskusstvennogo intellekta*, 2004, no. 1, pp. 56–72.
5. Shcheglov A.Yu. *Zashchita komp'yuternoi informatsii ot nesanktsionirovannogo dostupa* [Protection of computer information from unauthorized access]. Saint Petersburg, Science and Technology, 2004, 384 p.
6. Galatenko V.A. Upravlenie riskami: obzor upotrebitel'nykh podkhodov (chast' 2) [Risk management: a review of common approaches (part 2)]. *Jet Info*, no. 12, 2018, available at: `https://www.jetinfo.ru/upravlenie-riskami-obzor-upotrebitelnykh-podkhodov-chast-2/` (accessed: 29.01.2022).
7. Astakhov A. Vvedenie v audit informatsionnoi bezopasnosti [Introduction to information security audit [Report]], *GlobalTrust Solutions*, 2018, available at: `http://globaltrust.ru` (accessed: 29.01.2018).
8. Averchenkov V.I., Rytov M.Yu., Gainulin T.R Optimizatsiya vybora sostava sredstv inzhenerno-tekhnicheskoi zashchity informatsii na osnove modeli Klementsa–Khoffmana [Optimization of the choice of the composition of the means of engineering and technical protection of information based on the Clements–Hoffman model]. *Vestnik Bryanskogo gosudarstvennogo tekhnicheskogo universiteta*, Bryansk, 2008, no. 1(17).
9. *Markovskie protsessy v diskretnom vremeni* [Markov processes in discrete time], available at: `https://proproprogs.ru/dsp/markovskie-processy-v-diskretnom-vremeni` (accessed: 29.01.2022).

УДК 004.9
DOI: 10.55648/1998-6920-2022-16-3-14-28

Интегральная модель оценки защищенности объектов информатизации в условиях деструктивного воздействия

В. В. Баранов[1]

В работе проведено обоснование необходимости создания информационной системы поддержки принятия решений при разработке систем защиты объектов информатизации, проведен анализ существующих систем в различных областях деятельности, определены требования к функционалу системы применительно к области защиты информации, рассмотрены методы разработки моделей функционирования защищенных информационных систем в условиях деструктивного воздействия на основе байесовских сетей, приведено описание функционирования типового модуля данной модели, рассмотрены структуры вероятностных моделей взаимосвязей уязвимостей, угроз безопасности информации, способов и сценариев их реализации, формирования мероприятий по защите объектов информатизации, формирования и оценки рисков инцидентов и ущерба от них, определены кластеры формирования типовых событий информационной безопасности, приведен методический аппарат для проведения расчетов совместного распределения вероятностей защитных и деструктивных событий, выявлены типовые цепочки взаимосвязей таких событий, разработан математический аппарат для расчета их вероятностей, приведено вербальное описание закономерностей их взаимного влияния, а также представлена методика перевода количественных вероятностных значений показателей защищенности объекта информатизации в качественные и подведены итоги проведенного исследования.

Ключевые слова: поддержка принятия решений, байесовская сеть, деструктивные воздействия, меры защиты информации, угрозы безопасности информации, стратегия управления, события информационной безопасности, анализ влияний, структурный анализ, системы защиты.

1. Введение

Наиболее сложным аспектом в процессе разработки систем защиты является полнота и качество оценки угроз безопасности информации, принятие обоснованного решения об их актуальности, а также выбор комплекса мер и средств защиты информации, эффективных в складывающейся обстановке.

Данный процесс строго регламентирован и основывается на требованиях организационно-правовых и методических документов [1–9]. Их структура представлена на рис. 1.

На этапе функционирования в условиях динамично меняющегося деструктивного воздействия система защиты требует непрерывного оперативного управления, своевременного и

1 Работа выполнена при финансовой поддержке гранта MTUSI, предоставленного Министерством финансов Российской Федерации из федерального бюджета в 2021 году (научный проект № 35/21-d) в рамках федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации».

обоснованного реагирования на возникающие новые риски и угрозы безопасности информации.

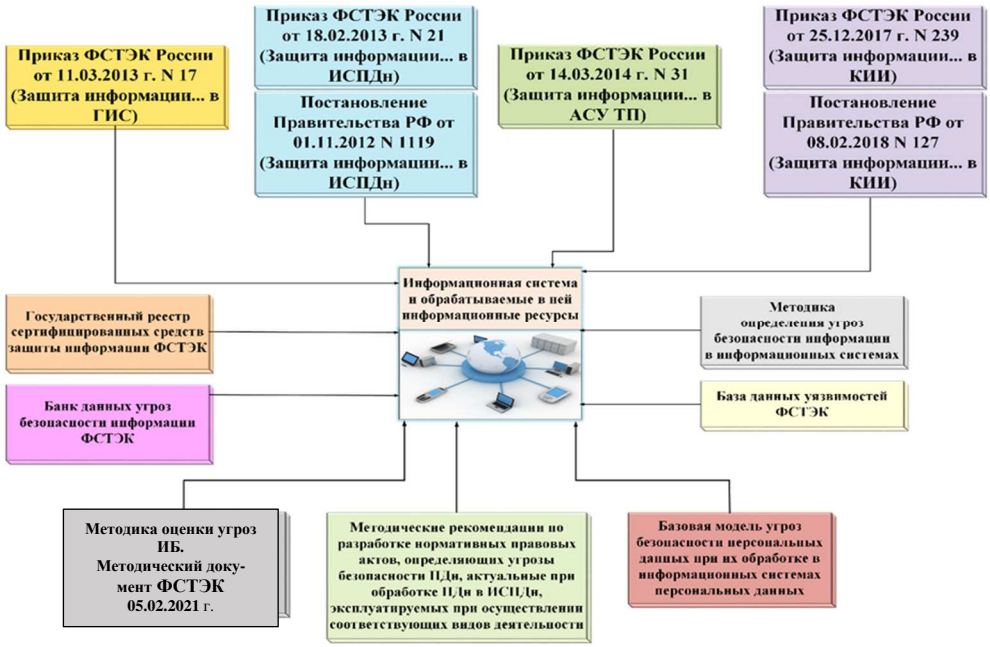

Рис. 1. Нормативно-правовое обеспечение формирования способов защиты информационных систем

Анализ содержания указанных организационно-руководящих методических документов показал, что данные задачи решаются методом экспертной оценки, что определяет субъективность принимаемых решений, качество которых зависит от полноты данных по складывающейся обстановке и подготовленности экспертов. В данном документе не рассматриваются методические подходы по оценке угроз безопасности информации, связанных с нарушением безопасности шифровальных (криптографических) средств защиты информации, а также угроз, связанных с техническими каналами утечки информации.

Это обстоятельство определяет необходимость создания новых и совершенствования существующих методических и инструментальных средств автоматизации процесса поддержки принятия экспертных решений в задачах разработки и оценки эффективности комплекса мер защиты информационных систем.

Анализ существующих автоматизированных информационных систем поддержки принятия решений (ИСППР) в различных областях деятельности позволяет выделить три их основных типа [10, 11].

Первый тип – это пассивные ИСППР, обрабатывающие данные и представляющие лицу, принимающему решение (ЛПР), структурированную информацию и отчеты. При этом конкретное решение принимается человеком.

Второй тип – это активные ИСППР. Данные системы формируют потенциальные решения на основе обработанной базы данных, а также предлагают возможные альтернативы действий.

К третьему типу относятся комбинированные ИСППР, которые предлагают вероятные решения и альтернативы, но при этом ЛПР может вносить уточнения, добавлять условия и отправлять проект на повторную обработку. В таких ситуациях прорабатываются различные модели, что позволяет принять оптимальное решение.

Исходя из существующего подхода к разработке способов защиты информационных ресурсов и подбору средств и мер защиты информации (рис. 2), наиболее подходящими для области информационной безопасности будут являться комбинированные ИСППР.

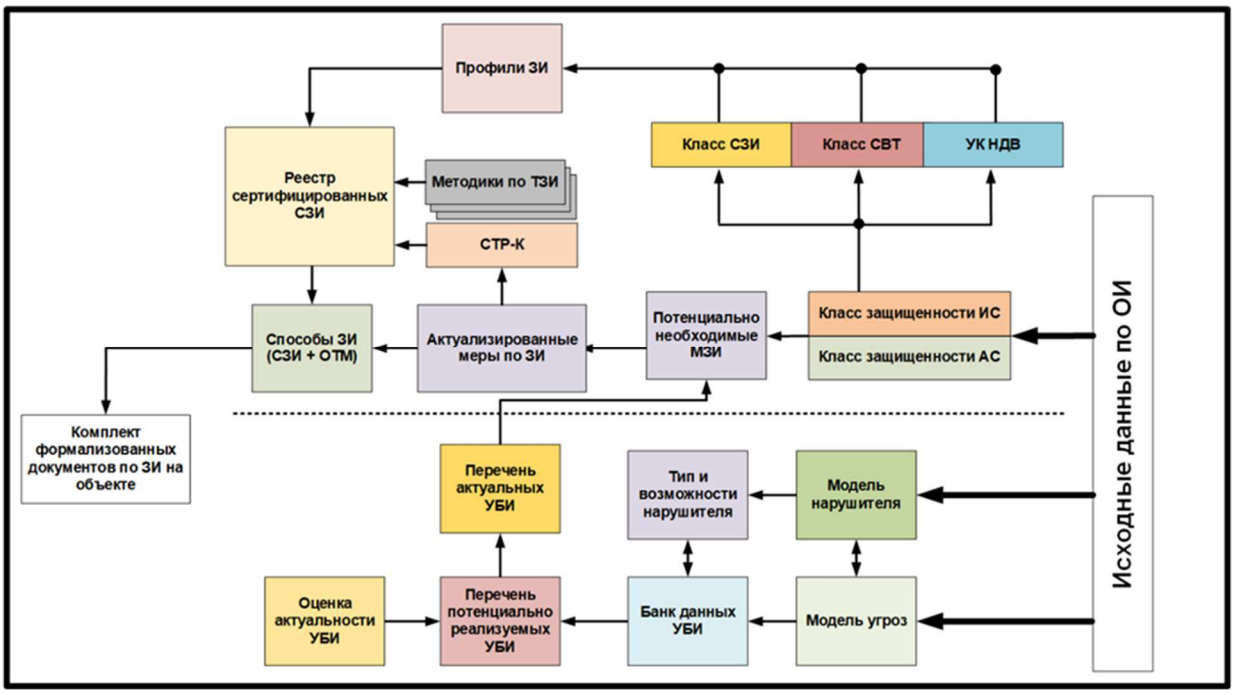

Рис. 2. Структурная схема процесса разработки способов защиты информационных ресурсов

Большинство существующих в настоящее время комбинированных ИСППР основаны на программных продуктах для работы с байесовскими сетями [12, 13, 14]. Их следует классифицировать прежде всего по способу использования. В случае, если основная задача исследователя – решить конкретную прикладную проблему, то необходимо выбрать готовый пакет, обладающий максимальными свойствами, необходимыми исследователю. В работе был проведен анализ ряда наиболее функционально адаптированных к области информационной безопасности программ.

BayesiaLab представляет собой комплексный инструмент для создания и использования байесовских сетей. С помощью пакета BayesiaLab можно определять, изучать, редактировать и анализировать байесовские сетевые модели. [15, 16, 17].

Программный продукт AgenaRisk можно применять для широкого круга проблем, связанных с неопределенностью. Пакет предназначен для моделирования проблем, связанных с использованием карт рисков – сочетание статистического моделирования и технологий BN. Это обеспечивает сочетание мощности, простоты использования и гибкости. AgenaRisk поддерживает как диагностические, так и интеллектуальные неопределенности. Сильной стороной AgenaRisk является возможность работы с различными типами моделей, обучение байесовской сети, применение различных типов распределений, а также графическая визуализация при анализе рисков [18, 19, 20].

Программный продукт Hugin и его ядро Hugin Development Environment состоят из трех основных компонентов.

Первый – Hugin GUI – это интерфейс для создания и модификации сетевых моделей и их реализации путем ввода фактов и отображения результирующих распределений вероятностей и ожидаемого использования. В режиме редактирования модуль позволяет определять узлы путем вставки узлов, их объединения, определения состояний и действий, таблиц условной вероятности и таблиц полезности.

Второй компонент – система принятия решений Hugin (HDE) – является ядром системы, которая выполняет вывод на основе данных, представленных байесовской сетью или диаграммой влияния. Система позволяет формировать и использовать базы знаний с применением объектно-ориентированных байесовских сетей. Она также позволяет использовать как дискретные, так и непрерывные переменные, прямое определение условного распределения

вероятностей, определять отношения вспомогательных функций с помощью математических и логических описаний [21, 22].

Анализ возможностей указанных программных продуктов позволил выделить их сильные стороны, необходимые для выполнения задачи поддержки принятия решений в области информационной безопасности. Такая информационная система должна обладать рядом перечисленных ниже функций.

Функция моделирования будет обеспечивать процесс разработки решений на основе построения вероятностных, ситуационных, аналитических, имитационных и других моделей.

Функция обработки баз данных (информационно-расчетная функция) обеспечивает принятие решений на основе цифровых хранилищ информации по конкретной организации, ее активам, информационной системе, классам нарушителей, угрозам безопасности информации, способам их реализации, уязвимостям, организационным и техническим мерам защиты информации и др.

Функция обработки баз знаний (аналитическая функция) реализует процесс принятия решений в условиях нечетких исходных данных на основе сценариев выполнения аналогичных задач с учетом статистических закономерностей, зависимостей и установленных методик и алгоритмов.

Функция обеспечения коммуникативности обеспечивает возможность взаимодействия нескольких должностных лиц, работающих над одной задачей.

Функция документирования обеспечивает процесс разработки комплекта документов по принятым решениям.

Реализация данной задачи может быть осуществлена путем разработки комплексной динамической модели функционирования защищенных информационных систем различного назначения в условиях деструктивного воздействия, позволяющей также моделировать процесс оперативного управления событиями информационной безопасности в условиях изменений воздействующих факторов.

2. Обсуждение

В основу данной модели предлагается заложить типовые модули, отражающие процесс функционирования защищаемой информационной системы в условиях деструктивного воздействия (рис. 3).

В составе модуля выделены четыре кластера:

1. Кластер формирования рисков угроз безопасности информации.
2. Кластер ликвидации рисков угрозы инцидента.
3. Кластер формирования рисков инцидента.
4. Кластер ликвидации последствий инцидента.

Моделирование в динамике складывающейся ситуации осуществляется, как описано ниже. Ввод исходных данных осуществляется по направлению деструктивных воздействий и направлению защитных мер.

Кластер рисков угроз безопасности информации формируется путем моделирования характеристик потенциальных возможностей нарушителя, который обладает неким функционалом показателей, соответствующих определенному классу $\{КлН_1 \ldots КлН_i\}$. Каждый из классов нарушителей способен с определенной вероятностью реализовать множество угроз безопасности информации (УБИ) определенными способами, составляющими для каждой УБИ множество $\{S_1 \ldots S_i\}$. Фрагмент матрицы потенциальных возможностей разных классов нарушителей по реализации УБИ представлен на рис. 4.

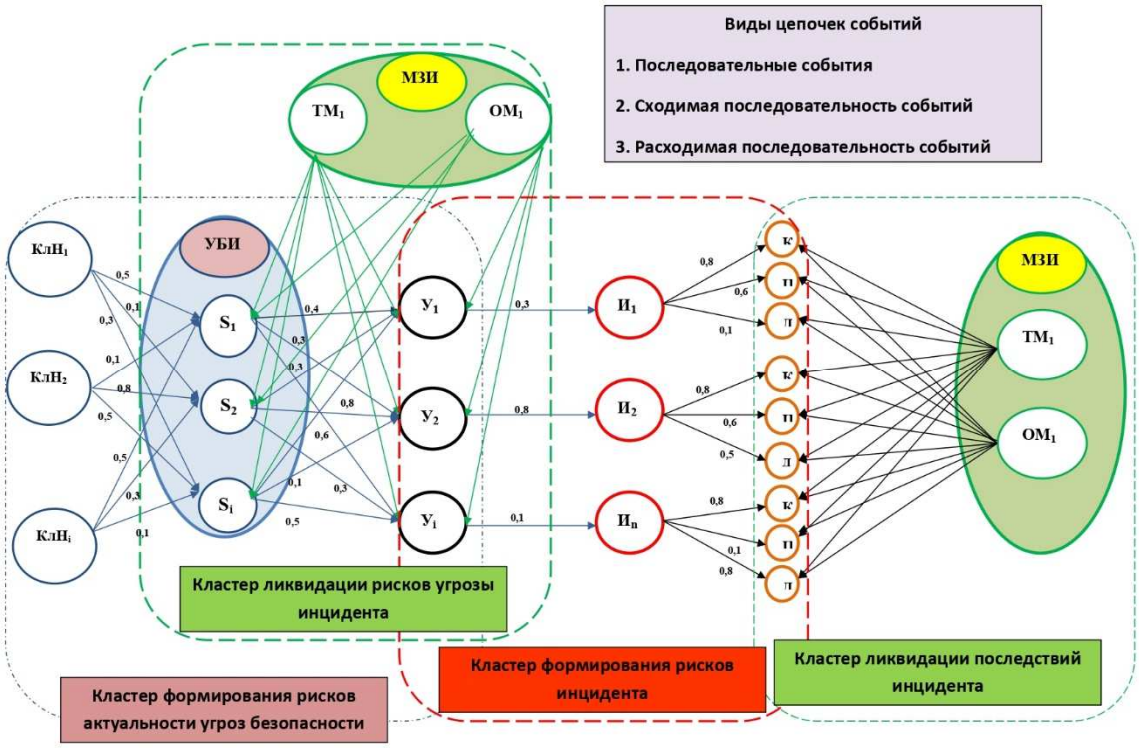

Рис. 3. Типовой модуль комплексной динамической модели функционирования защищенных информационных систем

УБИ реализуется через уязвимости, составляющие множество $\{Y_1 \ldots Y_i\}$. Исходные данные по типам, содержанию и характеру проявления УБИ и уязвимостей можно получить из банка на сайте ФСТЭК, перечней, разрабатываемых для каждого защищаемого объекта информатизации, и других баз данных.

		Нарушитель внутренний			Нарушитель внешний с высоким потенциалом		
		Нарушитель внутренний с высоким потенциалом	Нарушитель внутренний с средним потенциалом	Нарушитель внутренний с слабым потенциалом	Нарушитель внешний с высоким потенциалом	Нарушитель внешний с средним потенциалом	Нарушитель внешний с слабым потенциалом
24	Угроза изменения режимов работы аппаратных элементов	1					
25	Угроза изменения системных и глобальных переменных		1				
26	Угроза искажения XML-схемы		1			1	
27	Угроза искажения вводимой и выводимой на периферийные устройства информации			1	1		
28	Угроза использования альтернативных путей доступа к ресурсам			1			1
29	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами			1			1
30	Угроза использования информации идентификации/аутентификации, заданной по умолчанию			1		1	
31	Угроза использования механизмов авторизации для повышения привилегий			1			1
32	Угроза использования поддельных цифровых подписей BIOS					1	
33	Угроза использования слабостей кодирования входных данных		1			1	
34	Угроза использования слабостей протоколов сетевого/локального обмена данными			1			1
35	Угроза использования слабых криптографических алгоритмов BIOS				1		
36	Угроза исследования механизмов работы программы		1			1	
37	Угроза исследования приложения через отчёты об ошибках		1			1	
38	Угроза исчерпания вычислительных ресурсов хранилища			1			

Рис. 4. Модель возможностей различных классов нарушителей по реализации УБИ (фрагмент)

Перечень возможных способов реализации каждой УБИ $\{S_1 \ldots S_i\}$ формируется из данных, полученных с сайта ФСТЭК, а также в ходе разработки такого перечня на объекте.

Каждый способ имеет свой сценарий (тактику) реализации (T_i) через существующие уязвимости.

Таким образом, представляется возможность составить вероятностную модель взаимных влияний УБИ, способов и сценариев их реализации. Фрагмент данной модели представлен на рис. 5.

Она представляет собой матрицу, у которой по горизонтали размещены наименование и описание УБИ, а по вертикали – уязвимости. Если угроза может быть реализована через одну или несколько уязвимостей, то в клетке на их пересечении указываются наименование и содержание способов ее реализации M_i, вероятность предпочтительности его выбора $P(M_i)$ и успешной реализации, а также сценарий (тактика) применения.

Вероятность выбора конкретного способа реализации УБИ будет зависеть от возможностей нарушителя, требуемых ресурсов, ценности защищаемых информационных ресурсов, инфраструктурных характеристик объекта, его системы защиты, а также имеющихся уязвимостей.

Определив в модели критерии актуальности УБИ, способы и сценарии их реализации, мы получим соответствующую матрицу.

Кластер ликвидации рисков угроз инцидентов формируется путем ввода характеристик эффективности мер защиты информации (МЗИ), определенных в [1, 2, 3, 4] и состоящих из технических и организационных мер по локализации способов реализации УБИ и (или) ликвидации уязвимостей. Технические меры (ТМ) реализуются различными средствами защиты информации (СЗИ), а организационные меры (ОМ) – инженерно-техническими средствами и режимными мероприятиями, проводимыми на основе организационно-руководящих документов (ОРД).

Наименование угроз безопасности информации	Угроза физического выведения из строя средств хранения,	Угроза форматирования носителей	Угроза «форсированного веб-браузинга»	Угроза хищения средств хранения, обработки и (или)
Описание угрозы безопасности информации	Реализация данной угрозы возможна при условии получения нарушителем физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации (клавиатура и т.п.)	Угроза заключается в возможности утраты хранящейся на форматируемом носителе информации, зачастую без возможности её восстановления, из-за преднамеренного или случайного выполнения процедуры форматирования носителя информации.	Угроза заключается в возможности получения нарушителем доступа к защищаемой информации, выполнения привилегированных операций или осуществления иных деструктивных воздействий на некорректно защищённые компоненты веб-приложений. Данная угроза обусловлена слабостями (или отсутствием) механизма проверки корректности вводимых данных на веб-серверах. Реализация данной угрозы возможна при условии успешной реализации «ручного ввода» в адресную строку веб-браузера определённых адресов веб-страниц и осуществления принудительного перехода по древу веб-сайта к страницам, ссылки на которые явно не указаны на веб-сайте	Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации
Интерфейсы				
внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными (взаимодействующими) системами или сетями (проводные, б/проводные, веб-интерфейсы, др.)				
внутренние сетевые интерфейсы, обеспечивающие взаимодействие (в том числе через промежуточные компоненты) с компонентами систем и сетей, имеющими				$У_1$ $У_3$ / S_2 S_3, S_5 / T_1 T_2, T_3
интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др.)	$У_1$ $У_3$ $У_7$ / S_2 S_3, S_5 S_1, S_4 / T_1 T_2, T_3 T_1, T_2	$У_1$ $У_3$ / S_2 S_3, S_5 / T_1 T_2, T_3	$У_2$ $У_3$ $У_1$ $У_1$ / S_2 S_1 S_1, S_4 S_2 / T_1 T_3, T_3, T_2 T_1	$У_1$ $У_3$ / S_2 S_3, S_3 / T_1 T_2, T_4

Рис. 5. Вероятностная модель взаимосвязей уязвимостей, УБИ, способов и сценариев их реализации (фрагмент)

Процесс формирования базы данных защитных мероприятий представлен на рис. 6 в виде модели. Она представляет собой матрицу, где по горизонтали представлены МЗИ в соответствии с ОРД ФСТЭК, а по вертикали – УБИ. В клетках на пересечении УБИ и противопоставленных им МЗИ указываются перечни реализующих их СЗИ и ОРД.

После актуализации УБИ в модели останутся только актуальные УБИ, способы и сценарии их реализации, а также необходимые для их закрытия СЗИ и ОРД.

Критерии защищенности определяются организационно-руководящими и методическими документами. Способы реализации МЗИ будут иметь вероятностную степень эффективности, зависящую от функционала характеристик ТМ, ОМ и функционала показателей способа

реализации УБИ, а также появления новых уязвимостей, УБИ, способов и сценариев их реализации.

Рис. 6. Модель формирования базы данных защитных мероприятий

Кластер формирования рисков инцидента моделируется с учетом вероятности нанесения ущерба конфиденциальности (К), целостности (Ц) и доступности (Д) защищаемым информационным ресурсам с определенной степенью вероятности. Для этого на основе матрицы формируется вероятностная модель зависимостей вида и степени ущерба от типа инцидента. В ней по горизонтали указываются параметры оценки ущерба по каждому виду информационного ресурса (К, Ц, Д) (рис. 7). По вертикали указываются наименование и содержание инцидента. На пересечении указывается вербальное описание ущерба и вероятность его нанесения в случае реализации инцидента.

Рис. 7. Вероятностная модель зависимостей вида и степени ущерба от типа инцидента

Кластер ликвидации последствий инцидента моделируется аналогично кластеру ликвидации рисков угроз реализации инцидентов с составлением соответствующей модели.

Данную модель целесообразно изобразить в виде байесовской сети, которая представляет совместное распределение вероятностей с использованием направленного ациклического графа, в котором каждое ребро является условной зависимостью, а каждый узел – отдельной случайной величиной, отражающей события информационной безопасности [23, 24, 25]. Это позволяет проводить обновление вероятностей отраженных в ней событий информационной безопасности всякий раз, когда становится доступной новая информация. Математической основой для этого является теорема Байеса, суть которой описывает следующая формула:

$$P(\mathrm{A}|\mathrm{B})\,P(\mathrm{B}) = P(\mathrm{B}|\mathrm{A})\,P(\mathrm{A}). \quad (1)$$

При корректно составленной модели и достоверной информации о событиях ИБ можно доказать, что заложенная в ней методика обеспечивает правильное вычисление обновленных вероятностей относительно аксиом классической вероятности.

Любой узел в различных кластерах сети может получать информацию, так как метод не различает логический вывод в направлении ребер или наоборот. Одновременный ввод информации в несколько узлов не повлияет на алгоритм.

В модели взаимные влияния деструктивных воздействий и МЗИ представлены в виде цепочек последовательных событий, сходимой и расходимой последовательностей событий.

События в последовательных цепочках могут быть однородные (деструктивные или защитные) и разнородные (деструктивные и защитные) (рис. 8).

Расчет совместного распределения вероятностей для последовательных как однородных, так и разнородных событий осуществляется по приведенным ниже формулам.

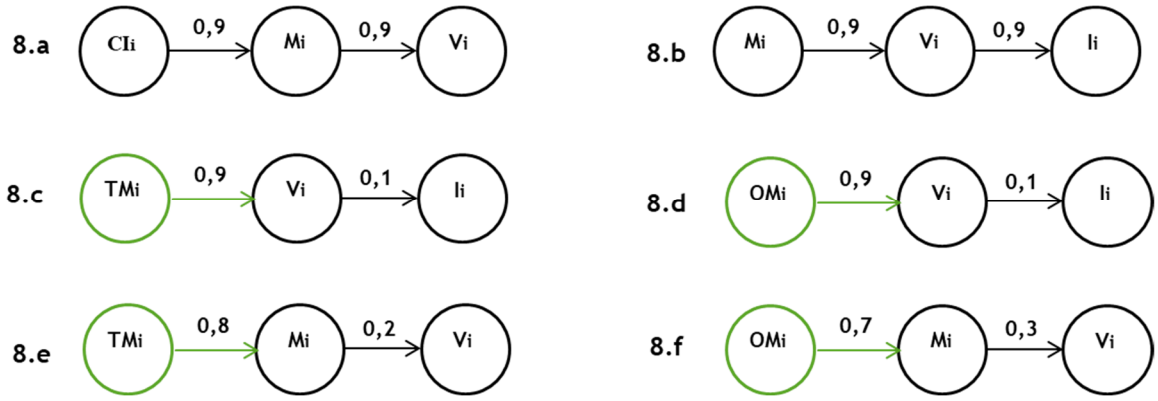

Рис. 8. Типы последовательных цепочек событий:
8 a, b – цепочки однородных (деструктивных) событий,
8 c, d, e, f – разнородные последовательности событий

Для варианта 8.a цепочки однородных (деструктивных) событий:

$$P(КлН_i, У_i \mid S_i) = \frac{P(КлН_i, S_i, У_i)}{P(S_i)} = \frac{P(КлН_i)(S_i|КлН_i)P(У_i|S_i)}{P(S_i)} = P(КлН_i \mid S_i)P(У_i \mid S_i). \quad (2)$$

Здесь априорная вероятность того, что нарушитель $КлН_i$ сможет реализовать УБИ способом S_i будет зависеть от апостериорной вероятности наличия незакрытой для данного способа уязвимости $У_i$.

Для варианта 8.c цепочки разнородных событий:

$$P(ТМ_i, И_i \mid У_i) = \frac{P(ТМ_i, У_i, И_i)}{P(У_i)} = \frac{P(ТМ_i)(У_i|ТМ_i)P(И_i|У_i)}{P(У_i)} = P(ТМ_i \mid У_i)P(И_i \mid У_i). \quad (3)$$

Здесь априорная вероятность эффективности технических мер будет зависеть от апостериорной вероятности наличия незакрытой уязвимости.

Аналогичным образом составляются формулы и устанавливаются вероятностные зависимости событий ИБ для других типов цепочек последовательных событий.

В модели также выявлено взаимное влияние деструктивных воздействий и МЗИ в виде цепочек сходимых событий (рис. 9).

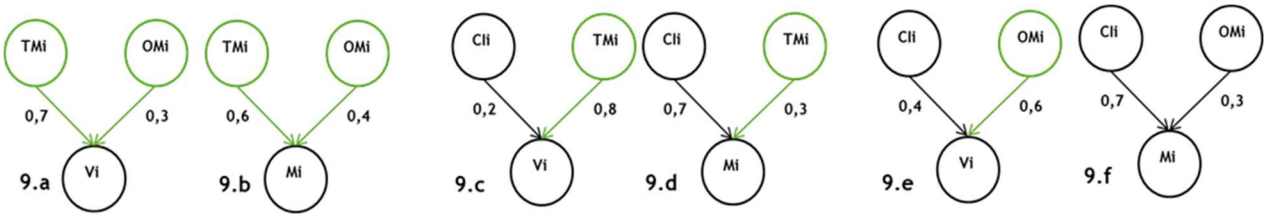

Рис. 9. Типы цепочек сходимых событий

Совместное распределение вероятностей для варианта 9.a сходимой последовательности событий ИБ рассчитывается по следующей формуле:

$$P(TM_i, OM_i, Y_i) = \sum_{y_i} P(TM_i)P(OM_i)P(Y_i \mid OM_i, TM_i) = P(OM_i \mid Y_i)P(TM_i \mid Y_i). \quad (4)$$

Для расходимых событий априорная вероятность существования уязвимости Y_i, будет зависеть от апостериорных вероятностей ее закрытия с помощью OM_i и TM_i.

Аналогичным образом составляются формулы и устанавливаются вероятностные зависимости событий ИБ для других типов цепочек расходимых событий.

Взаимное влияние деструктивных воздействий и МЗИ в виде цепочек расходимых событий представлено на рис. 10.

Рис. 10. Типы цепочек расходимых событий

Совместное распределение вероятностей для сходимой последовательности событий ИБ рассчитывается по следующей формуле:

$$P(S_i, Y_i \mid TM_i) = \frac{P(TM_i, S_i, Y_i)}{P(TM_i)} = P(S_i \mid TM_i)P(Y_i \mid TM_i). \quad (5)$$

Для расходимых событий априорная вероятность существования уязвимости Y_i и возможности реализации УБИ способом S_i будет зависеть от апостериорных вероятностей реализации OM_i и (или) TM_i.

Данный подход позволяет рассчитать зависимость априорной вероятности событий от вероятности событий, которые могут произойти, т.е. определить вероятностную зависимость деструктивных событий от защитных и наоборот.

Данная методика даёт возможность проведения универсальной оценки для событий информационной безопасности по количественным значениям подмножества переменных показателей МЗИ и деструктивного воздействия нарушителей, которая минимизирует вероятность ошибочного решения.

При принятии решения зачастую важна качественная оценка событий ИБ. Для перевода количественной оценки риска реализации инцидента ИБ в качественную применим нечетко-вероятностный метод [26].

Рассмотрим последовательность применения данного подхода для событий ИБ.

1. Зададим совместное распределение вероятностей событий ИБ $\{P(КлН_i,S_i,У_i)|P(ТМ_i,ОМ_i)\}$, где $P(ТМ_i,ОМ_i)$ – вероятная эффективность способа реализации МЗИ, $P(КлН_i,S_i,У_i)$ – вероятность риска реализации УБИ.

2. Проведем преобразование нечетких значений входных переменных $\{P(КлН_i,S_i,У_i)\}$ и $\{P(ТМ_i,ОМ_i)\}$ «Очень низкий (ОН)», «Низкий (Н)», «Средний (С)», «Высокий (В)», «Очень высокий (ОВ)» в числовые значения [27].

3. Зададим правила преобразования нечетких значений оценки риска реализации инцидента ИБ в числовые значения из диапазона [0, 1] в виде матрицы нечетких правил оценки риска реализации инцидента ИБ (табл. 1).

Соотношение количественных и качественных оценок риска реализации инцидента представлено в табл. 2.

Таблица 1. Матрица нечетких правил оценки риска реализации инцидента информационной безопасности

		Вероятная эффективность способа реализации МЗИ при локализации *i*-ой УБИ				
		ОН	**Н**	**С**	**В**	**ОВ**
Вероятность риска реализации УБИ при реализации *i*-го способа МЗИ	**ОН**	Н	Н	Н	ОН	ОН
	Н	Н	Н	Н	Н	ОН
	С	С	С	С	Н	Н
	В	ОВ	В	С	Н	Н
	ОВ	ОВ	ОВ	В	С	Н

Таблица 2. Соотношение количественных и качественных оценок риска реализации инцидента

Значения количественной оценки риска реализации инцидента	Значения качественной оценки риска реализации инцидента
$0 \le P(S_i У_i \mid И_i) \le 0.2$	Очень низкая
$0.2 \le P(S_i У_i \mid И_i) \le 0.4$	Низкая
$0.4 \le P(S_i У_i \mid И_i) \le 0.6$	Средняя
$0.6 \le P(S_i У_i \mid И_i) \le 0.8$	Высокая
$0.8 \le P(S_i У_i \mid И_i) \le 1$	Очень высокая

3. Заключение

Предлагаемая методика позволяет проводить универсальную оценку событий информационной безопасности по количественным значениям подмножества переменных показателей защитных мероприятий и деструктивного воздействия нарушителей, что сводит к минимуму вероятность ошибочного решения [28, 29].

Представленная в работе модель является масштабируемой, а это значит, что она обладает свойствами универсальности как с точки зрения критериальных требований, так и

вероятностных показателей. На её основе можно реализовать нейро-байесовский подход и получить систему поддержки принятия решений на основе искусственного интеллекта [30].

Литература

1. Приказ ФСТЭК России «Об утверждении требований к защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 12.02.2013 № 17 [Электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (дата обращения: 20.12.2021).
2. Приказ ФСТЭК России «Об утверждении состава и содержания организационных и технических мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013 № 21 [Электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения: 20.12.2021).
3. Приказ ФСТЭК России «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и окружающей среды» от 14.03.2014 № 31 [Электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (дата обращения: 20.12.2021).
4. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований к обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (с изменениями и дополнениями, 26 декабря 2019 г., № 60) [Электронный ресурс]. URL: https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (дата обращения: 20.12.2021).
5. Постановление Правительства Российской Федерации от 17.02.2018 № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры» [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/71783452 / (дата обращения: 20.12.2021).
6. Постановление Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категоризации объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» [Электронный ресурс ресурс]. URL: http://government.ru/docs/6339 / (дата обращения: 20.12.2021).
7. Постановление Правительства Российской Федерации от 01.10.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/72166260/ (дата обращения: 20.12.2021).
8. Методический документ. Утвержденная ФСТЭК России 5 февраля 2021 года «Методика оценки угроз информационной безопасности» [Электронный ресурс]. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021-g (дата обращения: 20.12.2021).
9. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России [Электронный ресурс]. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-

spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god (дата обращения: 20.12.2021).

10. *Джиарратано Д., Райли Г.* Экспертные системы: принципы разработки и программирования / изд. 4-е, перевод с англ. Изд. Уильямса. ISBN: 978-5-8459-1156-8, 2007. С. 115–201.
11. *Рассел С., Норвиг П.* Искусственный интеллект: современный подход / 2-е издание, перевод с англ. Изд. Уильямса, ISBN: 5-8459-0887-6, 2006. С. 345–428.
12. *Перл Д.* Байесовские сети. М.: Лаборатория когнитивных систем Калифорнийского университета, Лос-Анджелес, 2000. 102 с.
13. *Джаксен Ф.* Байесовские сети и графики принятия решений. Изд. Шпрингер, 2001. С. 54–120.
14. *Литвиненко Н. Г., Литвиненко А. Г., Мамырбаев О. Ж., Шаяхметова А. С.* Агенариск. Работа с байесовскими сетями. Алматы: Институт информационных и вычислительных технологий, 2019. 233 с.
15. *Конради С., Джуфф Л.* Байесовские сети и байесовская лаборатория. Практическое введение для исследователей.
16. Руководство пользователя BAYESIALAB. URL: https://library.bayesia.com/display/BlabC/BayesiAlab+Руководство пользователя+.
17. *Конради С., Джуфф Л.* Введение в байесовские сети и байесовскую лабораторию. URL: https://library.bayesia.com/download/attachments/10092794/BayesianNetworks Введение v16.pdf.
18. Расширенное моделирование с использованием AgenaRisk. URL: https://www.agenarisk.com.
19. Байесовская сетевая технология Agena. URL: https://www.agenarisk.com.
20. Начало работы с AgenaRisk. URL: https://www.agenarisk.com.
21. Эксперт Хугин. Построение байесовской сети. URL: https://www.hugin.com/wp-content/uploads/2016/05/Building-a-BN-Tutorial.pdf.
22. Эксперт Хугин. Технический документ. URL: http://download.hugin.com/webdocs/техническийдокумент/huginexpert-технический документ.pdf.
23. *Фентон Н., Нил М.* Оценка рисков и анализ решений с использованием байесовских сетей. ISBN 9781439809105.
24. *Басакер Р., Саати Т.* Конечные графы и сети. М.: Наука, 1974. С. 205–278.
25. *Свами М., Туласираман К.* Графики, сети и алгоритмы. М.: Мир, 1984. С. 55–146.
26. *Гавришев А. А.* Анализ программ моделирования нечетких систем // Дистанционное и виртуальное обучение. 2017. № 6. С. 76–83.
27. *Гавришев А. А.* Моделирование и количественный и качественный анализ широко распространенных систем защищенной связи // Прикладная информатика. 2018. Т. 13, № 5 (77). С. 84–122.
28. *Баранов В. В., Секретарев А. В., Игнатьева А. Р.* Автоматизация разработки методов защиты объектов информатизации // Материалы Всероссийской научно-практической конференции «Социотехнические и гуманитарные аспекты информационной безопасности», 2019. С. 21–30.
29. *Баранов В. В., Максимова Е. А., Лаута О. С.* Анализ модели информационной поддержки процессов и систем при реализации многоагентного интеллектуального взаимодействия // Устройства и системы. Управление, контроль, диагностика. 2019. № 4. С. 32–41.
30. *Баранов В. В., Максимова Е. А.* Прогнозирование разрушительных вредных воздействий на объекты критической информационной инфраструктуры // Коммуникации в компьютерных и информационных науках. 2021. 1395 CCIS. С. 88–99.

Статья поступила в редакцию 15.05.2022.

Баранов Владимир Витальевич
кандидат военных наук, доцент, заведующий кафедрой «Информационная безопасность» ФГБОУ ВО ЮРГПУ (НПИ) имени М. И. Платова (346428, Ростовская обл., Новочеркасск, ул. Просвещения, 132), e-mail: baranov.vv.2015@yandex.ru.

Models and methods for assessing the security of an informatization object

Baranov Vladimir
M.I. Platov South Russian State Polytechnic University, Novocherkassk, st. Troickaya 132, 346428, Russian Federation, baranov.vv.2015@yandex.ru.

The paper substantiates the need of creation an information decision support system in the development of systems for protecting informatization objects. Analyzes of existing systems in various fields of activity, the requirements for the functionality of the system in relation to the field of information protection, methods for developing models of functioning of protected information systems in a destructive environment impact on the basis of Bayesian networks are considered. The paper gives a description of a typical module functioning of this model. The structures of probabilistic models of the relationship of vulnerabilities, information security threats, methods and scenarios for their implementation, the formation of measures to protect informatization objects, the formation and assessment of the risks of incidents and their damage are considered. Clusters of typical information security events, methodological apparatus for calculating the joint distribution of the probabilities of protective and destructive events are determined. Finally, typical chains of interconnections of such events are identified. Mathematical apparatus for calculating their probabilities, a verbal description of the patterns of their mutual influence, and a method for converting quantitative probabilistic values of informatization object security indicators into qualitative ones are presented, and the results of the study are summarized.

Keywords: decision support; Bayesian network, destructive influences, information protection measures, information security threats, management strategy, information security events impact analysis, structural analysis, protection systems.

References

1. *Prikaz FSTEK Rossii "Ob utverzhdenii trebovanij k zashchite informacii, ne sostavlyayushchej gosudarstvennuyu tajnu, soderzhashchejsya v gosudarstvennyh informacionnyh sistemah" ot 12.02.2013 № 17* [Order of the FSTEC of Russia "On approval of requirements for the protection of information that does not constitute a state secret contained in state information systems" dated 12.02.2013 no. 17], available at: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (accessed 20.12.2021).
2. *Prikaz FSTEK Rossii "Ob utverzhdenii sostava i soderzhaniya organizacionnyh i tekhnicheskih meropriyatij po obespecheniyu bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh" ot 18.02.2013 № 21* [Order of the FSTEC of Russia "On approval of the composition and content of organizational and technical measures to ensure the security of personal data during their processing in personal data information systems" dated 02/18/2013 no. 21], available at: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (accessed 20.12.2021).
3. *Prikaz FSTEK Rossii "Ob utverzhdenii trebovanij k obespecheniyu zashchity informacii v avtomatizirovannyh sistemah upravleniya proizvodstvennymi i tekhnologicheskimi processami na kriticheski vazhnyh ob"ektah, potencial'no opasnyh ob"ektah, a takzhe ob"ektah, predstavlyayushchih povyshennuyu opasnost' dlya zhizni i zdorov'ya lyudej i okruzhayushchej sredy" ot 14.03.2014 № 31* [Order of the FSTEC of Russia "On approval of requirements for ensuring the protection of information in automated control systems for production and technological processes at critical facilities, potentially dangerous facilities, as well as facilities that pose an increased danger to human life and health and to the environment" dated 14.03.2014 no. 31], available at: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (accessed 20.12.2021).

4. *Prikaz FSTEK Rossii ot 25.12.2017 № 239 "Ob utverzhdenii trebovanij k obespecheniyu bezopasnosti znachimyh ob"ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii"* [Order of the FSTEC of Russia dated 25.12.2017 no. 239 "On Approval of requirements for ensuring the security of Significant Objects of Critical Information Infrastructure of the Russian Federation], available at: https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (accessed 20.12.2021).
5. *Postanovlenie Pravitel'stva Rossijskoj Federacii ot 17.02.2018 № 162 "Ob utverzhdenii Pravil osushchestvleniya gosudarstvennogo kontrolya v oblasti obespecheniya bezopasnosti znachimyh ob"ektov kriticheskoj informacionnoj infrastruktury"* [Resolution of the Government of the Russian Federation dated 17.02.2018 no. 162 "On approval of the Rules for the implementation of state control in the field of ensuring the security of significant objects of critical information infrastructure"], available at: https://www.garant.ru/products/ipo/prime/doc/ 71783452/ (accessed 20.12.2021).
6. *Postanovlenie Pravitel'stva Rossijskoj Federacii ot 08.02.2018 № 127 "Ob utverzhdenii Pravil kategorizacii ob"ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii, a takzhe perechnya pokazatelej kriteriev znachimosti ob"ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii i ih znachenij"* [Decree of the Government of the Russian Federation no. 127 dated 08.02.2018 "On approval of the Rules for categorizing objects of critical information infrastructure of the Russian Federation, as well as a list of indicators of criteria for the significance of objects of critical information infrastructure of the Russian Federation and their values"], available at: http://government.ru/docs/6339/ (accessed 20.12.2021).
7. *Postanovlenie Pravitel'stva Rossijskoj Federacii ot 01.10.2012 № 1119 "Ob utverzhdenii trebovanij k zashchite personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh"* [Decree of the Government of the Russian Federation no. 1119 of 01.10.2012 "On approval of requirements for the protection of personal data during their processing in personal data information systems"], available at: https://www.garant.ru/products/ipo/prime/doc/72166260/ (accessed 20.12.2021).
8. *Metodicheskij dokument. Utverzhdennaya FSTEK Rossii 5 fevralya 2021 goda "Metodika ocenki ugroz informacionnoj bezopasnosti"* [Methodological document. Approved by the FSTEC of Russia on February 5, 2021, "Methodology for assessing threats to information security"], available at: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021-g (accessed 20.12.2021).
9. *Bazovaya model' ugroz bezopasnosti 2008 "Bazovaya model' ugroz bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh. FSTEK Rossii"* [Basic model of security threats 2008 "Basic model of threats to the security of personal data during their processing in personal data information systems. FSTEC of Russia"], available at: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god (accessed 20.12.2021).
10. Giarratano D., Riley G. *Ekspertnye sistemy: principy razrabotki i programmirovaniya.* [Expert systems: principles of development and programming]. 4 nd edition, translated from English, Williams Publishing House, ISBN: 978-5-8459-1156-8, 2007, pp. 115-201.
11. Russell S., Norvig P. *Iskusstvennyj intellekt: sovremennyj podhod.* [Artificial Intelligence: a Modern approach]. 2 nd edition, translated from English, Williams Publishing House, ISBN: 5-8459-0887-6, 2006, pp. 345-428.
12. Pearl D. *Laboratoriya kognitivnyh sistem Kalifornijskogo universiteta, Los Angeles. Bajesovskie seti.* [Laboratory of Cognitive Systems of the University of California, Los Angeles. Bayesian networks]. Moscow, Mir, 2000, 102 p.
13. Jaxen F. *Bajesovskie seti i grafiki prinyatiya reshenij.* [Bayesian networks and decision graphs]. M, Springer, 2001, pp. 54-120.
14. Litvinenko N.G., Litvinenko A.G., Mamyrbayev O.J., Shayakhmetova A.S. *Agenarisk. Rabota s bajesovskimi setyami* [Agenarisk. Work with bayesian networks]. Almaty: Institut informacionnyh i vychislitel'nyh tekhnologij, 2019, 233 p.
15. Konradi S., Juff L. *Bajesovskie seti i Bajesovskaya laboratoriya, Prakticheskoe vvedenie dlya issledovatelej* [Bayesian networks and the Bayesian Laboratory, A practical introduction for researchers], available at: https://www.researchgate.net / publication/282362899 (accessed 20.12.2021).
16. BAYESIALAB User's Guide, available at: https://library.bayesia.com (accessed 20.12.2021).

17. Konradi S., Juff L. Introduction to Bayesian Networks and the Bayesian Laboratory, available at: https://library.bayesia.com/download/attachments/10092794/BayesianNetworks Introduction v16.pdf (accessed 20.12.2021).
18. Advanced modeling using AgenaRisk, available at: https://www.agenarisk.com (accessed 20.12.2021).
19. Agena Bayesian network technology, available at: https://www.agenarisk.com (accessed 20.12.2021).
20. Getting started with AgenaRisk, available at: https://www.agenarisk.com (accessed 20.12.2021).
21. Expert Hugin, Building a Bayesian network, available at: https://www.hugin.com/wp-content/uploads/2016/05/Building-a-BN-Tutorial.pdf (accessed 20.12.2021).
22. Expert Hugin, Technical Technical Document, available at: http://download.hugin.com / webdocs/technical document/huginexpert-technical document.pdf (accessed 20.12.2021).
23. Fenton N., Neil M. Risk assessment and decision analysis using Bayesian networks. *Queen Mary, University of London and Agena Ltd. CRC press*. ISBN: 9781439809105, ISBN 10: 1439809100.
24. Basaker R., Saati T. *Konechnye grafy i seti* [Finite graphs and networks]. Moscow, Nauka, 1974, pp. 205-278.
25. Swami M., Thulasiraman K. *Grafiki, seti i algoritmy* [Graphs, networks and algorithms]. Moscow, Mir, 1984, pp. 55-146.
26. Gavrishev A.A. *Analiz programm modelirovaniya nechetkih sistem.* [Analysis of fuzzy systems modeling programs]. *Distancionnoe i virtual'noe obuchenie*], 2017, no. 6, pp. 76-83.
27. Gavrishev A.A. Modelirovanie i kolichestvennyj i kachestvennyj analiz shiroko rasprostranennyh sistem zashchishchennoj svyazi. [Modeling and quantitative and qualitative analysis of widespread secure communication systems]. *Prikladnaya informatika*, 2018, vol. 13, no 5 (77), pp. 84-122.
28. Baranov V.V., Sekretarev A.V., Ignatieva A.R. Avtomatizaciya razrabotki metodov zashchity ob"ektov informatizacii [Automation of development of methods of protection of informatization objects]. *Vserossijskaya nauchno-prakticheskaya konferenciya. Sociotekhnicheskie i gumanitarnye aspekty informacionnoj bezopasnosti*, Pyatigorsk, Pyatigorskij gosudarstvennyj universitet, 10-13, April, 2019, pp. 21-30.
29. Baranov V.V., Maksimova E.A., Lauta O.S. Analiz modeli informacionnoj podderzhki processov i sistem pri realizacii mnogoagentnogo intellektual'nogo vzaimodejstviya [Analysis of the model of information support of processes and systems in the implementation of multi-agent intellectual interaction]. *Ustrojstva i sistemy. Upravlenie, kontrol', diagnostika,* 2019, no. 4, pp. 32-41.
30. Baranov V.V., Maksimova E.A. Prognozirovanie razrushitel'nyh vrednyh vozdejstvij na ob"ekty kriticheskoj informacionnoj infrastruktury [Forecasting destructive harmful effects on objects of critical information infrastructure]. *Kommunikacii v komp'yuternyh i informacionnyh naukah*, 2021, 1395 CCIS, pp. 88-99.

УДК 681.883.48
DOI: 10.55648/1998-6920-2022-16-3-29-37

Технология полигонных испытаний навигационных средств автономного необитаемого подводного аппарата[1]

В. Г. Арсентьев, Г. И. Криволапов

Предложена модифицированная технология натурных испытаний автономных необитаемых подводных аппаратов для проверки точности их навигационных средств и отработки различных траекторий подводного передвижения.

Ключевые слова: автономный необитаемый подводный аппарат, безэкипажное надводное судно, испытательный полигон, скоординированное движение, постобработка данных испытаний.

1. Введение

В настоящее время точность навигационных средств и состав навигационного оборудования автономных необитаемых подводных аппаратов (АНПА) обеспечиваются комплексированием данных счисления бортовой навигационной системы, включающей измеритель абсолютной скорости и инерциальную систему, с текущей коррекцией счисленных данных от внешних навигационных систем. Для коррекции используются спутниковые навигационные системы (СНС) на поверхности и гидроакустические – в подводном положении. Последние отличаются конфигурацией гидроакустического оборудования, реализованного в виде опорных маяков с известными или контролируемыми геодезическими координатами.

При проектировании, изготовлении и отладке АНПА решаются задачи оценки точности как отдельных элементов навигационных систем, так и навигационных комплексов в целом. Необходимые для этого работы невозможно выполнить в полном объёме в лабораторных условиях, поэтому их значительная часть соотносится с натурными испытаниями на специально оборудованных морских полигонах.

Известен специализированный полигон Института проблем морских технологий ДВО РАН [1], оборудованный в мелководной бухте, координаты ключевых точек которого определены геодезическими методами. В этих ключевых точках размещены три маяка-ответчика и две управляющие антенны, которые являются абонентами гидроакустической навигационной системы (ГНС) с длинной базой. В ходе испытаний эти устройства реализуют функции постоянно действующих стационарных измерительных дальномерных трасс в акватории движения подводного аппарата, выполняющего проверку своих навигационных средств.

Накопление измеряемых дальномерных данных по трём трассам (антенна – маяки) с оценкой эффективных скоростей распространения сигналов по различным направлениям в акватории позволяет дать достаточно точную оценку координат объекта навигации. При точной координатной привязке ключевых точек в условиях такого полигона можно выполнить оценку точности всего бортового навигационного комплекса АНПА.

[1] Работа выполнена в рамках государственного задания № 071-03-2022-001.

Для коррекции счисленных координат АНПА используются данные от СНС и ГНС с длинной базой. Скорость звука на АНПА определяется в режиме реального времени измерителем параметров среды.

Запуск АНПА осуществляется на испытательном полигоне в условиях глубин от 6 до 20 метров. Программная траектория представляет собой циклическое движение по квадрату со стороной 300 метров с двухмерной координатной привязкой. Средняя скорость передвижения АНПА составляет порядка одного метра в секунду. Коррекция счисленных координат при движении осуществляется на АНПА по данным ГНС с периодом около 30 секунд. Оценка точности навигации выполняется после подъёма АНПА на поверхность в ходе постобработки полученных траекторных данных, которая включает в себя две процедуры: обработку данных счисления пути навигационной системы АНПА для определения траектории его передвижения в процессе испытаний и оценку её отклонений от запрограммированной траектории, характеризующих точность проверяемых навигационных средств.

К недостаткам описанной трёхмаяковой технологии полигонной проверки навигационных средств АНПА следует отнести:

1) необходимость выполнения трудоёмких и продолжительных по времени работ, связанных с установкой и привязкой к геодезическим координатам акватории испытательного полигона местоположения подводных маяков-ответчиков и антенн ГНС с длинной базой перед соответствующим временным циклом испытаний АНПА;

2) достаточно большое время коррекции счисленных координат АНПА по данным ГНС во время движения, что ограничивает скорость и характер траекторий передвижения АНПА в акватории испытательного полигона во время испытаний;

3) отсутствие возможности оперативного визуального контроля с берегового поста или иного места наблюдения подводных перемещений АНПА, транспонированных на поверхность акватории испытательного полигона, в процессе проверки и отработки возможных траекторий его передвижения с использованием бортовых навигационных средств;

4) значительные затраты времени на постобработку полученных в процессе испытаний траекторных данных, снижающие оперативность используемой технологии.

Более перспективной в плане полигонных испытаний является одномаяковая [2] технология навигации АНПА, называемая ещё технологией синтезированной длинной базы. Суть технологии заключается в измерении на последовательных интервалах времени наклонного расстояния между мобильным надводным маяком и движущимся в подводном положении АНПА и использовании его для коррекции счисления местоположения АНПА по курсу и скорости, периодически измеряемых бортовыми средствами АНПА.

Технология имеет ряд разновидностей использования. Применительно к полигонным испытаниям она состоит в том, что АНПА сопровождает безэкипажное надводное судно (БНС), например, мини катер или глайдер, который периодически определяет своё местоположение в акватории с использованием СНС и передаёт свои текущие координаты на АНПА. Во время гидроакустического модемного обмена сигналами определяется время распространения сигнала от БНС до АНПА. На АНПА по времени распространения акустического сигнала между БНС и АНПА и предварительно измеренной скорости звука в акватории испытательного полигона рассчитывается наклонное расстояние между БНС и АНПА, затем с учётом измеренной глубины погружения АНПА вычисляется горизонтальное расстояние между БНС и АНПА, которое совместно с курсом, скоростью АНПА и переданными геодезическими координатами БНС используется для коррекции пути АНПА в акватории испытательного полигона. Оценка точности навигации выполняется также после подъёма АНПА на поверхность в ходе постобработки полученных траекторных данных.

Технология одномаяковой полигонной навигации лишена первого, весьма существенного, недостатка трёхмаяковой навигации, второй недостаток которой может быть устранён уменьшением интервала времени между измерениями геодезических координат БНС с использованием СНС, но остаются третий и четвёртый функционально значимые недостатки технологии, снижающие её технико-эксплуатационную эффективность.

Предлагаемая модифицированная технология позволяет расширить функциональные возможности одномаяковой технологии, обеспечивая визуальный контроль подводных перемещений АНПА при проверке траекторных возможностей подводного передвижения, и повысить её эффективность, сокращая время постобработки траекторных данных при проверке точности навигационных средств, позволяя причислить её к категории среднезатратных технологий натурных испытаний автономных подводных аппаратов.

2. Базовые процессы модифицированной технологии

АНПА с автономными средствами управления и движительным комплексом, гидроакустическим модемом и бортовыми средствами навигации, включающими в себя инерциальную навигационную систему, гидроакустический доплеровский лаг, датчик глубины дополнительно оснащается гидроакустическим маяком-пингером, а на БНС с автономной системой управления и движителем, приёмником сигналов СНС и гидроакустическим модемом дополнительно устанавливаются съёмное устройство хранения данных, инерциальная навигационная система и гидроакустический фазовый пеленгатор с четырёхэлементной антенной диаметрально-ортогональной геометрии. Возможное размещение антенн средств навигации и информационного обмена АНПА и БНС иллюстрируется рис. 1.

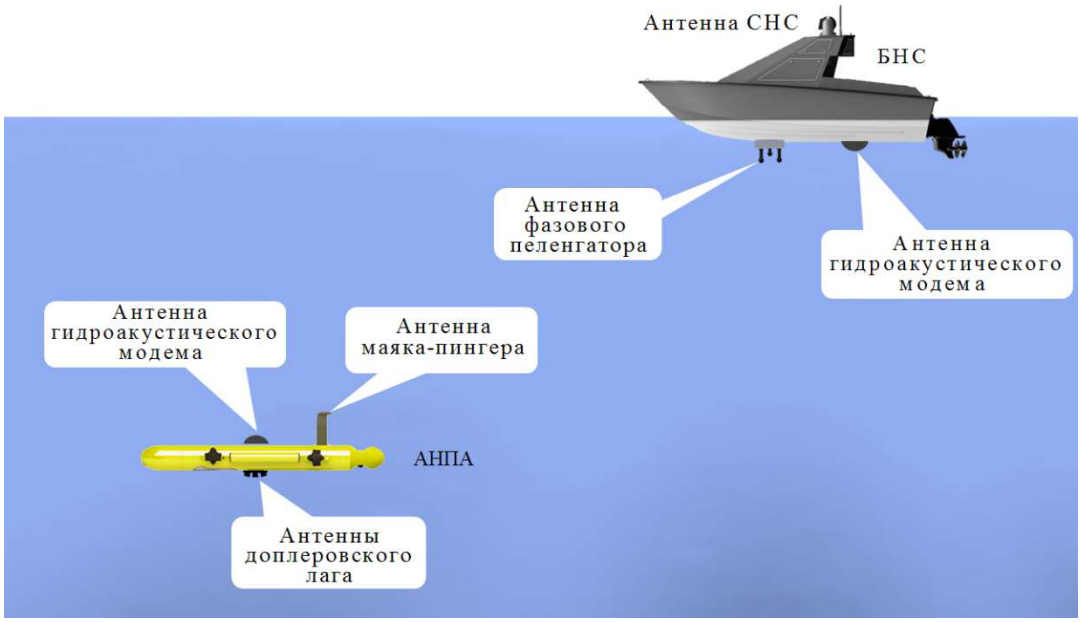

Рис. 1. Размещение антенн средств навигации и информационного обмена АНПА и БНС

С помощью вышеуказанных средств управления движением, навигации и информационного обмена осуществляется скоординированное передвижение АНПА (в подводном положении) и БНС (в надводном положении) по двухмерной траектории между двумя реперными точками акватории испытательного полигона с известными геодезическими координатами предварительно запрограммированного в АНПА маршрута (рис. 2).

Навигация АНПА и скоординированное передвижение АНПА и БНС в акватории испытательного полигона реализуются следующим образом.

На АНПА посредством инерциальной навигационной системы, гидроакустического доплеровского лага и датчика глубины периодически оцениваются навигационные параметры движения АНПА – курс, курсовая и бортовая скорости, являющиеся ортогональными составляющими путевой скорости, и глубина погружения, которые используются для счисления его

пути по запрограммированному маршруту акватории испытательного полигона и передаются с помощью гидроакустического модема на БНС.

На БНС посредством гидроакустического фазового пеленгатора с четырёхэлементной антенной диаметрально-ортогональной геометрии периодически осуществляется позиционирование АНПА относительно БНС, в процессе которого оцениваются пеленг, угол места АНПА, горизонтальное расстояние по курсу между БНС и АНПА в системе координат его пеленгационной антенны.

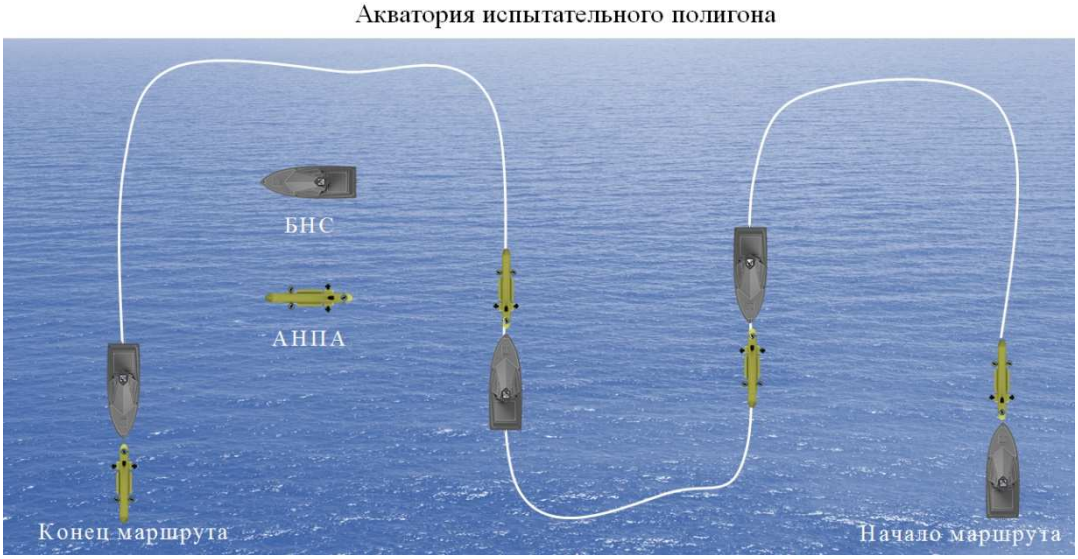

Рис. 2. Скоординированное передвижение АНПА и БНС в акватории полигона

Для гидроакустического позиционирования выбирается алгоритм [3, 4], позволяющий оценивать угловые координаты позиционируемого объекта с погрешностью менее одного градуса. Для антенны диаметрально-ортогональной геометрии [5] с соотношением размеров 2:1 (расстояние между парами приёмных гидрофонов в горизонтальной плоскости в два раза превышает расстояние между парами гидрофонов в вертикальной плоскости) в согласованной с курсом БНС системе координат (рис. 3) текущие пеленг $\varphi(t)$ и угол места $\theta(t)$ АНПА определяются по следующим тригонометрическим формулам:

$$\varphi(t)=\begin{cases}\arccos\left(\dfrac{-\Delta\psi_{12}(t)}{\sqrt{\Delta\psi_{12}^2(t)+\left[\Delta\psi_{13}(t)-\Delta\psi_{14}(t)\right]^2}}\right), & \text{если } \Delta\psi_{13}(t)-\Delta\psi_{14}(t)\ge 0\\ \pi+\arccos\left(\dfrac{\Delta\psi_{12}(t)}{\sqrt{\Delta\psi_{12}^2(t)+\left[\Delta\psi_{13}(t)-\Delta\psi_{14}(t)\right]^2}}\right), & \text{если } \Delta\psi_{13}(t)-\Delta\psi_{14}(t)<0\end{cases};\quad [0\le\varphi<2\pi]; \tag{1}$$

$$\theta(t)=\arccos\left(\frac{\Delta\psi_{12}(t)-\Delta\psi_{13}(t)-\Delta\psi_{14}(t)}{\sqrt{\Delta\psi_{12}^2(t)+\left[\Delta\psi_{13}(t)-\Delta\psi_{14}(t)\right]^2+\left[\Delta\psi_{12}(t)-\Delta\psi_{13}(t)-\Delta\psi_{14}(t)\right]^2}}\right)-\frac{\pi}{2};\quad \left[0\le\theta\le\frac{\pi}{2}\right], \tag{2}$$

где $\Delta\psi_{12}(t)$, $\Delta\psi_{13}(t)$, $\Delta\psi_{14}(t)$ являются текущими инструментально измеренными разностями фаз колебаний навигационного сигнала маяка-пингера АНПА для соответствующих пар

парциальных трактов приёма фазового пеленгатора БНС. Как видно из соотношений (1) и (2), для оценки угловых координат АНПА не требуется знание скорости звука в акватории испытательного полигона, что позволяет исключить погрешность измерения скорости звука при оценке пеленга и угла места АНПА, повышая точность позиционирования.

По рассчитанному углу места $\theta(t)$ и переданной с АНПА на БНС текущей глубине погружения $h_1(t)$ АНПА оценивается текущее горизонтальное расстояние $D(t)$ между БНС и АНПА:

$$D(t) = \frac{[h_1(t) - h_2]}{\mathrm{tg}\,\theta(t)}, \tag{3}$$

где h_2 – априорно известная глубина погружения антенны фазового пеленгатора БНС.

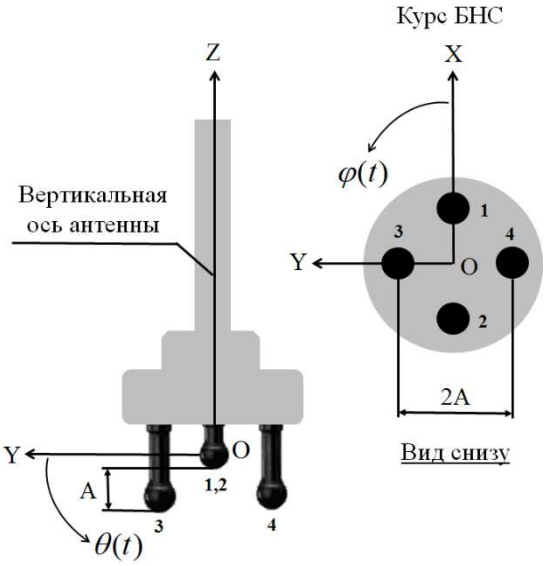

Рис. 3. Система координат антенны фазового пеленгатора БНС

Периодичность гидроакустического позиционирования АНПА относительно БНС согласовывается с периодичностью излучения навигационного сигнала маяка-пингера АНПА и периодичностью передачи с АНПА на БНС сообщений о курсе $k(t)$, курсовой $v_x(t)$ и бортовой $v_y(t)$ скоростях, являющихся ортогональными составляющими путевой скорости АНПА $v(t) = \sqrt{v_x^2(t) + v_y^2(t)}$, глубине погружения $h_1(t)$.

На БНС, используя СНС, периодически выполняется геодезическое позиционирование БНС в акватории испытательного полигона с оценкой геодезических координат, которые посредством гидроакустического модема передаются на АНПА, а с помощью инерциальной навигационной системы оцениваются курс $K(t)$, курсовая $V_x(t)$ и бортовая $V_y(t)$ скорости, являющиеся ортогональными составляющими путевой скорости БНС $V(t) = \sqrt{V_x^2(t) + V_y^2(t)}$.

С помощью автономной системы управления движением БНС совмещаются курсы $k(t) = K(t)$, $\varphi(t) = 0$ и выравниваются путевые скорости БНС и АНПА $v(t) = V(t)$ на основе сопоставления курсовых $k(t)$ и $K(t)$, скоростных $v(t)$ и $V(t)$ и траекторных параметров $\varphi(t)$ и $D(t)$ их передвижения (рис. 4) в акватории испытательного полигона.

Скоординированное движение АНПА и БНС описывается системой из пяти интегральных уравнений, используемых в итеративном алгоритме автономной системы управления движением БНС:

$$\begin{cases} \int_0^T V_x(t)dt - \int_0^T v_x(t)dt = 0\ ; \int_0^T V_y(t)dt - \int_0^T v_y(t)dt = 0\ ; \\ \int_0^T K(t)dt - \int_0^T k(t)dt = 0\ ; \int_0^T \dfrac{h_1(t)-h_2}{\operatorname{tg}\theta(t)}dt - D_0 = 0\ ; \\ \int_0^T \varphi(t)dt = 0\ . \end{cases} \quad (4)$$

Здесь T – время усреднения курсовых, скоростных и траекторных параметров движения АНПА и БНС; D_0 – установочное минимально допустимое горизонтальное расстояние между АНПА и БНС, которое выбирается с учётом мест размещения антенн маяка-пингера АНПА и фазового пеленгатора БНС и поддерживается постоянным $D_0 = D(t)$ в процессе скоординированного передвижения АНПА и БНС в акватории испытательного полигона.

В процессе скоординированного движения АНПА и БНС по запрограммированному маршруту с БНС на АНПА посредством гидроакустического модема с периодичностью геодезического позиционирования БНС передаются сообщения о горизонтальном расстоянии $D(t)$ по курсу между БНС и АНПА, которое совместно с переданными геодезическими координатами БНС, ортогональными составляющими путевой скорости $v(t)$ и курсом $k(t)$ АНПА используются для коррекции счисления его пути в акватории испытательного полигона.

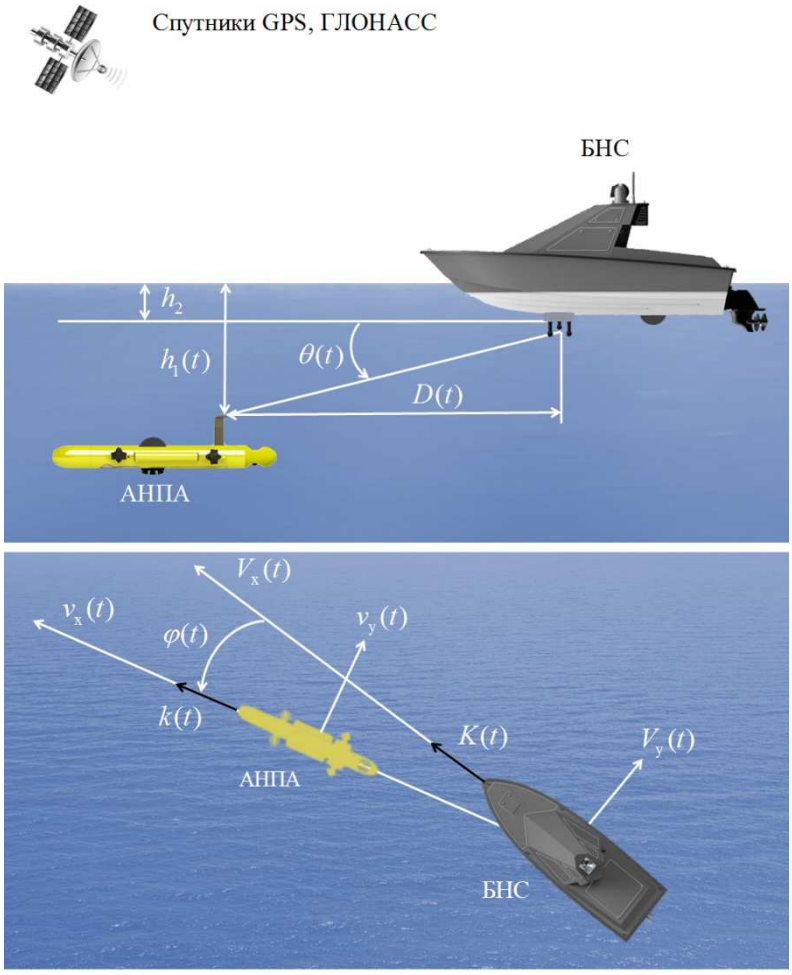

Рис. 4. Измеряемые параметры скоординированного передвижения АНПА и БНС

Периодичность геодезического позиционирования БНС выбирается кратно превышающей периодичность гидроакустического позиционирования АНПА с целью обеспечения завершения процессов итеративного корректирования движения БНС по результатам гидроакустического позиционирования АНПА и совмещения по времени оценок геодезических координат БНС и глубины погружения АНПА, которые записываются с периодичностью геодезического позиционирования в съёмное устройство хранения данных БНС в процессе скоординированного передвижения АНПА и БНС в акватории испытательного полигона.

После прибытия АНПА в конечную реперную точку запрограммированного маршрута по данным скоординированного движения АНПА и БНС, записанным в съёмное устройство хранения данных БНС, выстраивается трёхмерная или двухмерная (рис. 5) траектория движения АНПА в акватории испытательного полигона, при этом не требуются подъём АНПА на поверхность и процедура обработки данных счисления пути навигационной системы подводного аппарата, что значительно сокращает время постобработки траекторных данных.

Полученная таким образом траектория движения АНПА сравнивается с исходной запрограммированной, и по их расхождению оценивается точность навигационных средств АНПА при движении в акватории испытательного полигона.

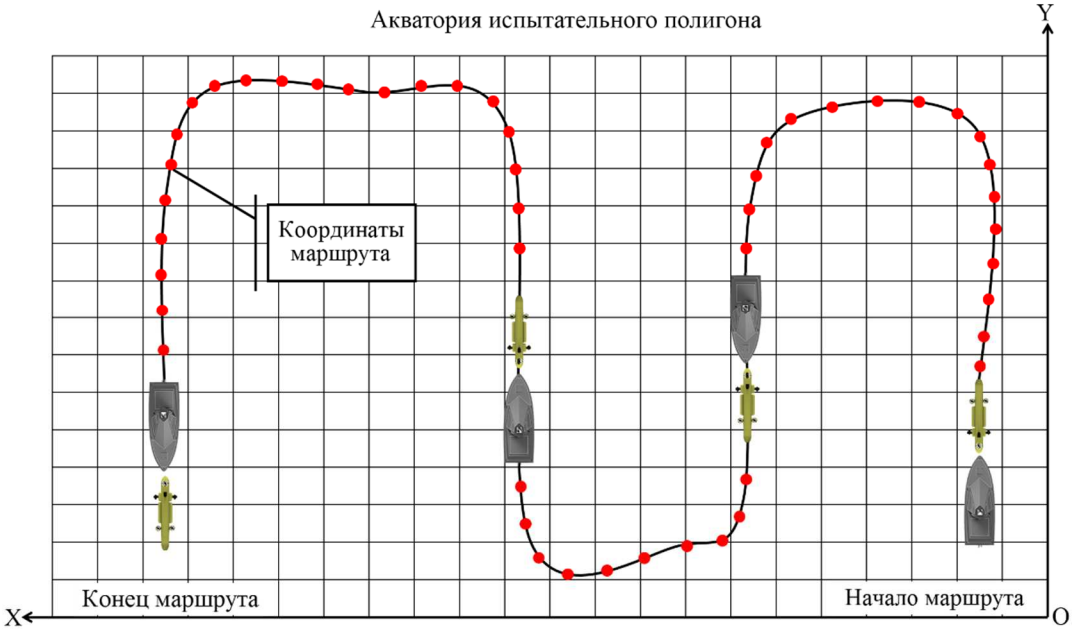

Рис. 5. Результат двухмерной обработки траектории передвижения АНПА

В ходе полигонных испытаний по предлагаемой технологии появляется возможность оперативного визуального контроля с берегового поста или иного места наблюдения подводных перемещений АНПА, транспонированных на поверхность акватории испытательного полигона в виде двухмерной траектории передвижения БНС, используемого в качестве поверхностного индикатора подводного перемещения АНПА, что облегчает процесс проверки и отработки возможных траекторий его передвижения.

3. Заключение

Технико-эксплуатационным результатом предлагаемой модифицированной технологии, обладающей расширенными функциональными возможностями и повышенной эффективностью, является обеспечение оперативного визуального контроля с берегового поста или иного места наблюдения подводных перемещений АНПА по двухмерной траектории, транспонированной на поверхность акватории испытательного полигона, в процессе проверки и отработки

возможных траекторий его передвижения и сокращение времени постобработки траекторных данных испытаний за счёт реализации скоординированного движения БНС и АНПА по запрограммированному маршруту акватории испытательного полигона, основанного на сочетании процессов их геодезического и гидроакустического позиционирования, с записью на БНС в режиме реального времени текущих геодезических координат БНС в акватории испытательного полигона и глубины погружения подводного аппарата на маршруте передвижения. Существенными отличиями технологии являются: использование БНС в качестве поверхностного индикатора подводного перемещения АНПА, отсутствие необходимости измерения скорости звука в акватории испытательного полигона для осуществления навигации АНПА и исключение из постобработки траекторных данных испытаний процедуры определения траектории передвижения АНПА в акватории испытательного полигона, требующей обработки данных счисления его пути и подъёма АНПА на поверхность.

Литература

1. *Ваулин Ю. В., Лаптев К. З.* Оценка точности плавания автономного необитаемого подводного аппарата в заданном районе // Известия ЮФУ. Технические науки. 2015. С. 74–86.
2. *Машошин А. И.* Исследование точности одномаяковой навигации автономных необитаемых подводных аппаратов // Подводные исследования и робототехника. 2017. № 2. С. 20–27.
3. *Арсентьев В. Г., Криволапов Г. И.* Позиционирование объектов в гидроакустической навигационной системе с ультракороткой базой // Вестник СибГУТИ. 2018. № 4. С. 66–75.
4. Патент РФ 2709100, МПК G01S 1/72. Способ определения местоположения подводного объекта / В. Г. Арсентьев, Г. И. Криволапов, А. Е. Малашенко, Д. Д. Минаев. Заявка 2018122532, заявлено 19.06.2018, опубликовано 16.12.2019. Бюл. № 35.
5. *Арсентьев В. Г., Криволапов Г. И.* О влиянии геометрических параметров антенны на характеристики гидроакустического фазового пеленгатора // Вестник СибГУТИ. 2019. № 1. С. 92–101.

Статья поступила в редакцию 26.04.2022.

Арсентьев Виктор Георгиевич

к.т.н., ведущий научный сотрудник научно-технического центра специализированных информационных систем СибГУТИ (630008, Новосибирск, ул. Бориса Богаткова, 51) тел. (383) 2-693-938, e-mail: viktor.arsentev.51@mail.ru.

Криволапов Геннадий Илларионович

к.т.н., доцент, заведующий лабораторией, руководитель научно-технического центра специализированных информационных систем СибГУТИ (630008, Новосибирск, ул. Бориса Богаткова, 51) тел. (383) 2-693-942, e-mail: krivolapov@sibsutis.ru

Field testing technology of an autonomous uninhabited underwater vehicle navigation aids

Viktor G. Arsent'ev
Candidate of technical sciences, Leading researcher, Siberian State University of Telecommunications and Information Science (SibSUTIS, Novosibirsk, Russia), viktor.arsentev.51@mail.ru.

Gennagy I. Krivolapov
Candidate of technical sciences, Head of laboratory, Siberian State University of Telecommunications and Information Science (SibSUTIS, Novosibirsk, Russia), krivolapov@sibsutis.ru.

The modified technology of full-scale tests of autonomous uninhabited underwater vehicles for checking the accuracy of their navigation aids and various trajectories development of underwater movement is proposed.

Keywords: autonomous uninhabited underwater vehicle, unmanned surface vessel, test site, coordinated movement, post-processing of test data.

References

1. Vaulin YU.V., Laptev K.Z. Ocenka tochnosti plavaniya avtonomnogo neobitaemogo podvodnogo apparata v zadannom rajone [Assessment of the accuracy of navigation of an autonomous uninhabited underwater vehicle in a given area]. *Izvestiya YUFU. Tekhnicheskie nauki,* 2015, pp. 74-86.
2. Mashoshin A.I. Issledovanie tochnosti odnomayakovoj navigacii avtonomnyh neobitaemyh podvodnyh apparatov [Investigation of the accuracy of single-beacon navigation of autonomous uninhabited underwater vehicles]. *Podvodnye issledovaniya i robototekhnika,* 2017, no. 2, pp. 20-27.
3. Arsent'ev V. G., Krivolapov G. I. Pozicionirovanie ob"ektov v gidroakusticheskoj navigacionnoj sisteme s ul'trakorotkoj bazoj [Positioning of objects in a hydroacoustic navigation system with an ultrashort base]. *Vestnik SibGUTI,* 2018, no. 4, pp. 66-75.
4. *Patent RF 2709100, MPK G01S 1/72. Sposob opredeleniya mestopolozheniya podvodnogo ob"ekta* [RF Patent. Method of determining the location of an underwater object]. V.G. Arsent'ev, G.I. Krivolapov, A.E. Malashenko, D.D. Minaev. *Zajavka 2018122532, zajavleno 19.06.2018, opublikovano 16.12.2019.*
5. Arsent'ev V. G., Krivolapov G. I. O vliyanii geometricheskih parametrov antenny na harakteristiki gidroakusticheskogo fazovogo pelengatora [On the influence of the geometrical parameters of the antenna on the characteristics of the hydroacoustic phase direction finder]. *Vestnik SibGUTI,* 2019, no. 1, pp. 92-101.

УДК 004.021
DOI: 10.55648/1998-6920-2022-16-3-38-47

Алгоритмы нерегулярных коллективных операций стандарта MPI для систем с разделяемой памятью

А. А. Романюта, М. Г. Курносов[1]

Предложены алгоритмы реализации коллективных операций MPI_Scatterv, MPI_Gatherv, MPI_Allgatherv для многопроцессорных SMP/NUMA-систем. Алгоритмы используют подход на основе копирования фрагментов сообщений через очереди в сегменте совместно используемой памяти (Copy-In-Copy-Out). Программная реализация выполнена на базе библитеки Open MPI и в среднем на 20–40 % обеспечивает меньшее время выполнения операций MPI_Scatterv, MPI_Gatherv, MPI_Allgatherv по сравнению с реализацией в компоненте coll/tuned библиотеки Open MPI.

Ключевые слова: Scatterv, Gatherv, Allgatherv, коллективные операции, MPI, вычислительные системы.

1. Введение

Современные высокопроизводительные вычислительные системы (ВС) строятся на базе многопроцессорных узлов с общей памятью. Как правило, каждый узел системы включает от одного до четырех процессоров общего назначения с архитектурой x86-64, POWER или ARM, а также группу сопроцессоров/ускорителей. Процессорные ядра одного узла могут передавать информацию через разделяемую память. Взаимодействие между узлами осуществляется через коммуникационную сеть (InfiniBand, 10X Gigabit Ethernet, Slingshot). Обмен информацией через разделяемую память узла, как правило, требует меньше времени. Поэтому двухуровневая иерархия коммуникационной среды активно эксплуатируется для оптимизации обменов информацией в системах параллельного программирования, распределенного машинного обучения и обработки больших массивов данных. Ключевая идея – выполнять обмены информацией между ядрами узла через разделяемую память и только для межузловых взаимодействий использовать коммуникационную сеть.

К наиболее ресурсоёмким коммуникационным операциям относятся коллективные обмены (глобальные, collective communication), в которых участвуют все или значительная часть процессов (процессорных ядер). По этой причине производители коммуникационного оборудования и библиотек уделяют значительное внимание созданию эффективных алгоритмов коллективных операций. В данной работе рассматриваются алгоритмы реализации коллективных операций стандарта MPI [1] `Scatterv`, `Gatherv`, `Allgatherv` через разделяемую память вычислительного узла. Интерес к указанным операциям обусловлен отсутствием эффективных алгоритмов их реализации в коммерческих и открытых библиотеках Open MPI [2], MPICH, MVAPICH. Ниже приведены прототипы операций:

[1] Работа выполнена в рамках государственного задания № 071-03-2022-001.

```
MPI_Scatterv(sbuf[p], scounts[p], displs[p], stype,
             rbuf, rcount, rtype, root)
MPI_Gatherv(sbuf, scount, stype, rbuf[p], rcounts[p], displs[p],
            rtype, root)
MPI_Allgatherv(sbuf, scount, stype,
               rbuf[p], rcounts[p], displs[p], rtype),
```

Операция `MPI_Scatterv` передаёт *scounts*[*rank*] элементов типа *stype* процессу *rank* = 0, 1, …, *p* – 1 из буфера *sbuf*[*rank*] + *displs*[*rank*] · *sizeof*(*stype*) корневого процесса *root*. Процессы принимают сообщение в свой буфер *rbuf* как *rcount* элементов типа *rtype*. В операции *Gatherv* корневой процесс *root* принимает в буфер *rbuf*[*rank*] + *displs*[*rank*] · *sizeof*(*rtype*) ровно *rcounts*[*rank*] элементов типа *rtype*. В операции *Allgatherv* каждый процесс передаёт своё сообщение, *scount* элементов типа *stype* из буфера *sbuf* и принимает от процесса *rank* в буфер *rbuf*[*rank*] + *displs*[*rank*] · *sizeof*(rtype) ровно *rcounts*[*rank*] элементов.

Основную сложность при разработке алгоритмов представляет нерегулярный размер сообщений, которые передаются в операции в виде векторов *scounts*, *rcounts* длины *p*, где *p* – число процессов.

Можно выделить два основных подхода к реализации обмена информацией между процессами с использованием разделяемой памяти многопроцессорного узла. Подход Copy-In-Copy-Out (CICO) основан на использовании сегмента памяти с общей для всех процессов очередью и системой флагов уведомления. Процесс-отправитель копирует в очередь фрагмент сообщения и уведомляет через флаги остальные процессы, после чего они копируют фрагмент в буфер пользователя в своем адресном пространстве. Таким образом, каждый фрагмент копируется дважды. Второй подход подразумевает использование специфичных для конкретного ядра операционной системы методов прямого доступа к памяти удаленного процесса: Linux Cross Memory Attach (CMA), KNEM, XPMEM [3–5]. Это позволяет сократить число копирований до одного, поэтому такой подход получил название ZeroCopy (нуль дополнительных копирований). Заметим, что ZeroCopy-подход эффективен, однако требует дополнительных модулей ядра или же повышения привилегий процессов, в то время как CICO-подход обеспечивает переносимость алгоритма на разные GNU/Linux-системы [6].

В данной работе рассматриваются алгоритмы на основе CICO-подхода. Предложены алгоритмы коллективных операции `MPI_Scatterv`, `MPI_Gatherv` и `MPI_Allgatherv`, использующие сегмент разделяемой памяти и систему очередей в нём. Приводится описание реализации алгоритмов на базе библиотеки Open MPI для операционной системы GNU/Linux и результаты экспериментов.

2. Описание алгоритма

Разработанные алгоритмы выполняются в два этапа:

1. Создание сегмента разделяемой памяти на этапе формирования нового MPI-коммуникатора и системы очередей и флагов в нём.
2. Реализация коллективной коммуникационной операции через очереди сегмента разделяемой памяти (при каждом вызове операции).

2.1. Структура сегмента разделяемой памяти

Нулевой процесс коммуникатора создает сегмент разделяемой памяти, используя системный вызов `mmap`. Остальные процессы подключаются к нему. В сегменте разделяемой памяти размещаются очереди для передачи фрагментов сообщений, массивы со счётчиками для уведомления процессов о готовности фрагментов в очереди, а также дополнительные флаги, обеспечивающие синхронизацию доступа к очередям при многократных вызовах

коллективных операций и смене корневых процессов. Для каждого из p процессов в сегменте хранятся:

- очередь $q[s]$ из s фрагментов (слотов) по f байт;
- массив $ctrl[s]$ для хранения размеров фрагментов, записанных в слоты очереди при выполнении корневых операций (one-to-all, all-to-one);
- массив $ctrlall[s \cdot p]$ для хранения размеров фрагментов, записанных в слоты очереди при выполнении операций all-to-all.

По умолчанию $s = 8$, $f = 8192$ байт, размеры и адреса массивов q, $ctrl$, $ctrlall$ выравнены на границу размера страницы памяти.

Для сокращения накладных расходов на ожидание освобождения очереди для повторного использования её слотов она разбивается на w множеств [7]. Для синхронизации доступа к множествам (частям очередей) в сегменте хранятся счётчики и флаги:

- op – счётчик количества обращений к коллективной операции;
- $nproc$ – количество процессов, читающих/записывающих слоты очереди.

По умолчанию каждая очередь логически разбита на $w = 2$ множества (множество – это s/w фрагментов очереди).

Для поддержки операций `MPI_Scatterv`, `MPI_Gatherv` с нерегулярными размерами сообщений корневой процесс уведомляет остальные процессы о размерах сообщений через разделяемые массивы:

- $typesize$ – размер типа данных в байтах;
- $counts[p]$ – массив с количеством элементов;
- $rootready[p]$ – флаги готовности данных в массиве $counts$.

Каждому процессу известно расположение в сегменте как своих блоков, так и блоков других процессов. У каждого процесса определена локальная для него переменная $local\_op$, использующаяся как счётчик количества обращений к коллективной операции. Счётчик $local\_op$ используется для синхронизации выполнения операции между процессами и должен иметь одинаковое значение у каждого процесса для корректного начала и завершения выполнения коллективной операции. В начале работы со слотами множества i корневой процесс устанавливает значение $ws[i].op = local\_op$, остальные процессы дожидаются, пока $ws[i].op$ не станет равно их локальному значению $local\_op$. После этого все процессы могут начать чтение/запись в слоты множества i. При задействовании процессом множества локальный счётчик его операций $local\_op$ увеличивается на единицу.

2.2. Алгоритм операции MPI_Scatterv

В алгоритме операции `MPI_Scatterv` только корневому процессу $root$ известны размеры сообщений $scount[i] \cdot sizeof(stype)$ для передачи процессам. Корневой процесс $root$ реализует передачу фрагментов сообщения через разделяемую память, используя фрагменты (слоты) очереди. Перед началом использования множества set процесс $root$ дожидается, когда значение $ws[set].nproc$ станет равным 0 (0 процессов работают со слотами). Синхронизация доступа к множеству осуществляется путем записи в $ws[set].op$ локального счётчика $local\_op$ и количества процессов, участвующих в обмене $ws[set].nproc = p$. Далее процесс $root$ размещает информацию о размерах сообщений $scounts$ в блоке разделяемой памяти $ws[set].counts$ и записывает размер типа данных $stype$ в блок $ws[set].typesize$, после чего уведомляет все процессы о готовности массива $scounts$: $ws[set].rootready[0..p-1] = 1$. После того как все процессы прочитают информацию о размерах сообщений, $root$ начинает выполнять передачу первого фрагмента длиной f байт каждому процессу в порядке их нумерации 0, 1, …, $p - 1$. Передача выполняется путем записи первых f байт для i-го процесса в фрагмент s очереди $q[s][i]$ процесса i. Уведомление процесса-получателя осуществляется путем записи в управляющий блок $ctrl[s][i]$ процесса i количества байт, записанных во фрагмент очереди. Цикл передачи повторяется, пока сообщения не будут переданы для всех процессов. После того как процесс запишет все данные в слоты множества, вызывается атомарная операция

уменьшения счётчика *ws*[*set*].*nproc* для уведомления о завершении работы процесса с множеством *set*. Если одного множества фрагментов недостаточно для обеспечения передачи всего сообщения, корневой процесс использует следующее множество фрагментов.

```
function MPI_Scatterv(sbuf, scounts[p], displs[p], stype, rbuf, rcount, rtype, root)
  is_first_iter = true
  if rank = root then
    nops = ceil(max(scounts, p) * sizeof(stype) / (f * s / w))
    // Копирование сообщения из sbuf в буфер корневого процесса
    copy(sbuf + displs[root] * sizeof(stype), rbuf, scounts[root] * sizeof(stype))
    nsend[root] = scounts[root] * sizeof(stype)
    while sum(nsend, p) < sum(scounts, p) * sizeof(stype) and nops > 0 do
      set = local_op % w          // Номер текущего множества фрагментов
      nops = nops - 1
      while ws[set].nproc > 0 do  // Ожидание освобождения множества очереди
      end while
      ws[set].nproc = p
      ws[set].op = local_op
      local_op = local_op + 1
      slot = set * s / w
      if is_first_iter then
        ws[set].typesize = sizeof(stype)   // Заполнение scounts[] размерами сообщений
        copy(scounts, ws[set].counts, p * sizeof(scounts))
        for i = 0 to p - 1 do            // Уведомления процессов о готовности scounts[]
          if root == i then continue
          ws[set].rootready[i] = 1
        end for
        is_first_iter = false
      end if
      while sum(nsend, p) < sum(scounts, p) * sizeof(stype) and
            slot < (set + 1) * s / w do
        for i = 0 to p - 1 do                       // Передача фрагмента каждому процессу
          if nsend[i] = scounts[i] * sizeof(stype) then continue
          fragsize = min(f, scounts[i] * sizeof(stype) - nsend[i])
          copy(sbuf + displs[i]* size(stype) + nsend[i], q[slot][i],
               fragsize)                     // Копирование фрагмента в очередь процесса i
          nsend[i] += fragsize
          ctrl[slot][i] = fragsize
        end for
        slot = slot + 1
      end while
      atomic_dec(ws[set].nproc)
    end while
  else // Некорневые процессы
    nrecv = 0
    nops = ceil(max(scounts, p) * sizeof(stype) / (f * s / w))
    while nrecv < rcount * sizeof(rtype) and nops > 0
      set = local_op % w                                  // Номер множества фрагментов
      while ws[set].op != local_op do  // Ожидание использования множества процессом root
      end while
      if is_first_iter then                              // Чтение размеров сообщений
        while ws[set].rootready[rank] != 0 do
        end while
        copy(ws[set].counts, scounts, p * size(scounts))
        ws[set].counts[rank] = 0                         // Уведомление о получении counts
        nops = ceil(max(scounts, p) * ws[set].typesize / (f * s / w))
        is_first_iter = false
      end if
      local_op = local_op + 1
      nops = nops - 1
      slot = set * s / w
      while nrecv < rcount * size(rtype) and slot < (set + 1) * s / w do
        while ctrl[slot][rank] != 0 do                    // Ожидание уведомления от root
        end while
        // Копирование фрагмента i из очереди процесса rank в буфер пользователя
        copy(q[slot][rank], rbuf + nrecv, ctrl[slot][rank])
        nrecv = nrecv + ctrl[slot][rank]
        ctrl[slot][rank] = 0                      // Уведомление о завершении копирования
        slot = slot + 1
      end while
```

```
      atomic_dec(ws[set].nproc)
    end while
  end if
end function
```

Рис. 1. Псевдокод алгоритма операции MPI_Scatterv

Операция `MPI_Scatter` является частным случаем операции `MPI_Scatterv`, в которой блоки данных, посылаемые каждому процессу, имеют одинаковый размер. На рис. 1 приведён псевдокод алгоритма операции `MPI_Scatterv`, в котором массив *nsend*[*i*] хранит суммарный размер фрагментов, переданных *root* процессу *i*.

Сложность алгоритма линейно зависит от количества p процессов и размера сообщения. Сложность по памяти определяется размером сегмента разделяемой памяти, который зависит от числа процессов p и длин очередей s и размеров фрагментов f.

2.3. Алгоритм операции MPI_Gatherv

Операция коллективного сбора данных `MPI_Gatherv` является обратной по отношению к `MPI_Scatterv`. Корневому процессу *root* известны размеры получаемых от процессов сообщений $rcounts[i] \cdot sizeof(rtype)$. В отличие от операции рассылки, алгоритм реализует сбор блоков данных различной длины, посылаемых всеми процессами группы, в один буфер *rbuf* процесса с номером *root*. Корневой процесс, как и в операции `MPI_Scatterv`, размещает информацию о размере сообщений *rcounts* в блок разделяемой памяти, после чего *root* ожидает уведомления о готовности фрагмента сообщения от всех некорневых процессов. Некорневой процесс i записывает первые f байт во фрагмент s очереди $q[s][i]$, после чего записывает в свой управляющий блок $ctrl[s][i]$ размер скопированного фрагмента, тем самым уведомляя *root* о завершении процесса записи в $q[s][i]$. После записи всех фрагментов в слоты множества вызывается атомарная операция уменьшения счётчика $ws[set].nproc$. Если одного множества фрагментов недостаточно для обеспечения передачи процессами всего сообщения, корневой процесс использует следующее множество фрагментов.

Операция `MPI_Gather` является частным случаем операции `MPI_Gatherv`, в которой блоки данных, посылаемые каждым процессом, имеют одинаковый размер.

2.4. Алгоритм операции MPI_Allgatherv

Функция MPI_Allgatherv является расширенной версией `MPI_Gatherv`, в которой получателями являются все процессы коммуникатора. Каждому процессу известны размеры получаемых сообщений $rcounts[i] \cdot sizeof(rtype)$. Для работы с множеством фрагментов процессы логически разделены – процесс с номером 0 обеспечивает синхронизацию для доступа к множеству, что в операции `MPI_Gatherv` выполняет процесс *root*.

Алгоритм операции `MPI_Allgatherv` не имеет корневого процесса, поэтому все процессы выполняют одинаковую последовательность действий. Каждый процесс i записывает первые f байт во фрагмент s очереди $q[s][i]$. После чего процесс i уведомляет остальные процессы о готовности данных в слоте очереди путем записи в управляющий блок $ctrlall[s][i \cdot j]$ количества байт для каждого процесса $j = 0, 1, \ldots, p - 1$, записанных во фрагмент очереди. Цикл записи в слоты очереди повторяется, пока не закончатся свободные слоты множества или сообщение не будет скопировано полностью. После завершения копирования фрагментов для передачи каждый процесс начинает активное ожидание уведомления от других процессов в порядке их нумерации $0, 1, \ldots, p - 1$ и копирует фрагмент сообщения в локальный буфер. Копирование фрагментов из очередей процессов повторяется, пока не закончатся слоты множества или сообщения от процессов не будут полностью получены. После того как процесс запишет и прочитает все данные из слотов множества, вызывается атомарная операция для уведомления о завершении работы процесса с множеством *set*. Если одного множества фрагментов

недостаточно для обеспечения передачи процессами всего сообщения, корневой процесс использует следующее множество фрагментов.

Операция `MPI_Allgather` является частным случаем операции `MPI_Allgatherv`, в которой блоки данных, посылаемые каждым процессом, имеют одинаковый размер.

3. Организация экспериментов

Алгоритмы реализованы на базе компонента `coll/sm` библиотеки Open MPI 4.1.2rc3. Компонент создает сегмент разделяемой памяти и очереди в нём, которые используют разработанные алгоритмы для обмена сообщениями. Для предотвращения некорректного уведомления процессами друг друга, в силу возможного внеочередного выполнения инструкций процессором, после записи в буферы очередей и управляющие блоки вызывается операция барьера записи в память (write memory barrier). Архитектурно-зависимые функции используются из подсистемы Open MPI OPAL (Open Portable Access Layer) [6].

Экспериментальная часть проводилась на сервере со следующей конфигурацией:

- двухпроцессорный сервер Intel Xeon Broadwell: 2 x Intel Xeon E5-2620 v4 (8 ядер, HyperThreading отключен, кеш-память L1 32 Кб, L2 256 Кб, L3 20 Мб);
- оперативная память: 64 Гб (2 NUMA-узла);
- ядро linux 5.14.10-300.fc35.x86_64 (ОС Fedora), gcc 11.2.1;
- MPI: Open MPI 4.1.2rc3.

В качестве теста производительности использовался пакет Intel MPI Benchmarks 2021 Update 3 (IMB-v2021.3). В работе использовалась методика оценки эффективности коллективных операций, описанная в работе [8]. Сравнение производительности осуществлялось с компонентом Open MPI `coll/tuned`. Для каждого размера сообщения операции запускались 5000 раз. Отключалось использование кеш-памяти (на каждом вызове использовался новый буфер, `-off_cache 20,64`), циклическое изменение номера корневого процесса контролировалось параметром `-root_shift 1`. При запуске разработанного алгоритма использовались параметры по умолчанию: количество множеств $w = 2$, количество фрагментов в очереди каждого процесса $s = 8$, размер одного фрагмента $f = 8192$ байт [7]. После каждого обращения к операции выполнялась барьерная синхронизация встроенным алгоритмом IMB. Параметры запуска теста:

```
IMB-MPI1 scatterv -off_cache 20,64 -iter 5000,250 -msglog 6:24 -sync 1
                  -imb_barrier 1 -root_shift 1 -time 600.0
```

В каждом эксперименте тест IMB запускался 5 раз, для каждого размера сообщения отбрасывались минимальное и максимальное значения t_max времени выполнения алгоритма, далее значение t_max усреднялось по результатам трех запусков.

3.1. Операция MPI_Scatterv

На рис. 2 и 3 показаны зависимости времени выполнения разработанного алгоритма операции `MPI_Scatterv` от размера сообщения при запуске 8 процессов и 16 процессов с различным распределением по ядрам NUMA-узлов. Время нормализовано относительно времени выполнения операции компонентом `coll/tuned`.

Разработанный алгоритм позволяет сократить время выполнения операции `MPI_Scatterv` на 60 % по сравнению с `coll/tuned` на сообщениях до 64 Кб. Пик времени выполнения при размере сообщения $m = 32$ Мб и количестве процессов $p = 16$ обусловлен накладными расходами на передачу сообщения и синхронизацию процессов на разных NUMA-узлах.

В среднем разработанный алгоритм показал сокращение времени на 30 % по сравнению с `coll/tuned`.

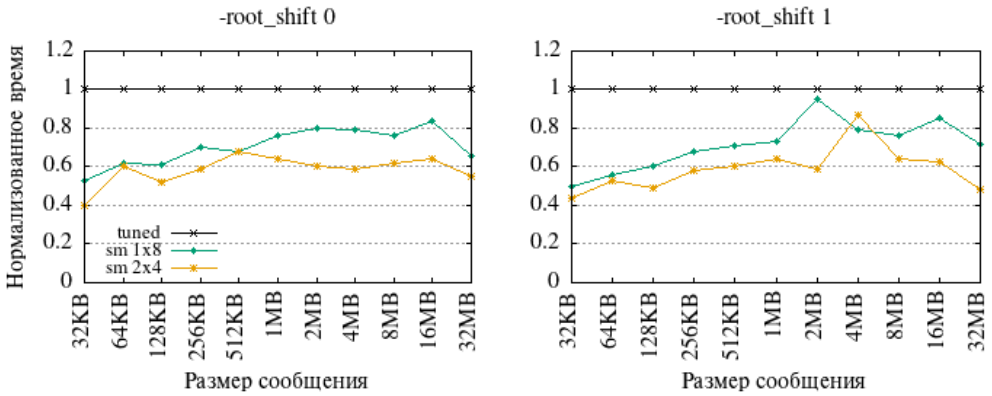

Рис. 2. Нормализованное время алгоритма MPI_Scatterv при запуске $p = 8$ процессов на одном NUMA-узле (1x8) и двух NUMA-узлах (2x4) с циклической сменой корневого процесса (-root_shift 1) и без (-root_shift 0). Время нормализовано относительно времени coll/tuned

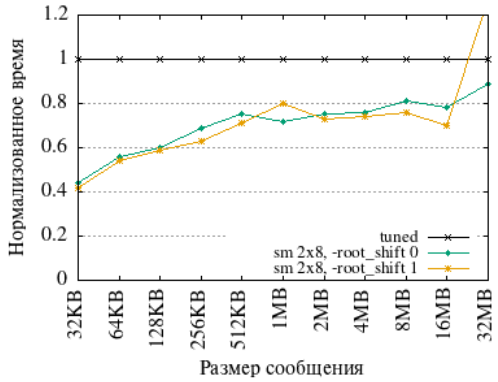

Рис. 3. Нормализованное время алгоритма `MPI_Scatterv` при запуске $p = 16$ процессов на двух NUMA-узлах (2x8) с циклической сменой корневого процесса (`-root_shift 1`) и без (`-root_shift 0`). Время нормализовано относительно времени компонента `coll/tuned`

3.2. Операция MPI_Gatherv

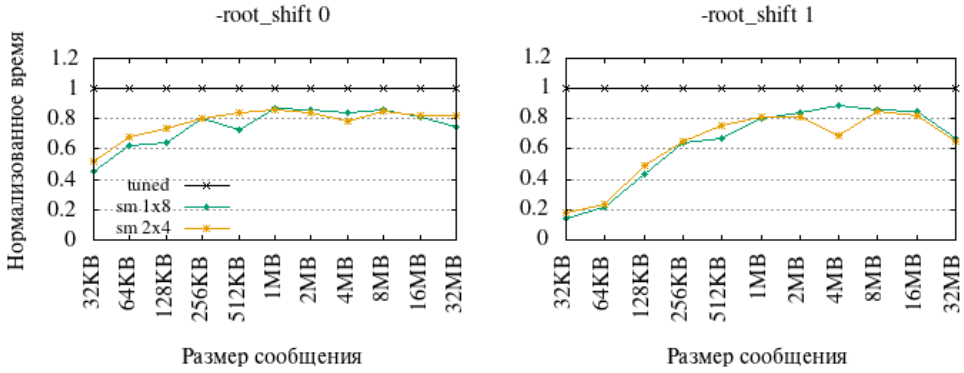

Рис. 4. Нормализованное время алгоритма `MPI_Gatherv` при запуске $p = 8$ процессов на одном NUMA-узле (1x8) и двух NUMA-узлах (2x4) с циклической сменой корневого процесса (`-root_shift 1`) и без (`-root_shift 0`). Время нормализовано относительно времени `coll/tuned`

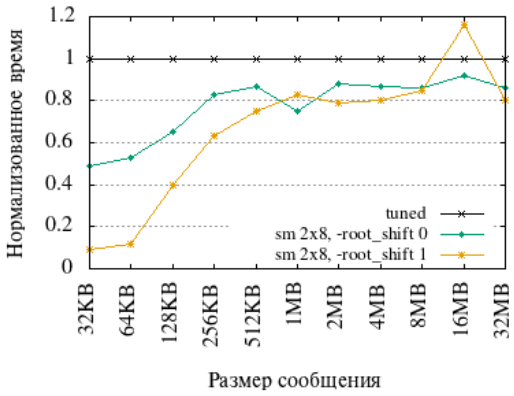

Рис. 5. Нормализованное время алгоритма `MPI_Gatherv` при запуске $p = 16$ процессов на двух NUMA-узлах (2x8) с циклической сменой корневого процесса (`-root_shift 1`) и без (`-root_shift 0`). Время нормализовано относительно времени компонента `coll/tuned`

На рис. 4 и 5 показаны зависимости времени выполнения алгоритма операции `MPI_Gatherv` от размера сообщения при запуске 8 и 16 процессов с различным распределением по ядрам NUMA-узлов. Время нормализовано относительно времени выполнения операции компонентом `coll/tuned`.

Предложенный алгоритм позволяет уменьшить время выполнения операции `MPI_Gatherv` на 90 % по сравнению с `coll/tuned` при передаче сообщений размером до 64 КБ. В проведенных экспериментах алгоритм показал время в среднем на 20–30 % меньше по сравнению с реализацией в компоненте `coll/tuned`.

3.3. Операция MPI_Allgatherv

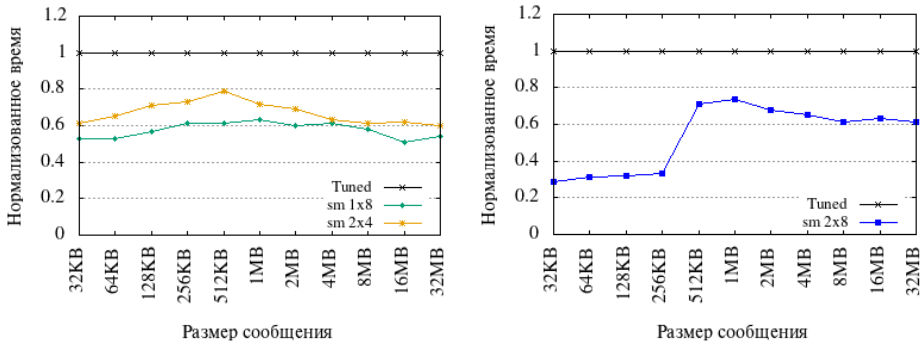

Рис. 6. Нормализованное время алгоритма `MPI_Algatherv` при запуске $p = 8$ процессов на одном NUMA-узле (1x8) и двух NUMA-узлах (2x4) и $p = 16$ процессов на двух NUMA-узлах (2x8). Время нормализовано относительно времени компонента `coll/tuned`

На рис. 6 представлены зависимости времени работы алгоритма операции `MPI_Allgatherv` от размера передаваемого сообщения при запуске 8 и 16 процессов с различным распределением по ядрам NUMA-узлов.

В проведенных экспериментах алгоритм показал время при передаче сообщений размером до $m = 256$ КБ и количестве процессов $p = 16$ на 70 % меньше, чем при использовании компонента `coll/tuned`. При запуске $p = 8$ процессов алгоритм показал стабильное сокращение времени выполнения на 30–40 % в сравнении с реализацией в компоненте `coll/tuned`.

4. Заключение

В работе предложены алгоритмы операции MPI_Scatterv, MPI_Gatherv и MPI_Allgatherv на многопроцессорных вычислительных SMP/NUMA-систем с использованием разделяемой памяти. Выполнена программная реализация алгоритмов на базе библиотеки Open MPI. Эксперименты на двухпроцессорном сервере показали: в среднем предложенные алгоритмы выполняют коллективные операции MPI_Scatterv, MPI_Gatherv и MPI_Allgatherv на 20–40 % быстрее алгоритмов компонента `coll/tuned`. Наибольшее сокращение времени достигается при передаче сообщений до 64 Кб для операций `MPI_Scatterv` и `MPI_Gather` и до 256 Кб для операции `MPI_Allgatherv`.

В дальнейшем планируется реализовать полный набор блокирующих коллективных операций, а также учесть возможности ZeroCopy-подхода (GNU/Linux CMA, XPMEM, KNEM).

Литература

1. MPI: A Message-Passing Interface Standard Version 4.0 [Электронный ресурс]. URL: `http://www.mpi-forum.org/docs/mpi-4.0/mpi40-report.pdf` (дата обращения: 15.05.2022).
2. Open MPI: Open Source High Performance Computing [Электронный ресурс]. URL: `http://www.open-mpi.org` (дата обращения: 15.05.2022).
3. CMA: Cross Memory Attach [Электронный ресурс]. URL: `https://lwn.net/Articles/405284/` (дата обращения: 20.05.2022).
4. KNEM High-Performance Intra-Node MPI Communication [Электронный ресурс]. URL: `https://knem.gitlabpages.inria.fr` (дата обращения: 20.05.2022).
5. XPMEM: Linux Cross-Memory Attach [Электронный ресурс]. URL: `https://github.com/hjelmn/xpmem` (дата обращения: 20.05.2022).
6. *Курносов М. Г., Токмашева Е. И.* Алгоритм широковещательной передачи стандарта MPI на базе разделяемой памяти многопроцессорных NUMA-узлов // Вестник СибГУТИ. 2020. № 1 (49). С. 42–59.
7. *Graham R. L., Shipman G.* MPI Support for Multi-core Architectures: Optimized Shared Memory Collectives // Proc. of the 15th European PVM/MPI Users' Group Meeting, 2008. P. 130–140.
8. *Jain S., Kaleem R., Balmana M., Langer A., Durnov D., Sannikov A. and Garzaran M.* Framework for Scalable Intra-Node Collective Operations using Shared Memory // Proc. of the International Conference for High Performance Computing, Networking, Storage, and Analysis (SC-2018), 2018. P. 374–385.

Статья поступила в редакцию 06.07.2022.

Романюта Алексей Андреевич
аспирант 1 курса, ассистент кафедры вычислительных систем Сибирского государственного университета телекоммуникаций и информатики (630102, Новосибирск, ул. Кирова, 86), e-mail: `alexey_r.98@ngs.ru`.

Курносов Михаил Георгиевич
д.т.н., профессор, профессор кафедры вычислительных систем Сибирского государственного университета телекоммуникаций и информатики, тел. (383) 269-83-82, e-mail: `mkurnosov@sibsutis.ru`;

старший научный сотрудник федерального государственного бюджетного учреждения науки Института физики полупроводников им. А. В. Ржанова СО РАН (630090, Новосибирск, пр. Ак. Лаврентьева, 13), тел. (383) 330-56-26, e-mail: mkurnosov@isp.nsc.ru.

Shared Memory-based Algorithms for Vector Collective Operations of the MPI Standard

Alexey A. Romanyuta
Computer systems department, Siberian State University of Telecommunications and Information Science (SibSUTIS, Novosibirsk, Russia), alexey_r.98@ngs.ru.

Mikhail G. Kurnosov
Doctor of Technical Science, Professor, Siberian State University of Telecommunications and Information Science (SibSUTIS, Novosibirsk, Russia), mkurnosov@sibsutis.ru.
Senior Research Scientist, Computer Systems Laboratory, Rzhanov Institute of Semiconductor Physics of the Siberian Branch of the RAS (Novosibirsk, Russia), mkurnosov@isp.nsc.ru.

Algorithms for MPI_Scatterv, MPI_Gatherv, MPI_Allgatherv collective operations using the shared memory of multiprocessor SMP/NUMA systems are proposed. The algorithms use an approach based on copying message fragments via queues in a shared memory segment (Copy-In-Copy-Out). The algorithms were implemented based on Open MPI and the execution time is reduced on average by 20-40% for the MPI_Scatterv, MPI_Gatherv, MPI_Allgatherv operations compared to the coll/tuned component of the Open MPI library.

Keywords: Scatterv, Gatherv, Allgatherv, collective operations, MPI, computer systems.

References

1. *MPI: A Message-Passing Interface Standard Version 4.0,* available at: http://www.mpi-forum.org/docs/mpi-4.0/mpi40-report.pdf (accessed: 15.05.2022).
2. *Open MPI: Open Source High Performance Computing*, available at: http://www.open-mpi.org (accessed: 15.05.2022)
3. *CMA: Cross Memory Attach*, available at: https://lwn.net/Articles/405284/ (accessed: 20.05.2022)
4. *KNEM High-Performance Intra-Node MPI Communication*, available at: https://knem.gitlabpages.inria.fr (accessed: 20.05.2022)
5. *XPMEM: Linux Cross-Memory Attach*, available at: https://github.com/hjelmn/xpmem (accessed: 20.05.2022)
6. Kurnosov, M. G., Tokmasheva E. I. Algoritm shirokoveshchatel'noj peredachi standarta MPI na baze razdelyaemoj pamyati mnogoprocessornyh NUMA-uzlov [MPI Broadcast Algorithm Based on Shared Memory of Multiprocessor NUMA Nodes]. *Vestnik SibGUTI*, 2020, no. 1, pp. 42-59.
7. Graham R. L., Shipman G. MPI Support for Multi-core Architectures: Optimized Shared Memory Collectives. *Proc. of the 15th European PVM/MPI Users' Group Meeting*, 2008, pp. 130–140.
8. Jain S., Kaleem R., Balmana M., Langer A., Durnov D., Sannikov A. and Garzaran M. Framework for Scalable Intra-Node Collective Operations using Shared Memory. *Proc. of the International Conference for High Performance Computing, Networking, Storage, and Analysis (SC-2018)*, 2018, pp. 374–385.

УДК 004.056.53
DOI: 10.55648/1998-6920-2022-16-3-48-55

Метод защиты программ от отладочных точек останова посредством исполнения фрагментов кода в общем буфере

И. В. Нечта[1]

Работа посвящена проблеме создания антиотладочных механизмов программы. Рассматривается один из наиболее стойких методов постановки точек останова для программ, который не может быть выявлен известными на сегодняшний день алгоритмами. В рамках исследования предлагается новый подход к написанию программ, который приводит к снижению эффективности самого принципа отладки, базирующегося на точках останова. Предлагается хранить функции программы в виде набора байт и перед их исполнением копировать код в один общий буфер. Учитывая, что точки останова привязаны к адресу, мы в результате получим остановку отладчика на каждой выполняемой в буфере функции, а не на какой-то определенной, что существенно увеличит время отладки.

Ключевые слова: антиотладочные механизмы, точки останова, распаковщики, протекторы.

1. Введение

При разработке программного обеспечения автор определяет в лицензионном соглашении условия распространения своего приложения. В одном случае это может быть бесплатная программа с открытым исходным кодом, в другом случае – платная (проприетарная). Часто в лицензионном соглашении указывается запрет не только на любые модификации программы, но и на попытки изучить алгоритмы её работы при помощи отладочных средств (дизассемблеров, декомпиляторов).

Модификация приложений может выполняться, например, с целью нарушения алгоритма проверки лицензионного ключа, когда злоумышленник пытается бесплатно воспользоваться программой. Другим примером может стать попытка встроить стороннюю рекламу в готовый продукт без согласия на то настоящего правообладателя. Если программа широко используема, то модифицированное приложение также будет использоваться и приносить доход постороннему лицу в обход лицензионного соглашения.

Очевидно, что для модификации скомпилированной программы требуется сначала изучить алгоритм её работы. Несмотря на наличие в лицензии явного запрета использовать отладочные средства, разработчики всё же стараются встроить в программу некоторые системы защиты или алгоритмы противодействия известным методам отладки и анализа программ.

Дизассемблер может анализировать программу как в статическом режиме, наглядно представляя код, так и в динамическом режиме, когда она запускается и пошагово выполняется с фиксированным набором входных данных. Очевидно, что статический и динамический анализ взаимно дополняют друг друга.

[1] Исследование выполнено в рамках НИОКТР № 122031600164-6 от 15.03.2022.

Согласно обзору, проведенному в работе [1], существует множество отладчиков, например, `IDA pro debugger`, `Immunity Debugger`, `OllyDebugger`, `Windbg` и другие. Полезным функционалом в современных отладчиках являются:

- поиск сигнатур, позволяющий распознать вызываемые функции программных компонент среды разработки (в статическом режиме);
- интерактивный анализ, использующий значения, передаваемые в регистры и арифметические преобразования в коде программы, для последующего определения особенностей хода выполнения алгоритма (в статическом режиме).
- точки останова (*breakpoints*), используемые при динамическом анализе для остановки программы во время её выполнения.

Развитие отладочных утилит повлекло за собой создание приёмов, препятствующих проведению статического и динамического анализа. Обзор таких подходов представлен в работах [2, 3]. Так, известны программы-*упаковщики* (packers) [4]: `UPX`, `ASPack`, `NsPack` и программы-протекторы: `Themida`, `Armadillo`, `ASProtect`, `ExeCryptor`. Упаковщики ориентированы на то, чтобы сжать и зашифровать программный код в файле, а перед его непосредственным исполнением – распаковать в оперативной памяти и продолжить выполнение. Протекторы в дополнение к шифрованию кода активно противодействуют или завершают работу программы при обнаружении факта работы отладчика.

Наиболее эффективным инструментом в отладке являются точки останова. Аппаратные точки реализованы на уровне процессора и настраиваются через отладочные регистры (*Dr0 – Dr7*). Программные представляют собой процессорную инструкцию с кодом операции `0xCC` (прерывание 3 применяемой в ОС Windows), которая вставляется вместо какой-либо инструкции кода. Когда процессор дойдет до такой перезаписанной команды, то управление перейдет в отладчик. Далее по команде от пользователя восстанавливается перезаписанная инструкция и продолжается выполнение программы. В период такой остановки пользователь может анализировать и изменять фактические значения переменных, регистров, блоков памяти, а также хода выполнения программы.

В качестве меры противодействия перезаписыванию кода протекторы нарушали корректный механизм работы прерываний (через собственную отладку), анализировали фрагменты кода с целью обнаружить вставку чужеродных инструкций и т.д. Тем не менее в работе [5] был предложен подход и программное средство *Spider*, не позволяющее проверить отлаживаемой программе наличие точек останова всеми известными на сегодняшний день способами. Согласно этому подходу производится перехват обращений к страницам памяти (при чтении, записи и исполнении) и подмена страниц. То есть существует две версии страницы в памяти. При обращении к странице в режиме исполнения кода программа предоставляет оригинальную страницу с точкой останова. При обращении к памяти для чтения, например, когда протектор пытается проанализировать код, ему предоставляется ложная страница без точек останова. Таким образом, работая на уровне драйвера операционной системы, предложенная программа реализует «*невидимые точки останова*». Единственным способом обнаружить факт отладки мог бы стать подсчет времени выполнения кода, которое естественно увеличится при отладке. Однако эта возможность нивелируется применением в *Spider* системы виртуализации, реализованной в `IntroLib` [6], когда подменяется время, считываемое командой *RDTSC*.

Упаковщики и протекторы работают, когда к ним на вход подается уже скомпилированный исполняемый файл. У них нет возможности дизассемблировать программу и исправлять вызовы между функциями, кроме случаев обращения к API-функциям через таблицу импорта. Обычно основная работа защитного механизма протектора заканчивается перед передачей управления в оригинальную точку входа программы (*Original Entry Point*). Если злоумышленнику удастся найти *OEP*, то с высокой вероятностью защита будет уничтожена.

В новом подходе защита реализуется на этапе создания исходного кода (до применения протектора) и, соответственно, служит дополнительным уровнем защиты программы.

Так, предлагается новый метод построения программного кода, который существенно осложняет применение точек останова. В дополнение к существующим методам противодействия предлагается выполнять фрагменты кода (функции) в общем буфере. То есть функции хранятся в виде зашифрованных данных и непосредственно перед выполнением они расшифровываются в буфер и там выполняются.

Ранние подходы, реализованные в пакерах [4], уже предполагали расшифровку кода, но позиция расшифрованных функций совпадала с их позицией в оригинальном незащищенном файле[2]. Таким образом, каждая функция была привязана к своему адресу. Использование программных и аппаратных точек останова позволяло отследить факт перехода на нужную функцию при существенной экономии времени (т.е. не задерживаясь в других местах). В настоящем подходе, когда большинство функций выполняется в одном и том же участке памяти, точки останова как программные, так и аппаратные будут возвращать управление в отладчик при выполнении каждой функции (т.е. анализ превратится в трудоёмкую пошаговую отладку). Более того, расшифровка программы происходит мелкими частями, что не даёт возможности одним действием скопировать её образ (дамп) и снять защиту, как это происходит при помощи программ-распаковщиков, например [4, 7].

2. Описание предлагаемого алгоритма

Дадим формальное описание предлагаемого метода. Пусть Prog – множество программ, имеющих одинаковые наборы входных и выходных данных (т.е. различные реализации выполнения некоторой задачи). Обозначим незащищенную программу как $\mathrm{P}\colon \mathrm{P} \in \mathrm{Prog}$. Программы в соответствии с принципом модульного программирования состоят из набора функций (подпрограмм или модулей) $P = \{p_1, p_2, \dots, p_n\}$. Функции попарно не пересекаются $\bigcap_i p_i = \emptyset$. Перед запуском программы они сначала загружаются в память M, и каждая функция получает свой участок памяти $m_i \in \mathrm{M}$, они также не пересекаются между собой $\bigcap_i m_i = \emptyset$. Обозначим процесс загрузки как $\mathrm{Load}\colon \mathrm{P} \to M$.

В рамках исследования требуется разработать метод преобразования программы $Protect\colon \mathrm{P} \to G$, где $\mathrm{G} \in \mathrm{Prog}$, но в отличие от незащищенной программы (с биективным отображением функций в память) в защищенной происходит сюръективное отображение $\mathrm{Load}\colon \mathrm{G} \to M^*$, т.е. $|G| > |M^*|$ и $\bigcap_j m_j^* = \emptyset$. Причем для эффективной защиты требуется выполнение: $|M^*| \to \min$.

Рассмотрим предлагаемый метод по шагам, представленным ниже. В данной статье используются примеры кода на языке программирования C++. Полный исходный код представлен в репозитории [8].

1. Выделяем буфер для записи и исполнения в нем функций, размер которого равен максимальному размеру из этих функций в скомпилированной программе. Блок памяти должен быть выровнен на границу 4 Кб. Например, `buffer=(char*) memalign(4096, CodeSize)`. Размеры функций можно посчитать непосредственно в самой программе (см. ниже) либо их можно посчитать дизассемблером.
2. Устанавливаем атрибуты страницы, где размещен буфер для чтения, записи и исполнения, т.к. область памяти для данных (буфера) не доступна для исполнения кода: `mprotect(buffer, CodeSize,PROT_WRITE|PROT_EXEC)`.
3. Копируем данные в буфер и вызываем функцию.

[2] Речь идет о адресах (смещениях) внутри секции кода, т.к. виртуальный базовый адрес (ImageBase) обычно меняется протектором.

Поясним первый пункт метода. Расчёт размера функции может быть выполнен внутри программы. Например:

```
extern char __start_func[];
extern char __stop_func[];

__attribute__((noinline, section("func")) ) void MyFunction( ){
    // Некоторый код функции
}

int main( ){
    long CodeSize = (long)__stop_func-(long)__start_func;
```

Отметим, что функция находится в секции, название которой выделено жирным шрифтом. `__start_func` и `__stop_func` преобразуются компилятором в константы, соответствующие началу и концу секции.

Для корректной работы алгоритма особое внимание следует уделить компилятору. Так, для Microsoft Visual Studio 2019 вызов функции осуществляется не напрямую, а через дополнительную переходную функцию, см. рис. 1. Здесь мы наблюдаем переходную функцию `sub_4111CC`, которая содержит еще один переход (команду `jmp`) уже на настоящую реализацию интересующей нас функции, реализованной в `sub_412460`. Соответственно, мы не сможем из кода C++ получить ни размер, ни адрес начала искомой функции. Поэтому предлагаемый алгоритм не будет работать с таким компилятором. В настоящем исследовании использовался компилятор *g++ Ubuntu v.9.4.0*.

Выполнение третьего пункта алгоритма – заполнение буфера – не должно вызывать трудностей, т.к. это обычный массив типа char, размещаемый в динамической области памяти. В свою очередь, данные для этого буфера могут быть скачаны по сети, храниться в стороннем файле или в секции исполняемого файла. Данные, очевидно, могут шифроваться. Первичное получение кода функций в виде массива реализовано в примере [8] (файл `Example.cpp`, функция `save()`.

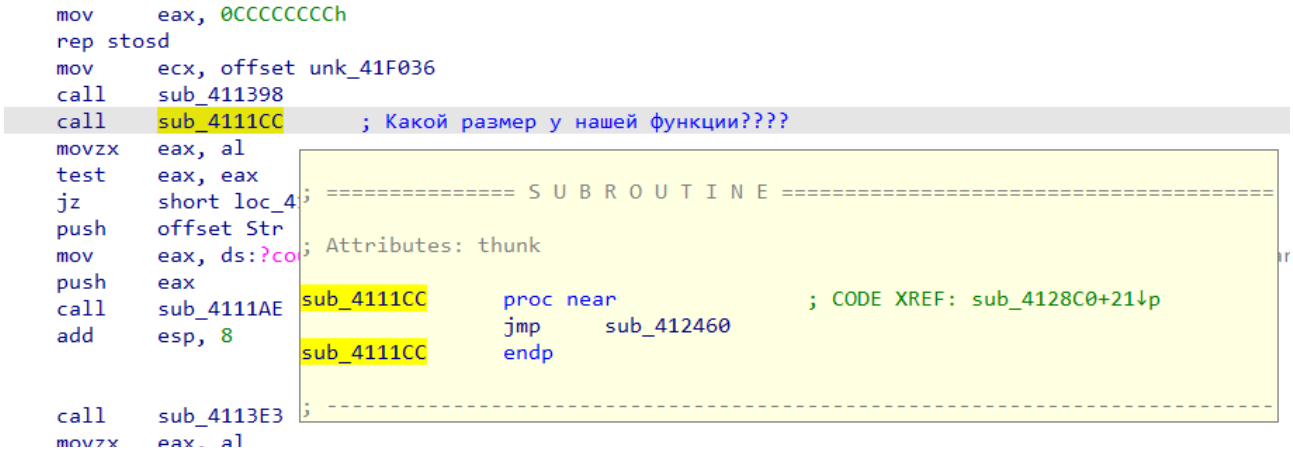

Рис. 1. Применение промежуточной функции перед вызовом основной

Для вызова буферной функции следует создать дополнительные переменные с типом данных – указатель на функцию:

```
typedef void (*PFunc)();
Pfunc* f=(Pfunc*)&buffer;

Load();                                    //загрузка функции в буфер.
f();                                       //вызов функции из буфера.
```

Если внутри функции буфера происходит вызов любой другой дочерней функции (назовем её подпрограммой), то компилятор будет указывать в процессорной инструкции

относительный адрес вида: *переход на несколько байт вперед или назад относительно текущего адреса*. Учитывая, что буфер выделяется в динамической области памяти (т.е. его адрес меняется при каждом запуске программы), следует передавать адрес вызываемой подпрограммы в качестве параметра функции. Например:

```
typedef double (*PFcos)(double x);
typedef double (*Pfunc)(PFcos MyCos);

__attribute__((noinline, section("func")) )
                                        double MyFunction (PFcos MyCos){
    return MyCos(0);
}
void main(){
    Pfunc* f=(Pfunc*)&buffer;
    Load();                                    //загрузка функции в буфер
    double y=(*f)(&cos);      //адрес мат. функции косинус как параметр
}
```

Стоит отметить, что в выбранном компиляторе g++ инициализация локальных переменных осуществляется корректно. Например, для следующего кода содержимое строки представлено в виде констант, что показано на рис. 2. В ряде компиляторов такие строки могут храниться в секции данных, тогда такая инициализация будет невозможна и потребуется передавать строку в качестве параметра.

```
__attribute__((noinline, section("func")) ) int func(PFcos _cos){
char WaterMark[]="Ivan V. Nechta";
    …
}
```

```
push    rbp
mov     rbp, rsp
sub     rsp, 30h
mov     [rbp-28h], rdi
mov     rax, fs:28h
mov     [rbp-8], rax
xor     eax, eax
pxor    xmm0, xmm0
movss   dword ptr [rbp-20h], xmm0
mov     rax, ' .V navI' ; Ivan V.
mov     [rbp-17h], rax
mov     dword ptr [rbp-0Fh], 'hceN' ; Nechta
mov     word ptr [rbp-0Bh], 'at'
mov     byte ptr [rbp-9], 0
mov     dword ptr [rbp-1Ch], 0
```

Рис. 2. Инициализация строковых переменных

3. Экспериментальный анализ параметров метода

Для реализации метода внутри защищаемой программы требуется экспериментально подобрать используемые параметры, например, размер буфера. Для проведения эксперимента были отобраны 50 исполняемый файлов (`*.exe`) из каталога имеющихся на компьютере программ `C:\Program Files (x86)`. Учитывая, что программы значительно варьируются по размеру, то все их функции объединялись в один общий набор и анализировались без учета принадлежности к конкретному файлу. Скрипт для анализа функций дизассемблером IDA [9] представлен по ссылке [8] (файл `Analyse.idc`).

В табл. 1 представлены результаты анализа длины функций. Данные сведения нужны для определения длины создаваемого буфера, который должен вмещать в себя любую выполняемую функцию.

Здесь погрешность определялась как $\Delta = \pm\frac{s}{\sqrt{N}} * t_a$, где s – исправленное среднеквадратическое отклонение, N – количество анализируемых функций, t_a – квантиль распределения Стьюдента с уровнем доверия $a = 95\ \%$.

Таблица 1. Результаты анализа длины функций исполняемых файлов

Кол-во функций	Средняя длина, байт	Исправл. СКО	Максимальная длина, байт
83853	180.2 ± 4.2	610	32986

Теперь оценим потенциальную эффективность метода. В формальной постановке задачи было упомянуто, что защищенность достигается при $|M^*| \to \min$. Такое возможно, когда доля функций, размещаемых и исполняемых в буфере, будет значительной. В идеальном случае – все функции выполняются в буфере.

Как уже упоминалось ранее, для вызовов подпрограмм из кода в буфере требуется передача адресов каждой подпрограммы в качестве параметров. Соответственно, простейшей ситуацией является та, при которой вызовов не происходит. Таким образом, был проведен анализ, в котором оценивалась доля функций в исполняемом файле к числу вызываемых ими подпрограмм. На рис. 3 показана доля функций, вызывающих разное количество подпрограмм. Общее количество функций составляет 83853 шт. Например, согласно диаграмме существует всего 1 % функций, у которых внутри не менее 50 вызовов подпрограмм.

Из диаграммы видно, что 32 % функций не делает вообще никаких вызовов (т.е. не требуется передавать дополнительных параметров), а 19 % вызывает только одну подпрограмму (требуется всего один дополнительный параметр). Таким образом, более половины всех функций может исполняться из буфера без существенного усложнения кода программы.

На основании полученных данных мы можем оценить, что в худшем случае для одной требуемой точки останова будут дополнительно возникать $\frac{83853}{50} \approx 1677$ ложных остановок, соответственно, в среднем 838.5 раз, что сделает процесс анализа программы достаточно трудоёмким.

4. Заключение

В настоящей работе предложен метод противодействия отладочным точкам останова. В ходе анализа существующих программ было показано, что метод может быть успешно реализован, т.к. более половины функций либо не вызывают, либо вызывают только одну дочернюю подпрограмму, что делает простой реализацию предлагаемого метода.

Анализ также показал увеличение среднего времени отладки в 839 раз, что является приемлемым результатом. При реализации защиты большое внимание следует уделить используемому компилятору и параметрам его использования. Полученный алгоритм защищает программу не только от статического и динамического анализа, но и от снятия дампа памяти процесса после обнаружения *OEP*.

Рис. 3. Распределение функций по числу вызываемых подпрограмм

Литература

1. *Apostolopoulos T., Katos V., Choo K. K. R., Patsakis C.* Resurrecting anti-virtualization and anti-debugging: Unhooking your hooks // Future Generation Computer Systems. 2021. V. 116. P. 393–405.
2. *Zhang B.* Research Summary of Anti-debugging Technology // Journal of Physics: Conference Series. IOP Publishing. 2021. V. 1744, № 4. P. 042186.
3. *Shields T.* Anti-debugging – a developers view. Veracode Inc., USA, 2010.
4. *Guo F., Ferrie P., Chiueh T. C.* A study of the packer problem and its solutions // Proc. of the International Workshop on Recent Advances in Intrusion Detection, 2008. P. 98–115.
5. *Deng Z., Zhang X., Xu D.* Spider: Stealthy binary program instrumentation and debugging via hardware virtualization // Proc. of the 29th Annual Computer Security Applications Conference, 2013. P. 289–298.
6. *Deng Z., Xu D., Zhang X., Jiang X.* Introlib: Efficient and transparent library call introspection for malware forensics // Digital Investigation. 2012. V. 9. P. S13–S23.
7. Программы-распаковщики [сайт]. URL: `http://www.all-for-rus.narod.ru/unpack.htm` (дата обращения: 21.06.2022).
8. Скрипт для анализа и исходный код примера [репозиторий]. URL: `https://github.com/ivannechta/UntiBPX/` (дата обращения: 21.06.2022).
9. Официальный сайт дизассемблера IDA [сайт]. URL: `https://www.hex-rays.com/ida-free/` (дата обращения: 21.06.2022).

Статья поступила в редакцию 27.06.2022.

Нечта Иван Васильевич
д.т.н., доцент, заведующий кафедрой прикладной математики и кибернетики СибГУТИ (630102, Новосибирск, ул. Кирова, 86), тел. (383) 2-698-216, e-mail: ivannechta@gmail.com.

Method for Programs Protection against Breakpoints by Code Fragments Execution in a Shared Buffer

Ivan V. Nechta
Doctor of technical sciences, Department chairman, Siberian State University of Telecommunications and Information Science (SibSUTIS, Novosibirsk, Russia), ivannechta@gmail.com.

The article is devoted to the problem of creating anti-debugging mechanisms of the program. One of the most robust methods of setting breakpoints for programs is considered which cannot be detected by currently known algorithms. As part of the study, a new approach for program development is proposed which leads to decreasing in the effectiveness of debugging based on breakpoints. It is proposed to store program functions as a set of bytes and copy their code into one shared buffer before executing them. Given that the breakpoints are bound to the address, as a result we will get a debugger stop at each function executed in the buffer, not at any specific one, that will significantly increase the debugging time.

Keywords: anti-debug mechanisms, breakpoints, unpackers, code protectors.

References

1. Apostolopoulos T., Katos V., Choo K. K. R., and Patsakis C. Resurrecting anti-virtualization and anti-debugging: Unhooking your hooks. *Future Generation Computer Systems*, 2021, vol. 116, pp. 393–405.
2. Zhang B. Research Summary of Anti-debugging Technology. *Journal of Physics: Conference Series. IOP Publishing*, 2021, vol. 1744. no. 4, p. 042186.
3. Shields T. Anti-debugging – a developers view. *Veracode Inc.*, USA, 2010.
4. Guo F., Ferrie P. and Chiueh T. C. A study of the packer problem and its solutions. *International Workshop on Recent Advances in Intrusion Detection*, 2008, pp. 98–115.
5. Deng Z., Zhang X. and Xu D. Spider: Stealthy binary program instrumentation and debugging via hardware virtualization. *Proceedings of the 29th Annual Computer Security Applications Conference,* 2013, pp. 289–298.
6. Deng Z., Xu D., Zhang X. and Jiang X. Introlib: Efficient and transparent library call introspection for malware forensics. *Digital Investigation,* 2012, vol. 9, pp. S13–S23.
7. *Programmy raspakovshhiki* [Programs for unpacking], available at: http://www.all-for-rus.narod.ru/unpack.htm (accessed: 21.06.2022).
8. *Skript dlja analiza i ishodnyj kod primera* [Analysis script and source code example], available at: https://github.com/ivannechta/UntiBPX/ (accessed: 21.06.2022).
9. *Oficial'nyj sajt dizassemblera IDA* [Official site of disassembler IDA], available at: https://www.hex-rays.com/ida-free/ (accessed: 21.06.2022).

УДК 681.7.068
DOI: 10.55648/1998-6920-2022-16-3-56-61

Модель надежности оптоволокна в условиях деградации

В. П. Шувалов[1], Б. П. Зеленцов, И. Г. Квиткова

Для расчёта надёжности оптического волокна в условиях деградации предложена марковская модель, позволяющая учитывать ухудшение характеристик оптического кабеля в процессе его эксплуатации. Приведена методика расчета коэффициента неготовности при различном времени эксплуатации, а также пример расчета коэффициента неготовности.

Ключевые слова: пассивная оптическая сеть доступа, деградация оптоволокна, деградационный отказ, показатели надежности, время эксплуатации оптического кабеля.

1. Введение

В 2019 году Международным союзом электросвязи (МСЭ-Т) была предложена концепция «Сеть – 2030» (Network 2030), представленная в документах [1, 2, 3].

Согласно этой концепции сеть доступа должна поддерживать «услуги с максимально доступным качеством (best effort), а также высоконадёжные (коэффициент готовности 0.9999999 и выше) и высокоскоростные услуги» [4]. В рамках концепции «Сеть – 2030» также ставится задача по преобразованию сетей доступа в многофункциональную платформу по предоставлению услуг и доступа с предоставлением услуг с коэффициентом готовности более семи девяток. Реализация таких сетей должна осуществляться на основе использования оптического кабеля. Известно, что в среднем на один километр число внезапных отказов оптического кабеля (ОК) на интервале 10^9 часов ровно 570 FIT (Failure in Time) [5], где один FIT – это один отказ за 10^9 часов. При увеличении длины ОК до 100 км число отказов за 10^9 часов возрастает до 57000. Такая длина ОК характерна для сетей доступа большого радиуса действия [6]. При этом для обеспечения значения коэффициента готовности 0.9999999 время восстановления должно быть не более 0.1 минуты, что невозможно обеспечить без резервирования.

В составе пассивной оптической сети доступа, кроме ОК, имеются: оптический линейный терминал (Optical Line Terminal, OLT), оптический сетевой терминал (Optical Network Terminal, ONT), сплиттеры, оптические мультиплексоры/демультиплексоры. Однако значение коэффициента готовности цепочки OLT–ONT будет в основном определяться интенсивностью отказов ОК.

Помимо внезапных отказов на определённом этапе жизни оптоволокна приходится считаться с постепенными или деградационными отказами. В ГОСТ 27.102-2021 [7] под деградационным отказом понимается «отказ, обусловленный естественными процессами старения, износа, коррозии и усталости при соблюдении правил и (или) норм проектирования, изготовления и эксплуатации». Именно деградационные отказы определяют срок службы ОК. Иногда к необходимости замены ОК приводит так называемый моральный износ - несоответствие параметров ОК современным условиям эксплуатации.

[1] Работа выполнена в рамках государственного задания № 122032300218-6.

В процессе деградации ОК может находиться в состояниях, которые можно охарактеризовать:

1. Значением вероятности отказа ОК на данном временном интервале.

2. Значением времени жизни ОК, т.е. временем до достижения им предельного состояния (ГОСТ 27.102–2021).

3. Значением ослабления сигнала [8] в цепочке OLT–ONT. При определённом значении ослабления обмен информацией в цепочке OLT–ONT станет невозможным.

4. Стоимостью выполнения ремонтных работ. Она растёт с годами, что рано или поздно приводит к необходимости замены ОК.

Выберем далее в качестве характеристики состояния деградации интенсивность отказов. Как отмечается в [9], именно возрастание интенсивности отказов $\lambda(t)$ с физической точки зрения является наиболее естественной характеристикой деградации. Перечисленные выше варианты фиксации состояний деградации можно в той или иной мере увязать с $\lambda(t)$.

В [10] рассмотрены два подхода к оценке срока жизни ОК: на основе анализа старения оболочки кабеля и старения оптоволокна (ОВ). В данной работе используется второй подход, основанный на прогнозе срока службы ОВ.

Разобьем время эксплуатации оптоволоконной линии на временные интервалы длительностью T. Каждый такой интервал назовем периодом эксплуатации. Будем полагать, что значения интенсивности отказов на каждом из временных интервалов известны [11]. Найдём выражение для расчёта коэффициента неготовности за i периодов эксплуатации.

2. Модель для расчета параметров надежности оптоволокна в условиях деградации

При формировании модели приняты следующие условия.

1. При эксплуатации ОВ имеют место отказы, обнаруживаемые в момент их возникновения (явные отказы). После обнаружения отказа происходит восстановление линейного участка, на котором произошел отказ, путем его замены.

2. Время эксплуатации ОВ разбивается на периоды с одинаковой продолжительностью T.

3. Каждый период характеризуется определенным состоянием деградации, который описывается соответствующей интенсивностью отказов.

4. С увеличением номера периода эксплуатации растёт число повреждений и, соответственно, возрастает интенсивность отказов.

5. Время восстановления (устранения отказа) на каждом периоде эксплуатации является случайным, интенсивность восстановления является постоянной и одной и той же на каждом периоде эксплуатации.

2.1. Диаграмма состояний модели

Для моделирования процессов деградации используются различные подходы и, в частности, моделирование на основе марковских или полумарковских процессов [12, 13]. Так как интенсивность отказов, обусловленных деградацией, может только увеличиться, то процесс деградации часто описывают процессом «чистой гибели».

Диаграмма состояний ОВ приведена на рис. 1. На диаграмме обозначено: D_i – состояние деградации на i-м периоде эксплуатации (i = 1, 2, 3, …), λ_i – интенсивность отказов на i-м периоде эксплуатации, R – восстановление работоспособного состояния отказавшего участка ОК, μ – интенсивность восстановления (определяется временем подъезда ремонтной бригады к месту неисправности и временем ремонта), iT – момент перехода из i-го в (i+1)-й период эксплуатации, отсчитываемый от начала эксплуатации ОК.

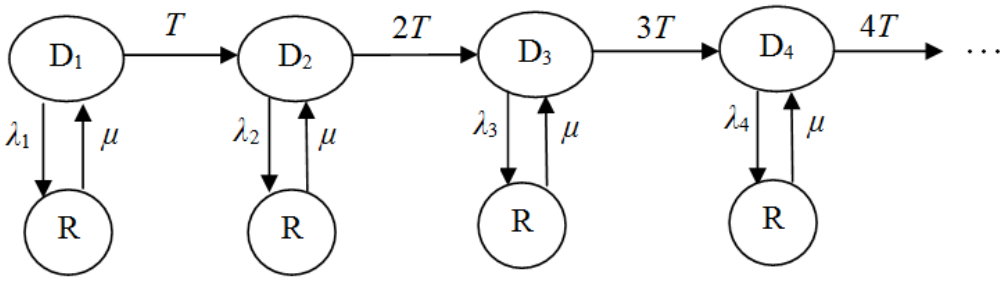

Рис. 1. Диаграмма состояний-переходов ОВ в процессе деградации

2.2. Определение параметров надежности модели

Будем считать, что на каждом периоде эксплуатации имеет место стационарный (установившийся) процесс отказов и восстановлений. В этом случае среднее число отказов в единицу времени на *i*-ом периоде с учётом восстановлений вычисляется по формуле [14]:

$$\omega_i = \lambda_i \cdot \mu / (\lambda_i + \mu). \quad (1)$$

Тогда среднее число отказов на *i*-м периоде эксплуатации равно:

$$n_i = \omega_i \cdot T. \quad (2)$$

Коэффициент готовности и коэффициент неготовности на *i*-м периоде эксплуатации:

$$k_{\text{г}i} = \frac{\mu}{\lambda_i + \mu}; \quad k_{\text{н}i} = \frac{\lambda_i}{\lambda_i + \mu}. \quad (3)$$

Для случая, когда время восстановления пренебрежительно мало (условие $\lambda_i << \mu$), выражения (1) и (2) имеют вид:

$$\omega_i' \approx \lambda_i, \; n_i' \approx \lambda_i \cdot T.$$

Среднее число отказов за *i* периодов:

$$N_i = \sum_{j=1}^{i} n_i = \mu \cdot T \cdot \sum_{j=1}^{i} \frac{\lambda_i}{\lambda_i + \mu}. \quad (4)$$

За *i* периодов эксплуатации суммарное среднее время восстановления составит:

$$T_{\text{в}i} = N_i / \mu = T \cdot \sum_{j=1}^{i} \frac{\lambda_i}{\lambda_i + \mu} \quad (5)$$

Коэффициент неготовности за *i* периодов эксплуатации составит:

$$K_{\text{н}i} = T_{\text{в}i} / (i \cdot T) = \left[\sum_{j=1}^{i} k_{\text{н}i} \right] / i, \quad (6)$$

где $k_{\text{н}i}$ определяется из выражения (3).

На рис. 2 изображен график зависимости $K_{\text{н}}(i)$ при постоянных значениях λ_i и μ = 1/3 (1/ч) [15]. Из рис. 2 видно, что коэффициент неготовности возрастает с увеличением времени эксплуатации ОК.

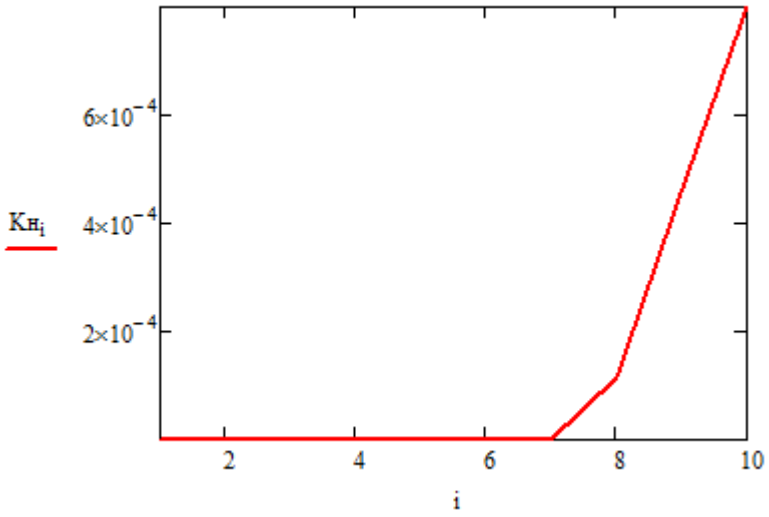

Рис. 2. Зависимость $K_{нi}$ от времени эксплуатации ОК

В табл. 1 представлены значения коэффициента неготовности для интенсивности отказов в зависимости от времени эксплуатации ОК для нагрузки 2.02 ГПа, приведенных в [11]. При этом время эксплуатации разбито на 10 интервалов времени T, равных 3.25 лет. [11]

Таблица 1. Значения коэффициента неготовности оптоволокна в зависимости от интенсивности отказов

Параметр	Значение									
μ, 1/ч	1/3									
i	1	2	3	4	5	6	7	8	9	10
$\lambda_i \cdot 10^{-8}$, 1/ч	2.217	2.389	4.938	5.871	6.716	8.279	10.23	$0.3805 \cdot 10^4$	$1.52 \cdot 10^4$	$2.66 \cdot 10^4$
$K_{нi} \cdot 10^{-8}$	6.651	7.167	14.87	17.61	20.15	24.84	30.69	$1.141 \cdot 10^4$	$4.558 \cdot 10^4$	$7.974 \cdot 10^4$

Из рис. 2 и табл. 1 виден характер зависимости коэффициента неготовности от времени эксплуатации ОК.

3. Заключение

В работе предложена марковская модель для расчета параметров надежности ОК в условиях деградации. Приведена методика определения коэффициента готовности и коэффициента неготовности ОК на различных периодах эксплуатации. Используя данную методику, можно определить момент, когда состояние ОК потребует его замены вследствие превышения коэффициентом неготовности критического значения. Определение критического значения коэффициента неготовности является отдельной технико-экономической задачей.

Литература

1. Network 2030 – A Blueprint of Technology, Applications, and Market Drivers towards the Year 2030 and Beyond // FG-NET-2030. May, 2019.
2. ITU-T FG-NET-2030 Deliverable: New services and capabilities for Network 2030: description, technical gap and performance target analysis, 2019.
3. ITU-T FG-NET-2030 Technical Specification: Network 2030. Architecture Framework, 2020.

4. *Пшеничников А. П.*, *Росляков А. В.* Будущие сети: учебник для вузов. М.: Горячая линия – Телеком, 2021. 300 с.
5. *Saxena J*, *Goel A.* Reliability and Maintainability of Passive optical component // International Journal of Computer Trends and Technology. 2011. V. 21, № l. P. 20–23.
6. *Шувалов В. П.*, *Фокин В. Г.* Оптические сети доступа большого радиуса действия. М.: Горячая линия – Телеком, 2018. 187 с.
7. ГОСТ Р 27.102-2021. Надежность в технике: надежность объекта. Термины и определения. М.: Российский институт стандартизации, 2021. 36 с.
8. *Maslo A., Hodzic M., Skaljo E., Mujcic A.* Aging and degradation of optical fiber parameters in a 16-year-long period of usage // Fiber and Integrated Optics. Feb., 2020. V. 39, № 1. P. 39–52.
9. *Ушаков И. А*. Курс теории надежности систем: учебное пособие для вузов. М.: Дрофа, 2008. 239 с.
10. *Цым А. Ю.* Сроки службы оптических кабелей Анализы. Риски. // Наука и техника. 2020, № 2 (382). С. 20–26.
11. *Ionikova E.*, *Karpov K.*, *Shuvalov V.* Reliability of optical cable under gradual failures taking into account the degree of fiber degradation // Proc. of the XV International scientific and technical conference “Actual problems of electronic instrument engineering” (APEIE-2021), Novosibirsk, 19–21 November, 2021. P. 327–332.
12. *El-Damcese V. A.*, *Temraz N. S.* Availability and reliability measures for multistate system by using Markov reward model // Reliability: Theory and Applications, 2011. V. 6, № 3. P. 68–85.
13. *Kharoufeh J. P., Solo C. J., Ulukus M. Y.* Semi-Markov models for degradation-based reliability // Journal of IIE Transactions. May, 2010. V. 42, № 8. P. 599–612.
14. *Зеленцов Б. П.* Частотный метод моделирования вероятностных систем длительного использования // Вестник СибГУТИ. 2016. № 4. С. 25–38.
15. *Алексеев Е. Б., Гордиенко В. Н., Крухмалев В. В. и др.* Проектирование и техническая эксплуатация цифровых телекоммуникационных сетей. М.: Горячая линия – Телеком, 2008. 392 с.

Статья поступила в редакцию 08.07.2022;
переработанный вариант – 26.07.2022.

Шувалов Вячеслав Петрович
д.т.н., профессор; профессор кафедры ИКСС СибГУТИ (630102, Новосибирск, ул. Кирова, 86), тел. (383) 269-82-43, e-mail: shvp04@mail.ru.

Зеленцов Борис Павлович
д.т.н., профессор кафедры высшей математики СибГУТИ, e-mail: zelentsov@mail.ru.

Квиткова Ирина Геннадьевна
старший преподаватель кафедры ИКСС СибГУТИ, тел. (383) 269-82-44, e-mail: irin.creme@yandex.ru.

Optical fiber reliability model under degradation conditions

Vyacheslav P. Shuvalov
Doctor of technical sciences, Professor, Siberian State University of Telecommunications and Information Science (SibSUTIS, Novosibirsk, Russia), shvp04@mail.ru.

Boris P. Zelencov
Doctor of technical sciences, Professor, Siberian State University of Telecommunications and Information Science (SibSUTIS, Novosibirsk, Russia), zelentsov@mail.ru.

Irina G. Kvitkova
Senior lecturer, Siberian State University of Telecommunications and Information Science (SibSUTIS, Novosibirsk, Russia), irin.creme@yandex.ru.

To calculate the reliability of an optical fiber under degradation conditions, the Markov model taking into account the worsening of fiber characteristics during its operation is proposed. The methodology for calculating the unavailability factor at different operating times is given as well as an example of estimating the unavailability factor.

Keywords: passive optical access network, degradation of fiber, degradation failure, reliability indicators, operating time of fiber.

References

1. Network 2030 – A Blueprint of Technology, Applications, and Market Drivers towards the Year 2030 and Beyond. *FG-NET-2030*, May, 2019.
2. *ITU-T FG-NET-2030 Deliverable: New services and capabilities for Network 2030: description, technical gap and performance target analysis*, 2019.
3. *ITU-T FG-NET-2030 Technical Specification: Network 2030. Architecture Framework*, 2020.
4. Pshenichnikov A.P., Roslyakov A.V. *Budushchie seti* [Future networks]. Moscow, Goryachaya liniya – Telekom, 2021, 300 p.
5. Saxena J, Goel A. Reliability and Maintainability of Passive optical component. *International Journal of Computer Trends and Technology*, 2011, vol. 21, iss. l, pp. 20-23.
6. SHuvalov V.P., Fokin V.G. *Opticheskie seti dostupa bol'shogo radiusa dejstviya* [Long-reach optical access networks]. Moscow, Goryachaya liniya – Telekom, 2018, 187 p.
7. GOST R 27.102-2021. *Nadezhnost' v tekhnike: nadezhnost' ob"ekta. Terminy i opredeleniya* [Reliability in technology: the reliability of the object. Terms and definitions]. Moscow, Rossijskij institut standartizacii, 2021, 36 p.
8. Maslo A., Hodzic M., Skaljo E. and Mujcic A. Aging and degradation of optical fiber parameters in a 16-year-long period of usage. *Fiber and Integrated Optics*, 2020, vol. 39, iss. 1, pp. 39-52.
9. Ushakov I.A. *Kurs teorii nadezhnosti system* [The course of the theory of systems reliability]. Moscow, Drofa, 2008, 239 p.
10. Cym A. YU. Sroki sluzhby opticheskih kabelej. Analizy. Riski [Lifetime of optical cables Analyses. Risks.]. *Nauka i tekhnika*, 2020, no. 2 (382), pp. 20-26.
11. Ionikova E., Karpov K., Shuvalov V. Reliability of optical cable under gradual failures taking into account the degree of fiber degradation. *Proceedings of the XV international scientific and technical conference «Actual problems of electronic instrument engineering» (APEIE-2021)*, Novosibirsk. 19-21 November, 2021, pp. 327-332.
12. El-Damcese V.A., Temraz N.S. Availability and reliability measures for multistate system by using Markov reward model. *Reliability: Theory and Applications*, 2011, vol. 6, iss. 3 (22), pp. 68-85.
13. Kharoufeh J.P., Solo C.J., Ulukus M.Y. Semi-Markov models for degradation-based reliability. *Journal of IIE Transactions*, 2010, vol. 42, iss. 8, pp. 599-612.
14. Zelencov B.P. CHastotnyj metod modelirovaniya veroyatnostnyh sistem dlitel'nogo ispol'zovaniya [Frequency method for modeling probabilistic systems of long-term use]. *Vestnik SibGUTI*, 2016, no. 4, pp. 25-38.
15. Alekseev E.B., Gordienko V.N., Kruhmalev V.V. et al. *Proektirovanie i tekhnicheskaya ekspluataciya cifrovyh telekommunikacionnyh setej* [Design and technical operation of digital telecommunication networks]. Moscow, Goryachaya liniya – Telekom, 2008, 392 p.

УДК 621.396.969
DOI: 10.55648/1998-6920-2022-16-3-62-83

Использование SDR-технологии для задач сетевого позиционирования. Модели приема и обработки опорных сигналов LTE[1]

Г. А. Фокин, Д. Б. Волгушев

Анализ состояния проблемы позиционирования пользовательских устройств UE с использованием инфраструктуры базовых стаций eNB сетей подвижной радиосвязи LTE по открытым зарубежным источникам показывает высокую актуальность и востребованность данного направления исследований. В настоящей работе приводится анализ состояния проблемы, а также формализация моделей приема и обработки опорных сигналов LTE для макета пользовательского устройства, построенного с использованием технологии программно-конфигурируемого радио.

Ключевые слова: 4G, LTE, PSS, SSS, CRS, PRS, SDR, позиционирование.

1. Введение

Анализ состояния проблемы позиционирования пользовательских устройств UE (User Equipment) с использованием инфраструктуры базовых стаций eNB (eNodeB) сотовых сетей подвижной радиосвязи LTE (Long-Term Evolution) показал высокую актуальность и востребованность данного направления исследований в последние годы и нашел отражение в ряде работ отечественных [1–3] и зарубежных [4–6] авторов. Обзор открытых зарубежных источников последних лет по данной тематике [7–40] позволяет выделить отдельное направление исследований в области технологий определения местоположения (ОМП), а именно – использование технологий программно-конфигурируемого радио SDR (Software-defined radio) для задач сетевого позиционирования [41–43]. Интерес к технологиям сетевого ОМП обусловлен, с одной стороны, невозможностью надежного приема сигналов глобальных навигационных спутниковых систем (ГНСС, GNSS – Global Navigation Satellite System) UE в плотной городской застройке в условиях отсутствия прямой видимости NLOS (Non-Line of Sight) [44–46], а с другой стороны, востребованностью сервисов ОМП в различных сценариях [47–50].

Альтернативой ГНСС в условиях городской застройки являются сигналы SOP (Signal of Opportunity), принимаемые из радиоэфира по возможности, например, опорные сигналы сетей радиодоступа LTE. При этом с точки зрения архитектуры системы сетевого позиционирования и степени вовлечения пользовательского устройства и сетевой инфраструктуры (опорных базовых станций и сервера геолокации) в процесс ОМП в настоящей работе рассматривается позиционирование на основе пользовательского устройства (UE-based) без участия сетевой инфраструктуры с обработкой принимаемых от eNB радиосигналов исключительно в устройстве UE. Для решения навигационной задачи пользовательскому устройству необходимы первичные измерения времени прихода сигналов TOA (Time of Arrival), излучаемых базовыми станциями eNB, а для их вторичной обработки UE нужно знать координаты eNB. Координаты

[1] Исследование выполнено при финансовой поддержке Российского научного фонда (грант № 22-29-00528). https://rscf.ru/project/22-29-00528/

eNB можно получить, воспользовавшись открытой базой данных, например, OpenCellid [51]; рис. 1 в качестве примера иллюстрирует экранную форму сервиса OpenCellid с местоположениями базовых станций в геоцентрической системе координат (СК) в формате широты и долготы в районе расположения СПбГУТ им. проф. М. А. Бонч-Бруевича [52].

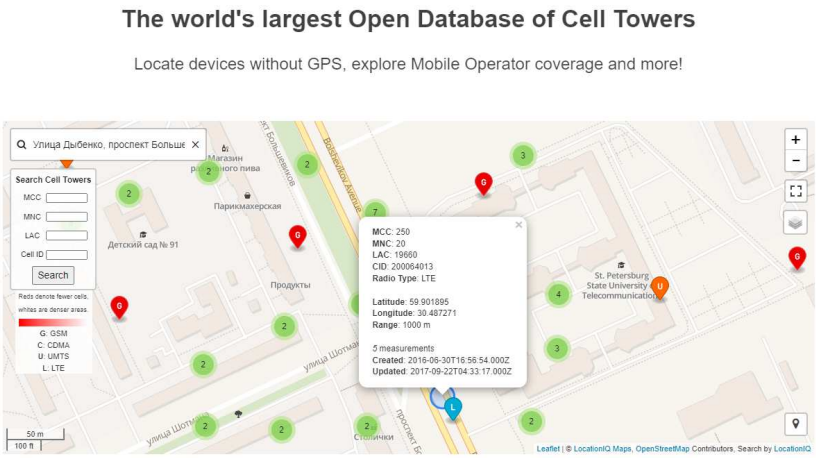

Рис. 1. Экранная форма сервиса OpenCellid

Для оценки координат пользовательского устройства разностно-дальномерным методом [53] в прямоугольной СК относительно базовых станций с известным местоположением в геоцентрической СК выполняется соответствующее преобразование форматов координат [54].

С точки зрения решения задачи ОМП радиотехническими методами сигналы SOP обладают рядом объективных конкурентных преимуществ по сравнению с ГНСС.

Основными преимуществами опорных радиосигналов LTE как частного примера сигналов SOP являются следующие. Во-первых, их изобилие в радиоэфире вследствие широкого радиопокрытия территории сетями LTE [55]. Во-вторых, возможность получения оптимистического геометрического фактора снижения точности GDOP (Geometric Dilution of Precision) вследствие достаточного количества базовых станций eNB, из которых можно выбрать наиболее удачную для ОМП топологию [56, 57]. В-третьих, достаточно высокая, по сравнению с ГНСС, мощность принимаемых сигналов [53]. В-четвертых, достаточно широкая, по сравнению с ГНСС, ширина полосы частот используемых сигналов, что теоретически повышает точность первичных дальномерных измерений по параметру времени прихода сигнала TOA [58]. В-пятых, позиционирование по доступным в радиоэфире сигналам SOP освобождает пользовательское устройство от необходимости быть абонентом сети, по сигналам которой решается навигационная задача, и, соответственно, вносить абонентскую плату; так, опорные сигналы сети LTE могут приниматься всеми устройствами [59]. В-шестых, позиционирование по сигналам SOP может считаться устойчивым к преднамеренному воздействию, так как, например, опорные сигналы LTE излучаются различными операторами в различных диапазонах частот, и, следовательно, подавить их все одновременно достаточно затруднительно [60]. Для верификации решения перечисленных задач широкое распространение в исследовательской среде получил подход программно-конфигурируемого радио SDR [41–43].

Несмотря на перечисленные преимущества, сигналы сотовых сетей радиодоступа LTE изначально разрабатывались не для навигации, а для радиосвязи. Для использования в задачах позиционирования опорных сигналов LTE, излучаемых базовыми станциями eNB, с точки зрения пользовательского устройства UE, являющегося приемником SOP и реализованного средствами SDR, необходимо предварительно решить следующие частные задачи. *Во-первых*, для пользовательского SDR-устройства UE необходимо разработать и программно реализовать специализированные функции приема и обработки SOP для извлечения первичных измерений из наблюдаемых в радиоэфире радиосигналов. *Во-вторых*, пользовательскому SDR-устройству необходимо заблаговременно «узнать» координаты базовых станций eNB, по опорным сигналам которых производятся первичные измерения TOA; однако с учетом

наличия открытых баз данных с известными координатами eNB, например, OpenCellid [51], данная частная задача решаема на уровне приложения UE. *В-третьих*, для пользовательского устройства следует реализовать процедуры вторичной обработки собранных по сигналам SOP первичных измерений с результирующей оценкой координат (ОК) UE при известных координатах eNB. *В-четвертых*, пользовательскому устройству UE необходимо оценить и компенсировать рассинхронизацию излучаемых базовыми станциями eNB сигналов SOP.

В сетях подвижной связи LTE [61, 62] и NR (New Radio) [63] на радиоинтерфейсе используется мультиплексирование с ортогональным частотным разделением OFDM (Orthogonal Frequency Division Multiplexing), а также технологии пространственного мультиплексирования MIMO (Multiple Input Multiple Output) [64, 65]. Для радиоинтерфейса OFDM прием и обработка радиосигналов SOP пользовательским SDR-устройством UE имеет определенную специфику и включает следующие частные подзадачи: а) извлечение из наблюдаемых в радиоэфире OFDM-сигналов SOP-параметров, необходимых для последующего приема и обработки первичных измерений; б) захват и подстройка к OFDM-радиосигналам SOP, излучаемым несколькими базовыми станциями eNB; в) извлечение навигационных параметров – первичных измерений кода, фазы и доплеровского сдвига частоты – из принимаемых OFDM-радиосигналов SOP. Для сбора и обработки первичных навигационных измерений в сетях радиодоступа LTE вместе с сигналами первичной синхронизации PSS (Primary Synchronization Signal) и вторичной синхронизации SSS (Secondary Synchronization Signal) используются специальные опорные сигналы соты CRS (Cell Specific Reference Signal) и специальные опорные сигналы позиционирования PRS (Positioning Reference Signal).

Материал настоящей работы организован далее следующим образом. В разделе 2 приводится анализ состояния проблемы использование SDR-технологии для задач сетевого позиционирования по открытым зарубежным источникам последних лет [7–40]. В разделе 3 рассмотрены проблемы приема сигналов SOP стандарта LTE устройством SDR. В разделе 4 формализованы модели опорных OFDM-сигналов стандарта LTE с целью последующего анализа соответствующих процедур. Раздел 5 содержит выводы и направления дальнейших исследований.

2. Анализ состояния проблемы использование SDR-технологии для задач сетевого позиционирования

На сегодняшний день из анализа открытых зарубежных источников [7–37] можно выделить ряд исследовательских групп, занимающихся вопросами использования SDR-технологии для задач сетевого позиционирования – это группы под руководством J.A. del Peral-Rosado [7–18], K. Shamaei [22–26] и M. Driusso [37–37]. Проведем обзор их основных результатов.

Диссертация J.A. del Peral-Rosado [7] посвящена разработке и экспериментальной апробации алгоритма оценки задержки и характеристики канала применительно к OFDM-сигналам в задачах позиционирования устройств UE сетей LTE в условиях многолучевого распространения радиоволн (РРВ). Одна из первых методологий по оценке точности позиционирования пользовательских устройств в сетях LTE на основе опорных сигналов позиционирования PRS предложена в [8]. Оценка потенциальной точности позиционирования пользовательских устройств UE в сетях LTE посредством обработки сигналов PRS в зависимости от ширины полосы частот и отношения сигнал/шум SNR (Signal to Noise Ratio) и сигнал/(шум+помеха) SINR (Signal to Interference plus Noise Ratio) выполнена в [9]; в частности, средствами имитационного моделирования (ИМ) продемонстрировано, что потенциальная точность первичных дальномерных (ДМ) измерений времени прихода сигнала TOA в терминах нижней границы Крамера–Рао (НГКР) достигает единиц метров в полосе 1.4 МГц при SNR > 10 дБ, а точность оценок координат (ОК) в результате вторичной обработки для сценария из 7 трехсекторных базовых станций зависит от уровня внутрисистемных помех, лежит в пределах от единиц до десятков метров и снижается на границе сот вследствие снижения SINR. Механизм учета погрешности первичных ДМ-измерений при вторичной обработке с оценкой координат в комплексной ИМ описан в [10]. В работе [11] посредством ИМ выполнена оценка влияния

ширины полосы сигнала LTE на точность первичных ДМ-измерений при определении местоположения UE в условиях многолучевого РРВ (MPPB); в частности, показано, что ошибка ДМ-измерений при корреляционной обработке в целом снижается с увеличением ширины полосы частот сигнала LTE с 1.4 до 20 МГц. В работе [12] предложен алгоритм совместной максимально правдоподобной оценки JML (Joint Maximum Likehood) задержки времени прихода и характеристики канала для первичных ДМ-измерений по сигналам PRS. Результаты исследования и разработки этого алгоритма для первичных ДМ-измерений по сигналам PRS описаны в [13], где, в частности, установлено, что он позволяет эффективно разрешать многолучевые компоненты в канале LTE даже с минимальной полосой 1.4 МГц. Одной из первых работ группы под руководством J.A. del Peral-Rosado с экспериментальной апробацией SDR-технологии для задач сетевого позиционирования на базе приемопередающей платы USRP (Universal Software Radio Peripheral) в 2013 году стала публикация [14], в которой рассмотрена архитектура устройства приема и обработки опорных сигналов LTE для определения местоположения UE методом наблюдаемой разности времен прихода сигналов OTDOA (Observed Time Difference of Arrival). Продолжение эксперимента с приемной платой RTL-SDR подтвердила возможность использования доступных SDR-устройств для захвата опорных сигналов LTE с шириной полосы 1.4 МГц в 2014 году [15]. Продолжение экспериментальной апробации SDR-технологии для задач сетевого позиционирования в 2015 году связано с проверкой синхронизации излучающих базовых станций eNB сети LTE макетом пользовательского SDR-устройства UE при условии известного местоположения eNB и UE [16]. В 2016 году предложен механизм синхронизации доступных SDR-плат HackRF по метке времени ГНСС [17]. Лабораторный стенд для эмуляции процедур формирования, передачи, приема и обработки первичных ДМ-измерений по сигналам PRS в сценариях трилатерации в сетях LTE представлен в [18]. Эмуляция сценария первичной и вторичной обработки сигналов PRS в лабораторных условиях подтвердила работоспособность алгоритма совместной максимально правдоподобной оценки JML задержки времени прихода и характеристики канала при работе в полосе 10 МГц для позиционирования устройства LTE с точностью порядка 10 м [19]. В одной из последних работ коллектив авторов под руководством J.A. del Peral-Rosado [20] исследует вопросы позиционирования транспортных средств (ТС) с использованием дорожной инфраструктуры сверхплотных сетей 5G; в частности, средствами ИМ показано достижение точности позиционирования менее одного метра при комплексировании дальномерных TOA и угломерных AOA (Angle of Arrival) измерений с восьмиэлементной антенной решеткой в канале с шириной полосы 10 МГц и расстоянием между соседними базовыми станциями от 40 до 230 м в условиях городской застройки. При использовании ДМ-измерений в канале с шириной полосы 50 МГц достигается точность позиционирования ТС до 30 см [21].

Диссертация K. Shamaei [22] посвящена разработке и экспериментальной апробации алгоритмов приема и обработки опорных радиосигналов SOP стандартов LTE и 5G NR для сетевого позиционирования пользовательских устройств в условиях отсутствия сигналов ГНСС. Комплексное устройство приема и обработки опорных радиосигналов LTE для сетевого позиционирования запатентовано в 2021 году [23]. Одной из первых работ K. Shamaei по оценке точности сетевого позиционирования на основе SDR-устройства приема и обработки сигналов LTE является исследование [24]; результаты эксперимента с использованием SDR-макета UE, расположенного на борту ТС, показали среднее смещение первичных ДМ-измерений ~12 м со среднеквадратическим отклонением (СКО) ~7 м на интервале движения ТС в ~1.5 км. Сравнение точности первичных измерений в сетях LTE на основе сигналов SSS и CRS выполнено в [25]; в частности, представлены архитектуры устройства приема и обработки сигналов SSS и CRS; прием сигналов CRS служит для уточнения грубой оценки TOA, полученной по сигналам SSS; оценка времени прихода по сигналам CRS осуществляется по характеристике канала в частотной области; СКО ОК UE составило ~50 м по сигналам SSS и ~9 м по сигналам CRS. В работе [26] представлен экспериментальный анализ точности ДМ-измерений по сигналам SSS в условиях отсутствия прямой видимости NLOS, построенный на основе приемопередающей платы USRP и алгоритмов обработки, программно реализованных в Matlab; показано

различие влияния многолучевости на результаты обработки радиотехнических сигналов спутниковых GPS и наземных LTE-систем позиционирования. Эффективное с вычислительной точки зрения устройство приема и обработки опорных сигналов LTE в условиях МРРВ описано в [27]; в частности, предложенный контур подстройки по задержке DLL (Delay-Locked Loop) показал устойчивость к МРРВ и СКО ОК UE ~5 м на интервале движения ТС в ~1.5 км. Процедуры сбора первичных ДМ-измерений посредством обработки сигналов SSS с помощью дискриминатора для условий LOS и NLOS формализованы и экспериментально апробированы в [28]. В [29] предложено устройство приема и обработки опорных сигналов LTE на основе контура DLL с поддержкой фазовой автоподстройки частоты (ФАПЧ, PLL – Phased Lock Loop); экспериментальная апробация показала СКО ОК UE ~ 3 м на интервале движения ТС в ~1.5 км. Теоретические основы и практические результаты использования опорных сигналов LTE в задачах сетевого позиционирования систематизированы в [30]; экспериментальная апробация показала СКО ОК UE ~ 5 м в условиях NLOS. Комплексирование первичных ДМ-измерений по параметрам кода и фазы несущей опорных радиосигналов LTE вместе с инерциальными измерениями в расширенном фильтре Калмана (РФК, EKF – Extended Kalman Filter) для сценария внутри помещений показало СКО ОК UE ~ 3 м [31]. В [32] обоснован выигрыш в точности ОК при сборе и обработке первичных ДМ-измерений по опорным сигналам в сетях LTE за счет калмановской фильтрации коррелированных ошибок, образованных в условиях МРРВ. Исследование [33] посвящено комплексированию радиотехнических (GNSS+SOP LTE) и инерциальных (IMU – Inertial Measurement Unit) первичных измерений, а также их сопоставлению с данными видеоаналитики на основе цифровых карт; для комплексирования используется РФК; результаты эксперимента показали СКО ОК UE в 2.8 м с приемом сигнала ГНСС и 3.1 м без ГНСС на интервале движения ТС в ~1.4 км. Работы последних лет [34, 35] посвящены вопросам приема и обработки сигналов стандарта 5G NR для задач позиционирования. Так, в [34] формализована структура сигналов 5G NR, после чего представлено SDR-устройство их приема и обработки на базе платы USRP; СКО ОК UE составило ~15 м на интервале движения ТС в ~1 км. В [35] после исключения рассинхронизации базовых станций gNB (gNodeB) сети 5G результаты эксперимента показали уже СКО ОК UE ~1 м. В одной из последних работ коллектив авторов под руководством K. Shamaei [36] экспериментально апробирует структуру устройства приема, обработки и комплексирования дальномерных (TOA) и угломерных (AOA) измерений для позиционирования.

Работы авторов под руководством M. Driusso [37–39] посвящены экспериментальной апробации процедур приема и обработки опорных сигналов CRS SDR-устройством USRP для позиционирования в сетях LTE. В [37] обосновывается возможность приема сигналов CRS различных операторов «на лету» без регистрации в сети соответствующего оператора; СКО ОК UE составила ~43 м. Использование алгоритма ESPRIT (Estimating Signal Parameters via Rotational Invariance Techniques) для оценки времени прихода TOA по сигналам CRS позволило получить СКО ОК UE от 9 до 123 м в [38] и до ~31 м в [39].

К сожалению, на сегодняшний день в открытых отечественных источниках отсутствуют исследования, подобные проанализированным выше. Настоящая работа является продолжением исследования [41], открывает цикл из трех публикаций, посвященных подсистеме приема и обработки опорных сигналов LTE в задачах ОМП UE, и имеет своей конечной целью разработку и экспериментальную апробацию отечественной SDR-технологии сетевого позиционирования. Целью настоящего цикла является разработка подсистемы приема и обработки опорных сигналов LTE для сбора первичных измерений времени прихода сигнала TOA. Частной задачей настоящей публикации является формализация моделей приема и обработки опорных сигналов LTE с целью последующего анализа соответствующих процедур, их программной реализации и экспериментальной апробации на SDR-макете.

3. Проблемы приема опорных сигналов стандарта LTE устройством SDR

При реализации SDR-устройства приема и обработки OFDM-радиосигналов SOP стандарта LTE для решения задач сетевого позиционирования встают следующие проблемы [22]. *Первая проблема* заключается в одновременном приеме сигналов первичной синхронизации PSS от нескольких базовых станций eNB. Коэффициент повторного использования частот в сетях LTE равен единице и OFDM-сигналы PSS, излучаемые разными eNB, занимают в частотно-временной структуре кадра одинаковые ресурсные элементы. Поэтому при одновременном приеме нескольких опорных OFDM-сигналов PSS от разных eNB в тракте приема UE будут наблюдаться внутрисистемные помехи. Вследствие внутрисистемных помех SDR-приемник UE сможет достоверно обнаружить и принять только самый сильный OFDM-сигнал PSS, излучаемый той eNB, которая расположена наиболее близко к UE. Это обстоятельство объясняется затуханием сигнала при распространении радиоволн и известным эффектом «ближе-дальше», когда OFDM-сигналы PSS от удаленных базовых станций будут подавлены сигналом от близко расположенной eNB. Если для радиосвязи данное обстоятельство не является критичным, то для позиционирования UE на плоскости или в пространстве с использованием метода наблюдаемой разности времен прихода сигналов OTDOA пользовательскому устройству необходимо одновременно вести прием не менее трех или четырех опорных OFDM-сигналов PSS соответственно. За счет корреляционных свойств сигналов первичной синхронизации практически реализуемым оказывается одновременный прием порядка трех наиболее сильных сигналов PSS. Что касается одновременного приема более трех сигналов PSS, что крайне желательно в задачах позиционирования, то это представляет определенную техническую сложность. Таким образом, *вторая проблема* заключается в ограниченном числе одновременно принимаемых сигналов, по которым могут осуществляться первичные навигационные измерения. Для исключения этой проблемы при сборе первичных измерений пользовательским устройством UE могут использоваться другие опорные сигналы, например, CRS или PRS, однако для их приема и обработки UE должно по протоколам верхних уровней заблаговременно получить следующие параметры: идентификатор соты Cell ID, ширину полосы частот и число антенн на передающей стороне базовой станции eNB. Если прием опорных сигналов LTE ведет пользовательское устройство UE, являющееся абонентом данной сети LTE, тогда ему данные параметры известны. Однако для приема сигналов SOP SDR-устройству UE по возможности необходимо самостоятельно «на лету» определять данные параметры из принимаемых в радиоэфире опорных сигналов. Таким образом, *третья проблема* заключается в необходимости извлечения «на лету» параметров Cell ID, ширины полосы частот и числа антенн eNB. После приема опорных сигналов, например, CRS, SDR-устройству UE необходимо оценить их время прихода TOA. Известны различные алгоритмы и методики оценки параметра времени прихода TOA по принимаемым OFDM-сигналам LTE: совместная оценка канала и задержки [12], алгоритмы сверхразрешения [37, 37] и пороговые алгоритмы [37, 40]. Данные подходы характеризуются либо высокой вычислительной сложностью реализации, либо низкой точностью оценки TOA. Таким образом, *четвертая проблема* заключается в реализации алгоритма измерения времени прихода по принимаемым OFDM-сигналам LTE с требуемой точностью оценки TOA и допустимой вычислительной сложностью. Одним из основных источников погрешностей при решении навигационной задачи SDR-устройством UE является временная рассинхронизация излучаемых базовыми станциями eNB OFDM-радиосигналов. Исключить эффект рассинхронизации eNB можно в лабораторных условиях путем эмуляции синхронного излучения OFDM-радиосигналов LTE [14], однако на практике базовые станции не могут быть синхронизированы идеально. Другим подходом к решению проблемы рассинхронизации базовых станций является оценка и компенсация временной расстройки моментов излучения радиосигналов eNB посредством постобработки с использованием известных дальномерных измерений TOA, полученных по сигналам ГНСС [37], однако данный подход непрактичен в системах позиционирования подвижных устройств в режиме

реального времени. Таким образом, *пятая проблема* заключается в необходимости реализации алгоритма оценки и компенсации рассинхронизации eNB «на лету».

Далее рассмотрим модель опорных OFDM-сигналов LTE согласно 3GPP TS 36.211 [61] и 3GPP TS 36.212 [62].

4. Модели опорных сигналов стандарта LTE

Для использования опорных сигналов SOP стандарта LTE в задачах позиционирования SDR-устройством «на лету» следует формализовать модель этих OFDM-сигналов на физическом уровне. В контексте решения навигационной задачи по сигналам SOP SDR-устройство UE, которое не является абонентом сети LTE, должно «на лету» принимать опорные сигналы сети LTE из радиоэфира и извлекать из них первичные измерения времени прихода сигнала TOA. Формат опорных сигналов стандарта LTE известен и определен в спецификации 3GPP TS 36.211 [61]. Зная формат опорных сигналов, можно обосновать выбор структуры SDR-приемника, который будет решать задачу сбора первичных измерений TOA по сигналам SOP с необходимыми показателями по точности и реализуемыми требованиями по вычислительной сложности. В разделе 4.1 рассмотрена структура формируемого OFDM-сигнала LTE на физическом уровне. В разделе 4.2 представлен анализ применимости опорных сигналов LTE для сбора первичных измерений «на лету» по сигналам SOP. В разделе 4.3. формализованы модели опорных сигналов SSS и CRS для сбора первичных измерений в сетях стандарта LTE.

4.1. Структура OFDM-кадра LTE на физическом уровне

При OFDM-модуляции в стандарте LTE передаваемые символы отображаются на поднесущие с разносом $\Delta f = 15\,\text{кГц}$. Если предположить, что все N_r поднесущих при OFDM-модуляции выделяются для передачи данных, то последовательный поток символов данных на входе OFDM-модулятора должен быть предварительно разделен на группы по N_r символов для их последующего отображения на N_r поднесущих. Отображение символов на поднесущие зависит от структуры кадра LTE. Для снижения внутрисистемных помех по соседнему частотному каналу в сигналах OFDM используются защитные полосы, образованные поднесущими, на которых полезные символы данных не передаются. Данные защитные полосы образованы неиспользуемыми защитными поднесущими по обеим сторонам спектра относительно используемых N_r поднесущих, на которых передаются полезные символы данных. Из общего числа N_c поднесущих N_r используются для передачи символов данных, а $N_c - N_r$ заполняются нулями. В радиоинтерфейсе LTE нулевая DC (Direct Current) поднесущая также не используется для передачи данных. После отображение N_r символов данных и дополнения их нулями до N_c полученная в частотном домене группа из N_c поднесущих поступает на блок обратного быстрого преобразования Фурье (ОБПФ, IFFT – Inverse Fast Fourier Transform). На выходе блока ОБПФ получается последовательный поток OFDM-символов во временном домене; длительность OFDM-символа равна $T_{symb} = 1/\Delta f$. Последние L_{CP} элементов каждого OFDM-символа повторяются в его начале и образуют так называемый циклический префикс (ЦП, CP – Cyclic Prefix), который служит для компенсации межсимвольной интерференции (МСИ, ISI – Intersymbol Interference), являющейся результатом многолучевого распространения радиоволн (РРВ). Рис. 2. иллюстрирует обобщенную структурную схему формирования OFDM-сигнала стандарта LTE на передающей стороне. Для восстановления переданных символов на приемной стороне описанные выше процедуры следует выполнить в обратном порядке. Так как коэффициент повторного использования частот в сетях радиодоступа LTE равен единице, все базовые станции eNB данного оператора используют единственную выделенную ему полосу частот. Для снижения внутрисистемных помех при работе базовых

станций с разными Cell ID в общей полосе частот их сигналы ортогонализируются посредством кодового разделения. При использовании отдельного частотного канала базовые станции другого оператора могут использовать те же Cell ID. Общее число поднесущих N_c в кадре LTE и число используемых поднесущих N_r однозначно определяются оператором в зависимости от ширины частного канала. Таблица 1 содержит параметры общего N_c и используемого N_r числа поднесущих для каждого значения ширины полосы выделенного частотного канала стандарта LTE. Занимаемая ширина полосы частотного канала определяется как $W = N_r \cdot \Delta f$ и оказывается меньше выделенной полосы частотного канала стандарта LTE.

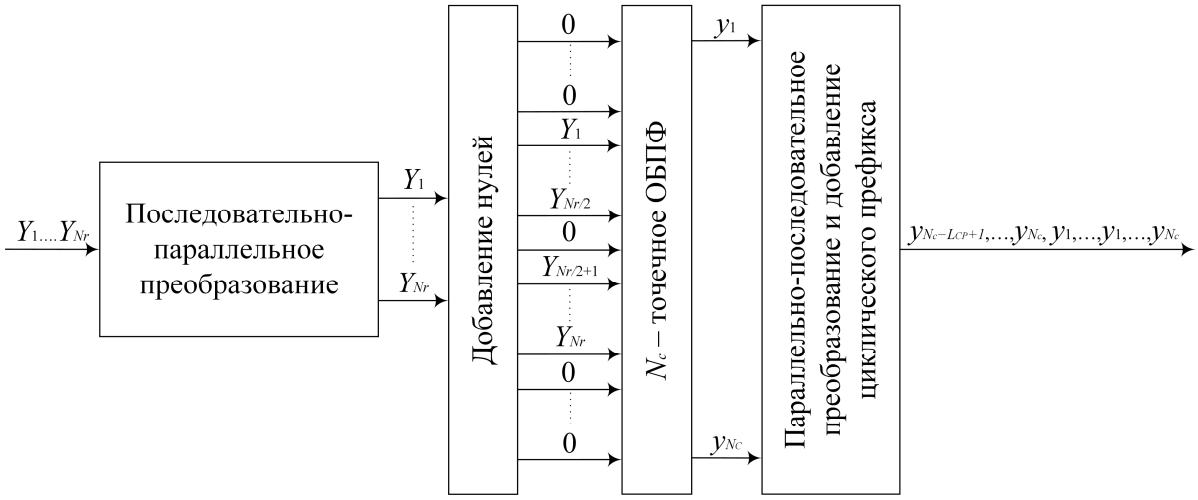

Рис. 2. Структурная схема формирования OFDM-сигнала

OFDM-символы на выходе схемы формирования группируются в кадры длительностью $T_f = 10$ мс. В стандарте LTE структура кадра зависит от режима дуплексирования; различают частотный FDD (Frequency Division Duplexing) и временной TDD (Time Division Duplexing) дуплекс. По ряду причин, в числе которых меньшая задержка и большая дальность радиосвязи, наибольшее распространение в сетях LTE получил частотный дуплекс, поэтому далее рассматривается структура кадра для режима FDD [22].

Таблица 1. Параметры физических ресурсных блоков

Выделенная / занимаемая полоса, МГц	**Число ресурсных блоков**	**Общее число поднесущих N_c**	**Используемые поднесущие N_r**	**Частота дискретизации, МГц**	**Размерность БПФ**
1.4 / 1.08	6	128	72	1.92	128
3 / 2.7	15	256	180	3.84	256
5 / 4.5	25	512	300	7.68	512
10 / 9.0	50	1024	600	15.36	1024
15 / 13.5	75	1536	900	30.72	2048
20 / 18.0	100	2048	1200	30.72	2048

Кадр длительностью 10 мс состоит из 10 субкадров длительностью 1 мс или 20 слотов длительностью 0.5 мс. Слот, в свою очередь, в частотно-временном домене можно рассмотреть в терминах ресурсной сетки RG (Resource Grid), которая образована несколькими ресурсными блоками RB (Resource Block). Ресурсные блоки RB, в свою очередь, состоят из простейших единиц ресурсной сетки – ресурсных элементов RE (Resource Element). Каждый ресурсный элемент RE характеризуется своим индексом поднесущей k в частотной области и номером OFDM-символа i во временной области.

Рис. 3. иллюстрирует структуру кадра стандарта LTE в режиме FDD. Рис. 4. иллюстрирует развернутую структуру кадра стандарта LTE в режиме FDD для полосы 1.4 МГц: число поднесущих $N_r = 72$. В частотном домене опорные сигналы PSS и SSS передаются на 62 центральных поднесущих; во временном домене для передачи опорных сигналов PSS выделяется седьмой (последний) OFDM-символ слотов 0 и 10; во временном домене для передачи опорных сигналов SSS выделяется шестой (предпоследний) OFDM-символ слотов 0 и 10. Опорные сигналы соты CRS распределены по поднесущим и слотам в пределах всей частотно-временной структуры кадра; распределение опорных сигналов CRS зависит от идентификатора соты Cell ID и номера OFDM-символа.

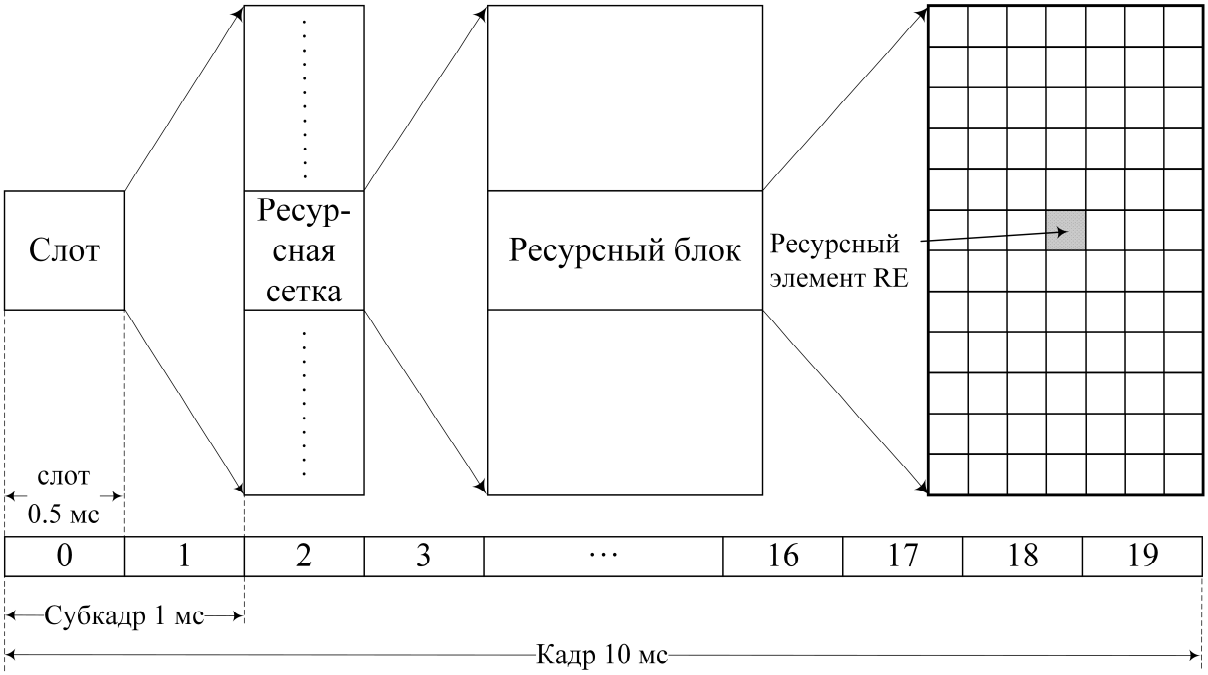

Рис. 3. Структура кадра стандарта LTE в режиме FDD

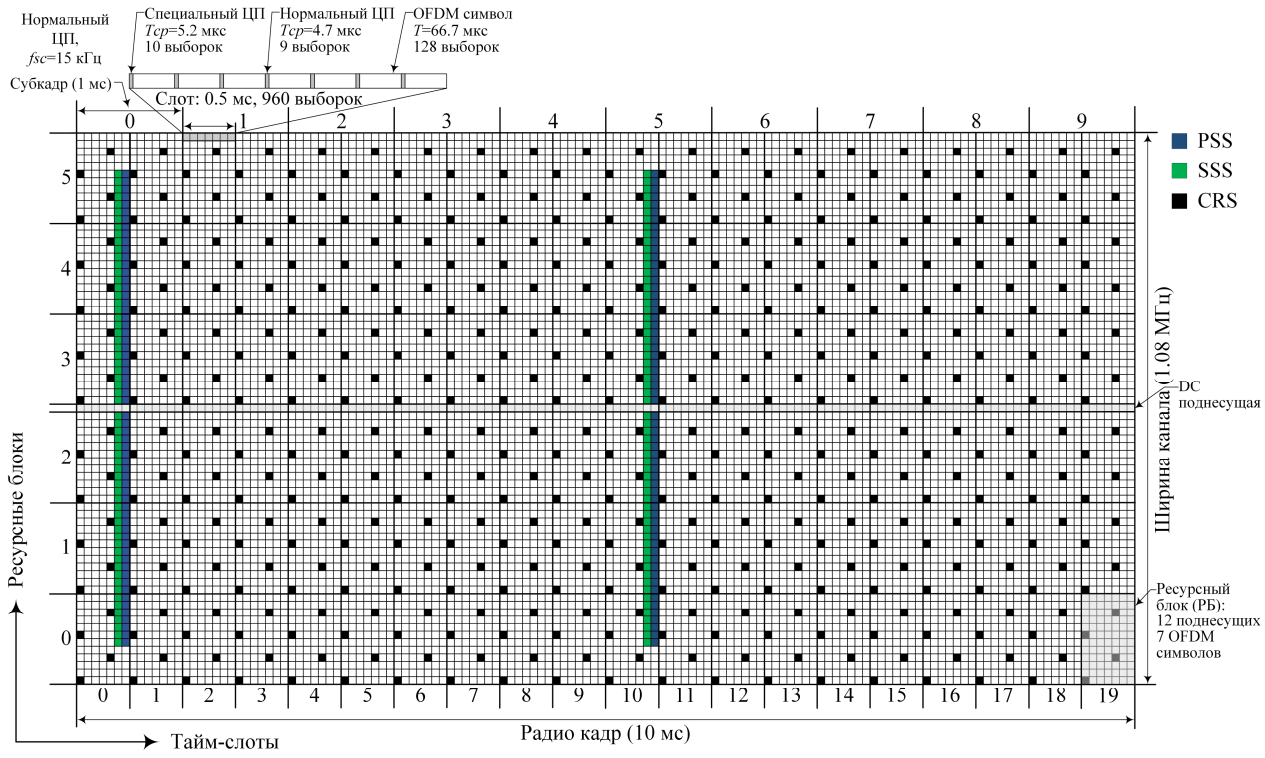

Рис. 4. Развернутая структура кадра стандарта LTE в режиме FDD для полосы 1.4 МГц

Так как каждый сигнал данных стандарта LTE отображается на строго определенный частотно-временной ресурс внутри кадра, пользовательское устройство UE для извлечения интересующих его данных должно предварительно преобразовать принимаемый OFDM-сигнал в структуру кадра. Для этого необходимо сначала определить время начала кадра. Начало кадра определяется пользовательским устройством UE по опорным первичным PSS и вторичным SSS сигналам синхронизации, передаваемым в каждом кадре LTE. UE определяет начало кадра LTE путем нахождения пика корреляционной функции (КФ) принимаемого сигнала с локально генерируемой копией сигналов PSS и SSS. Зная начало кадра LTE, приемник UE может далее исключить циклический префикс CP и взять быстрое преобразование Фурье (БПФ, FFT – Fast Fourier Transform) каждого из N_c символов: длительность нормального ЦП равна 5.21 мкс в первом OFDM-символе каждого слота и 4.69 мкс в остальных OFDM-символах слота (рис. 4.).

4.2. Анализ применимости опорных сигналов LTE для сбора первичных измерений

Для сбора первичных дальномерных измерений времени прихода сигнала TOA путем корреляционной обработки могут использоваться следующие последовательности опорных сигналов физического уровня стандарта LTE.

CP. Циклический префикс служит для компенсации МСИ, являющейся результатом многолучевого РРВ. Последовательность ЦП длиной L_{CP} выборок повторяет последние L_{CP} выборок каждого OFDM-символа в начале этого OFDM-символа. Таким образом, при вычислении КФ принятых L_{CP} выборок ЦП в начале OFDM-символа с L_{CP} выборками ЦП в конце OFDM-символа можно оценить частотно-временную расстройку принятого сигнала [66].

PSS. Для обеспечения символьной синхронизации опорные сигналы PSS передаются в последнем (седьмом) символе слота 0 и повторяются в последнем символе слота 10. Сигнал PSS представляет собой последовательность Задова–Чу длиной 62, символы которой располагаются в 62 центральных поднесущих выделенной полосы пропускания, исключая нулевую поднесущую DC. Опорные сигналы PSS передают только три возможных кодовых последовательности, которые соответствуют целочисленному значению идентификатора соты в пределах группы $N_{ID}^{(2)}$; $N_{ID}^{(2)}$ определяет сектор соты eNB и может принимать три значения: $N_{ID}^{(2)} \in \{0,1,2\}$.

SSS. Опорный сигнал SSS представляет собой ортогональную последовательность длиной 62, которая передается в предпоследнем символе слотов 0 и 10 и располагается в тех же поднесущих, что и PSS. Последовательность SSS получается объединением двух последовательностей максимальной длины 31 с последующим скремблированием третьей ортогональной последовательностью, которая формируется на основе идентификатора соты в пределах группы $N_{ID}^{(2)}$. Существует 168 различных последовательностей SSS, которые соответствуют целочисленному значению идентификатора группы $N_{ID}^{(1)}$; $N_{ID}^{(1)}$ определяет группу сот и может принимать 168 значений: $N_{ID}^{(2)} \in \{0,\ldots,167\}$. После оценки $N_{ID}^{(1)}$ и $N_{ID}^{(2)}$ можно определить уникальный идентификатор соты Cell ID N_{ID}^{Cell} базовой станции eNB:

$$N_{ID}^{Cell} = 3N_{ID}^{(1)} + N_{ID}^{(2)}. \quad (1)$$

CRS. Сигнал CRS служит для оценки характеристики канала и передается в ресурсных элементах, которые распределены в пределах всего частотно-временного домена кадра. Последовательность опорного сигнала CRS формируется на основе идентификатора соты

N_{ID}^{Cell}, номера выделенного OFDM-символа, слота и антенного порта таким образом, что последовательности опорных сигналов CRS разных базовых станций eNB ортогональны друг другу. Идентификатор соты N_{ID}^{Cell} определяет выделенные поднесущие для опорного сигнала CRS данной базовой станции. Обозначим через $S_i(k)$ сигнал CRS, передаваемый на k-й поднесущей в i-м OFDM-символе, где $k = m\Delta_{CRS} + \kappa$, $m = 0,\ldots,M-1$, $M = \lfloor N_r / \Delta_{CRS} \rfloor$, $\Delta_{CRS} = 6$ и κ – это постоянный сдвиг, определяемый идентификатором соты N_{ID}^{Cell} и номером символа i; далее в тех случаях, когда результат не зависит от индекса i, номер символа i будем опускать.

PRS. Сигнал PRS был предложен в 9-м релизе LTE, служит для сбора первичных измерений при позиционировании разностно-дальномерным методом (РДМ) OTDOA и передается в ресурсных элементах, которые распределены в пределах всего частотно-временного домена кадра. Централизованное распределение ортогональных в частотно-временном домене ресурсных элементов RE сигналам PRS, передаваемых одновременно соседними базовыми станциями eNB, обеспечивает отсутствие внутрисистемных помех при сборе первичных ДМ-измерений пользовательским устройством UE. Точность позиционирования по сигналам PRS составляет порядка 50 м [67].

Все перечисленные выше последовательности опорных сигналов, за исключением PRS, транслируются базовыми станциями eNB в каждом кадре в режиме широковещания независимо от наличия в зоне обслуживания eNB пользовательских устройств UE, являющихся абонентами сети LTE данного оператора. Поэтому широковещательные опорные сигналы CP, PSS, SSS и CRS сетей LTE разных операторов можно использовать для целей позиционирования «на лету» пользовательскими устройствами UE, не являющимися абонентами сети LTE какого-либо отдельного оператора. Несмотря на применимость в задачах сетевого позиционирования всех перечисленных сигналов, наиболее подходящими для сбора первичных ДМ-измерений являются опорные сигналы SSS и CRS. Сформулируем основные проблемы использования опорных сигналов CP, PSS и PRS в задачах сетевого позиционирования «на лету».

Проблема использования CP для оценки времени прихода сигнала TOA заключается в большой ошибке ДМ-измерений в условиях многолучевого РРВ; также циклические префиксы CP различных eNB неортогональны, что препятствует одновременному сбору первичных ДМ-измерений от нескольких базовых станций.

Проблема использования PSS для задач позиционирования заключается в том, что число первичных ДМ-измерений при работе устройства UE в одном диапазоне частот ограничено тремя допустимыми последовательностями опорных сигналов первичной синхронизации PSS.

Проблема использования PRS заключается в следующем. Во-первых, при выделении в кадре LTE специальных сигналов позиционирования нарушается конфиденциальность пользователя, так как при использовании UE сигналов PRS оценка его местоположения становится известна оператору [68]. Во-вторых, ОМП по сигналам PRS доступно исключительно абонентам сети LTE данного оператора. В-третьих, при сетевом позиционировании по сигналам PRS другие доступные опорные сигналы других операторов оказываются недоиспользованными. В-четвертых, выделение ресурсных элементов в частотно-временном домене под передачу специальных опорных сигналов позиционирования PRS приводит к уменьшению полезной нагрузки кадра, которая могла бы использоваться для передачи полезных данных трафика. Для исключения перечисленных недостатков бо́льшой интерес в задачах сетевого позиционирования представляют подходы, основанные на использовании сигналов CRS. Далее рассматриваются модели приема сигналов SSS и CRS для сбора первичных ДМ-измерений.

4.3. Модели опорных сигналов LTE для сбора первичных измерений

4.3.1. Модель приема опорных сигналов SSS для сбора первичных измерений

Обозначим через $S_{sss}(f)$ последовательность переданного опорного вторичного сигнала синхронизации SSS в частотном домене. Допустим, опорный сигнал SSS передается один раз (в 0-м или 10-м слоте) за время передачи кадра. Тогда, взяв обратное преобразование Фурье IFT (Inverse Fourier Transform) от $S_{sss}(f)$, получим последовательность переданного опорного сигнала SSS $s_{sss}(t)$ во временном домене:

$$s_{sss}(t)=\begin{cases}\mathrm{IFT}\{S_{sss}(f)\}, & t\in(0,T_{symb})\\ 0, & t\in(T_{symb},T_f)\end{cases}, \tag{2}$$

где $T_{symb}=1/\Delta f$ – длительность одного OFDM-символа, а $T_f=10$ мс – длительность кадра.

Принятый опорный сигнал SSS обрабатывается блоками, каждый из которых занимает длительность кадра. Допустим, опорный сигнал SSS передается в модели радиоканала с аддитивным белым гауссовским шумом (АБГШ, AWGN – Additive White Gaussian Noise), тогда принятый опорный сигнал SSS во временном домене можно представить выражением [22]:

$$r_{sss}(t)=\sqrt{C}e^{j(2\pi f_D t+\phi)}\cdot\left[s_{code}\left(t-t_{TOA_k}-kT_f\right)+d\left(t-t_{TOA_k}-kT_f\right)\right]+n(t),\quad \text{при}\, kT_f\le t\le(k+1)T_f,\ k=0,1,2,\ldots, \tag{3}$$

где k – номер кадра; C – мощность принятого сигнала, включая коэффициенты усиления (КУ) антенн и потери в антенно-фидерном тракте (АФТ); t_{TOA} – время прихода опорного сигнала SSS; ϕ – фаза несущей опорного сигнала SSS; f_D – сдвиг несущей частоты вследствие эффекта Доплера, рассинхронизации опорных генераторов передатчика и приемника по частоте и фазе; $n(t)$ – выборка АБГШ с постоянной спектральной плотностью мощности (СПМ) $N_0/2$ Вт/Гц; $d(t)$ – данные, передаваемые eNB в канале вниз, отличные от опорного сигнала SSS; при этом с точки зрения первичных ДМ-измерений времени прихода сигнала TOA на интервале длительности OFDM-символа T_{symb} для данных, отличных от опорного сигнала SSS, справедливо:

$$d(t)=0 \text{ при } t\notin(t_{TOA},t_{TOA}+T_{symb}). \tag{4}$$

Последовательность опорного сигнала SSS определяется выражением:

$$s_{code}(t)=\sqrt{\frac{T_f}{W_{SSS}}}s_{sss}(t), \tag{5}$$

где $W_{SSS}=945$ кГц – ширина полосы опорного сигнала SSS [22].

4.3.2. Модель приема опорных сигналов CRS для сбора первичных измерений

Обозначим через $Y_i(k)$ сигнал, переданный на *k*-й поднесущей в *i*-м OFDM-символе, тогда условие наличия опорного сигнала CRS в $Y_i(k)$ можно представить выражением:

$$Y_i(k)=\begin{cases} S_i(k), & k \in N_{CRS} \\ D_i(k), & \text{при остальных } k \end{cases}, \tag{6}$$

где N_{CRS} обозначает набор поднесущих, содержащих опорные сигналы CRS, а $D_i(k)$ обозначает другие, отличные от опорных сигналов CRS, передаваемые данные.

Допустим, опорный сигнал CRS передается в модели многолучевого радиоканала с замираниями, который на интервале передачи одного OFDM-символа характеризуется импульсной характеристикой канала CIR (Channel Impulse Response):

$$h_i(\tau)=\sum_{l=0}^{L-1}\alpha_{i,l}\delta\left(\tau-\tau_{i,l}\right), \tag{7}$$

где i – номер OFDM-символа; L – число многолучевых компонент (МЛК); $\alpha_{i,l}$ и $\tau_{i,l}$ – ослабление и задержка *l*-й МЛК относительной первой МЛК; $\delta(\cdot)$ – дельта-функция Дирака. Будем считать, что первая МЛК с индексом $l=0$ является компонентой LOS и характеризуется параметрами $\alpha_{i,0}=1$ и $\tau_{i,0}=0$. Тогда принятый опорный сигнал CRS после исключения циклического префикса и взятия БПФ в условиях идеальной синхронизации можно представить в частотном домене следующим выражением [22]:

$$R_i(k)=\sqrt{C}Y_i(k)H_i(k)+W_i(k),\ k=0,\ldots,N_c-1, \tag{8}$$

где $W_i(k)\sim\mathcal{CN}\left(0,\sigma^2\right)$; выражение $\mathcal{CN}(a,b)$ обозначает комплексное нормальное распределение с математическим ожиданием a и дисперсией b. Частотная характеристика канала CFR (Channel Frequency Response) $H_i(k)$, полученная на основе опорных сигналов CRS, в частотном домене определяется следующим выражением [22]:

$$H_i(k)=\sum_{l=0}^{L-1}\alpha_{i,l}e^{-j2\pi\tau_{i,l}k/T_{symb}}. \tag{9}$$

Как правило, существует несоответствие между оценкой начала времени приема символов и фактическим началом символа, что может быть связано с неидеальной синхронизацией по времени и частоте вследствие временных и частотных рассогласований в приемопередающем тракте, а также доплеровским сдвигом несущей частоты вследствие движения UE. Допустим, рассогласование по времени не превышает длительности циклического префикса, тогда модель принятого сигнала CRS в *i*-м OFDM-символе можно представить выражением [69–71]:

$$R_i(k)=e^{j\pi e_f}e^{j2\pi(iN_t+L_{CP})e_f/N_c}e^{j2\pi e_\tau k/N_c}\sqrt{C}Y_i(k)H_i(k)+W_i(k),\ k=0,\ldots,N_c-1, \tag{10}$$

где $N_t=N_c+L_{CP}$, $e_f=f_D/\Delta f$ и $e_\tau=\left(\hat{t}_{TOA}-t_{TOA}\right)/T_s$ – ошибка символьной синхронизации, нормированная периодом дискретизации $T_s=T_{symb}/N_c$. Первые две экспоненты в представленном выше выражении $e^{j\pi e_f}e^{j2\pi(iN_t+L_{CP})e_f/N_c}$ моделируют эффект частотной рассинхронизации, а третья экспонента $e^{j2\pi e_\tau k/N_c}$ моделирует эффект символьной/временной рассинхронизации. Строго говоря, для каждой поднесущей OFDM-сигнала значение доплеровского сдвига отличается вследствие различных номиналов поднесущих частот, однако для простоты

будем считать, что доплеровский сдвиг определяется относительно номинала центральной несущей радиочастоты f_c.

5. Заключение

В настоящей работе выполнен анализ состояния проблемы использования SDR-технологии для задач сетевого позиционирования, проанализированы проблемы приема опорных сигналов стандарта LTE устройством SDR, а также формализованы модели опорных сигналов стандарта LTE с целью последующего анализа соответствующих процедур, их программной реализации и экспериментальной апробации на SDR-макете. Далее планируется рассмотреть структуру устройства приема и обработки опорных OFDM-сигналов SOP стандарта LTE для сбора первичных измерений TOA, специфика процедур выполнения которых заключается в необходимости извлечения первичных разностно-дальномерных измерений для последующего их использования в задачах сетевого позиционирования.

Литература

1. *Фокин Г. А.* Технологии сетевого позиционирования. Санкт-Петерб.: СПбГУТ, 2020. 558 с.
2. *Фокин Г. А.* Технологии сетевого позиционирования 5G. М.: Горячая Линия – Телеком, 2021. 456 с.
3. *Фокин Г. А.* Комплекс моделей и методов позиционирования устройств в сетях пятого поколения. Диссертация на соискание ученой степени доктора технических наук: 05.12.13. Санкт-Петербург. 2021. 499 с.
4. *Zekavat R., Buehrer R. M.* Handbook of position location: Theory, practice and advances. John Wiley & Sons, 2019. 1376 p.
5. *Campos R. S., Lovisolo L.* RF Positioning: Fundamentals, Applications, and Tools. Artech House, 2015. 369 p.
6. *Sand S., Dammann A., Mensing C.* Positioning in Wireless Communications Systems. Wiley, 2014. 276 p.
7. *del Peral-Rosado J. A.* Evaluation of the LTE positioning capabilities in realistic navigation channels. Universitat Autònoma de Barcelona, 2014.
8. *del Peral-Rosado J. A., López-Salcedo J. A., Seco-Granados G., Zanier F., Crisci M.* Preliminary analysis of the positioning capabilities of the positioning reference signal of 3GPP LTE // Proc. European Workshop on GNSS Signals and Signal Processing, 2011.
9. *del Peral-Rosado J. A., López-Salcedo J. A., Seco-Granados G., Zanier F., Crisci M.* Achievable localization accuracy of the positioning reference signal of 3GPP LTE // Proc. International Conference on Localization and GNSS, 2012. P. 1–6.
10. *del Peral-Rosado J. A., López-Salcedo J. A., Seco-Granados G., Zanier F., Crisci M.* Analysis of positioning capabilities of 3GPP LTE // Proc. 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012), 2012. P. 650–659.
11. *del Peral-Rosado J. A., López-Salcedo J. A., Seco-Granados G., Zanier F., Crisci M.* Evaluation of the LTE positioning capabilities under typical multipath channels // Proc. 6th Advanced Satellite Multimedia Systems Conference (ASMS) and 12th Signal Processing for Space Communications Workshop (SPSC), 2012. P. 139–146.
12. *del Peral-Rosado J. A., López-Salcedo J. A., Seco-Granados G., Zanier F., Crisci M.* Joint channel and time delay estimation for LTE positioning reference signals // Proc. 6th ESA Workshop on Satellite Navigation Technologies (Navitec) & European Workshop on GNSS Signals and Signal Processing, 2012. P. 1–8.

13. *del Peral-Rosado J. A., López-Salcedo J. A., Seco-Granados G., Zanier F., Crisci M.* Joint maximum likelihood time-delay estimation for LTE positioning in multipath channels // EURASIP Journal on Advances in Signal Processing. 2014. № 1. P. 1–13.
14. *del Peral-Rosado J. A. et al.* Software-defined radio LTE positioning receiver towards future hybrid localization systems // Proc. 31st AIAA International Communications Satellite Systems Conference, 2013. P. 14–17.
15. *del Peral-Rosado J.A. et al.* Comparative results analysis on positioning with real LTE signals and low-cost hardware platforms // Proc. 7th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (Navitec), 2014. P. 1–8.
16. *del Peral-Rosado J. A., López-Salcedo J. A., Seco-Granados G., Crosta P., Zanier F., Crisci M.* Downlink synchronization of LTE base stations for opportunistic ToA positioning // Proc. International Conference on Localization and GNSS (ICL-GNSS), 2015. P. 1–6.
17. *Bartolucci M., Del Peral-Rosado J. A., Estatuet-Castillo R., Garcia-Molina J. A., Crisci M., Corazza G. E.* Synchronization of low-cost open source SDRs for navigation applications // Proc. 8th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (Navitec), 2016. P. 1–7.
18. *Müller P., del Peral-Rosado J. A., Piché R., Seco-Granados G.* Statistical Trilateration with Skew-t Distributed Errors in LTE Networks // IEEE Transactions on Wireless Communications. 2016. V. 15, № 10. P. 7114–7127.
19. *del Peral-Rosado J. A., López-Salcedo J. A., Zanier F., Seco-Granados G.* Position Accuracy of Joint Time-Delay and Channel Estimators in LTE Networks // IEEE Access. 2018. V. 6. P. 25185–25199.
20. *del Peral-Rosado J. A., Seco-Granados G., Kim S., López-Salcedo J. A.* Network Design for Accurate Vehicle Localization // IEEE Transactions on Vehicular Technology. 2019. V. 68, № 5. P. 4316–4327.
21. *del Peral-Rosado J. A., López-Salcedo J. A., Kim S., Seco-Granados G.* Feasibility study of 5G-based localization for assisted driving // Proc. International Conference on Localization and GNSS (ICL-GNSS), 2016. P. 1–6.
22. *Shamaei K.* Exploiting Cellular Signals for Navigation: 4G to 5G. University of California, Irvine, 2020.
23. *Kassas Z. M., Shamaei K., Khalife J.* SDR for navigation with LTE signals. Patent US11187774B2. United States. University of California. Publication 30.11.2021.
24. *Shamaei K., Khalife J., Kassas Z.* Performance characterization of positioning in LTE systems // Proc. 29th international technical meeting of the satellite division of the institute of navigation (ION GNSS+), 2016. P. 2262–2270.
25. *Shamaei K., Khalife J., Kassas Z. M.* Comparative results for positioning with secondary synchronization signal versus cell specific reference signal in LTE systems // Proc. International Technical Meeting of the Institute of Navigation, 2017. P. 1256–1268.
26. *Shamaei K., Khalife J., Kassas Z. M.* Ranging precision analysis of LTE signals // Proc. 25th European Signal Processing Conference (EUSIPCO), 2017. P. 2719–2723.
27. *Shamaei K., Khalife J., Souradeep B., Kassas Z. M.* Computationally efficient receiver design for mitigating multipath for positioning with LTE signals // Proc. 30th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+), 2017. P. 3751–3760.
28. *Shamaei K., Khalife J., Kassas Z. M.* Pseudorange and multipath analysis of positioning with LTE secondary synchronization signals // Proc. IEEE Wireless Communications and Networking Conference (WCNC), 2018. P. 1–6.
29. *Shamaei K., Kassas Z.* LTE receiver design and multipath analysis for navigation in urban environments // NAVIGATION Journal of the Institute of Navigation. 2018. V. 65, № 4. P. 655–675.
30. *Shamaei K., Khalife J., Kassas Z. M.* Exploiting LTE Signals for Navigation: Theory to Implementation // IEEE Transactions on Wireless Communications. 2018. V. 17, № 4. P. 2173–2189.

31. *Abdallah A. A., Shamaei K. Kassas Z. M.* Performance characterization of an indoor localization system with LTE code and carrier phase measurements and an IMU // Proc. International Conference on Indoor Positioning and Indoor Navigation (IPIN), 2019. P. 1–8.
32. *Shamaei K., Morales J. J., Kassas Z. M.* A framework for navigation with LTE time-correlated pseudorange errors in multipath environments // Proc. IEEE 89th Vehicular Technology Conference (VTC2019-Spring), 2019. P. 1–6.
33. *Kassas Z. M., Maaref M., Morales J. J., Khalife J. J., Shamei K.* Robust Vehicular Localization and Map Matching in Urban Environments Through IMU, GNSS, and Cellular Signals // IEEE Intelligent Transportation Systems Magazine. 2020. V. 12, № 3. P. 36–52.
34. *Abdallah A. A., Shamaei K., Kassas Z. M.* Assessing real 5G signals for opportunistic navigation // Proc. 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+), 2020. P. 2548–2559.
35. *Shamaei K., Kassas Z. M.* Receiver Design and Time of Arrival Estimation for Opportunistic Localization With 5G Signals // IEEE Transactions on Wireless Communications. 2021. V. 20, № 7. P. 4716–4731.
36. *Shamaei K., Kassas Z. M.* A joint TOA and DOA acquisition and tracking approach for positioning with LTE signals // IEEE Transactions on Signal Processing. 2021. V. 69. P. 2689–2705.
37. *Knutti F., Sabathy M., Driusso M., Mathis H., Marshall C.* Positioning using LTE signals // Proc. of Navigation Conference in Europe, 2015. P. 1–8.
38. *Driusso M., Babich F., Knutti F., Sabathy M., Marshall C.* Estimation and tracking of LTE signals time of arrival in a mobile multipath environment // Proc. 9th International Symposium on Image and Signal Processing and Analysis (ISPA), 2015. P. 276–281.
39. *Driusso M., Marshall C., Sabathy M., Knutti F., Mathis H., Babich F.* Vehicular Position Tracking Using LTE Signals // IEEE Transactions on Vehicular Technology. 2017. V. 66, № 4. P. 3376–3391.
40. *Xu W., Huang M., Zhu C., Dammann A.* Maximum likelihood TOA and OTDOA estimation with first arriving path detection for 3GPP LTE system // Transactions on Emerging Telecommunications Technologies. 2016. V. 27, № 3. P. 339–356.
41. *Фокин Г. А., Волгушев Д. Б., Харин В. Н.* Использование SDR технологии для задач сетевого позиционирования. Формирование опорных сигналов LTE // T-Comm: Телекоммуникации и транспорт. 2022. Т. 16, № 5. С. 28–47.
42. *Фокин Г. А., Лаврухин В. А., Волгушев Д. А., Киреев А. В.* Модельно-ориентированное проектирование на основе SDR // Системы управления и информационные технологии. 2015. № 2 (60). С. 94–99.
43. *Фокин Г. А.* Технологии программно-конфигурируемого радио. М.: Горячая Линия – Телеком, 2019. 316 с.
44. *Фокин Г. А.* Методика идентификации прямой видимости в радиолиниях сетей мобильной связи 4-го поколения с пространственной обработкой сигналов // Труды Научно-исследовательского института радио. 2013. № 3. С. 78–82.
45. *Фокин Г. А.* Имитационное моделирование процесса распространения радиоволн в радиолиниях сетей мобильной связи 4-го поколения с пространственной обработкой сигналов // Труды Научно-исследовательского института радио. 2013. № 3. С. 83–89.
46. *Фокин Г. А.* Комплексная имитационная модель для позиционирования источников радиоизлучения в условиях отсутствия прямой видимости // Труды учебных заведений связи. 2018. Т. 4, № 1. С. 85–101.
47. *Фокин Г. А.* Сценарии позиционирования в сетях 5G // Вестник связи. 2020. № 2. С. 3–9.
48. *Фокин Г. А.* Сценарии позиционирования в сетях 5G // Вестник связи. 2020. № 3. С. 13–21.
49. *Фокин Г. А., Кучерявый А. Е.* Сетевое позиционирование в экосистеме 5G // Электросвязь. 2020. № 9. С. 51–58.
50. *Фокин Г. А.* Использование методов сетевого позиционирования в экосистеме 5G // Электросвязь. 2020. № 11. С 29–37.

51. OpenCellid. [Электронный ресурс]. URL: https://opencellid.org/ (дата обращения: 29.09.2022).
52. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича. [Электронный ресурс]. URL: https://www.sut.ru/ (дата обращения: 29.09.2022).
53. *Сиверс М. А., Фокин Г. А., Духовницкий О. Г.* Позиционирование абонентских станций в сетях мобильной связи LTE разностно-дальномерным методом // Системы управления и информационные технологии. 2015. Т. 59, № 1. С. 55–61.
54. Свидетельство о государственной регистрации программы для ЭВМ № 2022617912, 26.04.2022. Программный модуль комплекса функций представления и преобразования форматов оценок координат при позиционировании в сетях мобильного широкополосного беспроводного доступа (МШБД) / В. О. Аксенов, Г. А. Фокин. Правообладатель ООО «Лаборатория инфокоммуникационных сетей». Заявка № 2022616360 от 11.04.2022.
55. *Дворников С. В., Фокин Г. А., Аль-Одхари А. Х., Федоренко И. В.* Оценка влияния свойств сигнала PRS LTE на точность позиционирования // Вопросы радиоэлектроники. Серия: Техника телевидения. 2017. № 4. С. 94–103.
56. *Дворников С. В., Фокин Г. А., Аль-Одхари А. Х., Федоренко И. В.* Исследование зависимости геометрического фактора топологии для разностно-дальномерного метода позиционирования // Вопросы радиоэлектроники. Серия: Техника телевидения. 2017. № 2. С. 86–93.
57. *Дворников С. В., Фокин Г. А., Аль-Одхари А. Х., Федоренко И. В.* Исследование зависимости значения геометрического фактора снижения точности от топологии пунктов приема // Вопросы радиоэлектроники. Серия: Техника телевидения. 2018. № 2. С. 99–104.
58. *Гельгор А. Л., Павленко И. И., Горлов А. И., Фокин Г. А., Попов Е. А., Лаврухин В. А., Сиверс М. А.* Первичная синхронизация с базовыми станциями LTE // Электромагнитные волны и электронные системы. 2014. Т. 19, № 7. С. 54–62.
59. *Гельгор А. Л., Павленко И. И., Фокин Г. А., Горлов А. И., Попов Е. А., Лаврухин В. А., Сиверс М. А.* Пеленгация базовых станций в сетях LTE // Электросвязь. 2014. № 9. С. 34–39.
60. *Борисов Е. Г., Машков Г. М., Фокин Г. А.* Экспериментальный стенд оценки точности позиционирования на основе программно-конфигурируемого радио // Сборник научных статей V международной научно-технической и научно-методической конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании», 2016. С. 120–125.
61. 3GPP TS 36.211 V16.7.0 (2021-12). Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation (Release 17).
62. 3GPP TS 36.212 V17.1.0 (2022-03). Evolved Universal Terrestrial Radio Access (E-UTRA); Multiplexing and channel coding (Release 17).
63. *Drozdova V. G., Kalachikov A. A.* SDR Based Evaluation of the Initial Cell Search In 5G NR OpenAirInterface Implementation // Proc. XV International Scientific-Technical Conference on Actual Problems of Electronic Instrument Engineering (APEIE), 2021. P. 248–251.
64. *Петров В. П., Якушев И. Ю.* Современные технологии в системе MIMO // Вестник СибГУТИ. 2019. № 2. С. 94–108.
65. *Калачиков А. А., Безгодкин Р. О., Петров И. А., Винников А. А.* Исследование модели канала связи MIMO на основе открытого пакета моделирования // Вестник СибГУТИ. 2021. № 4 (56). С. 43–55.
66. *van de Beek J. J., Sandell M., Borjesson P. O.* ML estimation of time and frequency offset in OFDM systems // IEEE Transactions on Signal Processing. 1997. V. 45, № 7. P. 1800–1805.
67. *Fischer S.* Observed time difference of arrival (OTDOA) positioning in 3GPP LTE. Qualcomm White Pap. July. 2014. P. 1–62.
68. *Hofer M., McEachen J., Tummala M.* Vulnerability Analysis of LTE Location Services // Proc. 47th Hawaii International Conference on System Sciences. 2014. P. 5162–5166.
69. *Speth M., Fechtel S. A., Fock G., Meyr H.* Optimum receiver design for wireless broad-band systems using OFDM. I // IEEE Transactions on Communications. 1999. V. 47, № 11. P. 1668–1677.

70. *Speth M., Fechtel S. A., Fock G., Meyr H.* Optimum receiver design for OFDM-based broadband transmission. II. A case study // IEEE Transactions on Communications. 2001. V. 49, № 4. P. 571–578.
71. *Yang B., Letaief K. B., Cheng R. S., Cao Z.* Timing recovery for OFDM transmission // IEEE Journal on Selected Areas in Communications. 2000. V. 18, № 11. P. 2278–2291.

Статья поступила в редакцию 20.07.2022;
переработанный вариант – 15.08.2022.

Фокин Григорий Алексеевич
д.т.н., доцент, профессор кафедры радиосвязи и вещания СПбГУТ (193232, Санкт-Петербург, пр. Большевиков д. 22, к. 1, а. 407/2), e-mail: grihafokin@gmail.com.

Волгушев Дмитрий Борисович
научный сотрудник СПбГУТ (193232, Санкт-Петербург, пр. Большевиков д. 22, к. 1, а. 407/2), e-mail: d.volgushev@yandex.ru.

Development of SDR-based network positioning technology. LTE reference signals reception and processing models

Grigoriy A. Fokin
Doctor of technical sciences, docent, professor, The Bonch-Bruevich Saint Petersburg State University of Telecommunications (SPbSUT, Saint Petersburg, Russia), grihafokin@gmail.com.

Dmitry B. Volgushev
Research assistant, The Bonch-Bruevich Saint Petersburg State University of Telecommunications (SPbSUT, Saint Petersburg, Russia), d.volgushev@yandex.ru.

The analysis of the problem status of positioning user UE devices using the infrastructure of the eNB base stations of LTE mobile radio networks according to open foreign sources shows the high actuality and relevance of this research area. This paper provides an analysis of the problem status, as well as, formalization of models for receiving and processing LTE reference signals for the layout of a user device built using software-configurable radio technology.

Keywords: 4G, LTE, PSS, SSS, CRS, PRS, SDR, positioning.

References

1. Fokin G.A. *Tekhnologii setevogo pozitsionirovaniya* [Network positioning technologies]. St. Petersburg, SPbGUT, 2020, 558 p.
2. Fokin G.A. *Tekhnologii setevogo pozitsionirovaniya 5G* [5G network positioning technologies]. Moscow, Goryachaya liniya–Telekom, 2021, 456 p.
3. Fokin G.A. *Kompleks modeley i metodov pozitsionirovaniya ustroystv v setyakh pyatogo pokoleniya. Dissertatsiya na soiskaniye uchenoy stepeni doktora tekhnicheskikh nauk* [A set of models and methods for positioning devices in fifth-generation networks]. Doctor's degree dissertation 05.12.13, St. Petersburg, 2021, 499 p.
4. Zekavat R., Buehrer R. M. *Handbook of position location: Theory, practice and advances*. John Wiley & Sons, 2019, 1376 p.

5. Campos R. S., Lovisolo L. *RF Positioning: Fundamentals, Applications, and Tools*. Artech House, 2015, 369 p.
6. Sand S., Dammann A., Mensing C. *Positioning in Wireless Communications Systems*. Wiley, 2014, 276 p.
7. del Peral-Rosado J.A. *Evaluation of the LTE positioning capabilities in realistic navigation channels*. Universitat Autònoma de Barcelona, 2014.
8. del Peral-Rosado J.A., López-Salcedo J.A., Seco-Granados G., Zanier F., Crisci M. Preliminary analysis of the positioning capabilities of the positioning reference signal of 3GPP LTE. *Proceedings of European Workshop on GNSS signals and Signal Processing*, 2011.
9. del Peral-Rosado J.A., López-Salcedo J.A., Seco-Granados G., Zanier F., Crisci M. Achievable localization accuracy of the positioning reference signal of 3GPP LTE. *2012 International Conference on Localization and GNSS*, 2012, pp. 1-6.
10. del Peral-Rosado J.A., López-Salcedo J.A., Seco-Granados G., Zanier F., Crisci M. Analysis of positioning capabilities of 3GPP LTE. *Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012)*, 2012, pp. 650-659.
11. del Peral-Rosado J.A., López-Salcedo J.A., Seco-Granados G., Zanier F., Crisci M. Evaluation of the LTE positioning capabilities under typical multipath channels. *2012 6th Advanced Satellite Multimedia Systems Conference (ASMS) and 12th Signal Processing for Space Communications Workshop (SPSC)*, 2012, p. 139-146.
12. del Peral-Rosado J.A., López-Salcedo J.A., Seco-Granados G., Zanier F., Crisci M. Joint channel and time delay estimation for LTE positioning reference signals. *2012 6th ESA Workshop on Satellite Navigation Technologies (Navitec 2012) & European Workshop on GNSS Signals and Signal Processing*, 2012, pp. 1-8.
13. del Peral-Rosado J.A., López-Salcedo J.A., Seco-Granados G., Zanier F., Crisci M. Joint maximum likelihood time-delay estimation for LTE positioning in multipath channels. *EURASIP Journal on Advances in Signal Processing*, 2014, № 1, pp. 1-13.
14. del Peral-Rosado J.A. et al. Software-defined radio LTE positioning receiver towards future hybrid localization systems. *Proceedings of 31st AIAA International Communications Satellite Systems Conference*, 2013, pp. 14-17.
15. del Peral-Rosado J.A. et al. Comparative results analysis on positioning with real LTE signals and low-cost hardware platforms. *2014 7th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (Navitec)*, 2014, pp. 1-8.
16. del Peral-Rosado J.A., López-Salcedo J.A., Seco-Granados G., Crosta P., Zanier F., Crisci M. Downlink synchronization of LTE base stations for opportunistic ToA positioning. *2015 International Conference on Localization and GNSS (ICL-GNSS)*, 2015, pp. 1-6.
17. Bartolucci M., Del Peral-Rosado J.A., Estatuet-Castillo R., Garcia-Molina J.A., Crisci M., Corazza G.E. Synchronization of low-cost open source SDRs for navigation applications. *2016 8th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, 2016, pp. 1-7.
18. Müller P., del Peral-Rosado J.A., Piché R., Seco-Granados G. Statistical Trilateration with Skew-t Distributed Errors in LTE Networks. *IEEE Transactions on Wireless Communications*, 2016, vol. 15, no. 10, pp. 7114-7127.
19. del Peral-Rosado J.A., López-Salcedo J.A., Zanier F., Seco-Granados G. Position Accuracy of Joint Time-Delay and Channel Estimators in LTE Networks. *IEEE Access*, 2018, vol. 6, pp. 25185-25199.
20. del Peral-Rosado J.A., Seco-Granados G., Kim S., López-Salcedo J.A. Network Design for Accurate Vehicle Localization. *IEEE Transactions on Vehicular Technology*, 2019, vol. 68, no. 5, pp. 4316-4327.
21. del Peral-Rosado J.A., López-Salcedo J.A., Kim S., Seco-Granados G. Feasibility study of 5G-based localization for assisted driving. *2016 International Conference on Localization and GNSS (ICL-GNSS)*, 2016, pp. 1-6.
22. Shamaei K. *Exploiting Cellular Signals for Navigation: 4G to 5G*. University of California, Irvine, 2020.
23. Kassas Z.M., Shamaei K., Khalife J. SDR for navigation with LTE signals. Patent US11187774B2. United States. University of California. Publication 30.11.2021.
24. Shamaei K., Khalife J., Kassas Z. Performance characterization of positioning in LTE systems. *Proceedings of the 29th international technical meeting of the satellite division of the institute of navigation (ION GNSS+ 2016)*, 2016, pp. 2262-2270.
25. Shamaei K., Khalife J., Kassas Z.M. Comparative results for positioning with secondary synchronization signal versus cell specific reference signal in LTE systems. *Proceedings of the 2017 International Technical Meeting of the Institute of Navigation*, 2017, pp. 1256-1268.

26. Shamaei K., Khalife J., Kassas Z.M. Ranging precision analysis of LTE signals. *2017 25th European Signal Processing Conference (EUSIPCO)*, 2017, pp. 2719-2723.
27. Shamaei K., Khalife J., Souradeep B., Kassas Z.M. Computationally efficient receiver design for mitigating multipath for positioning with LTE signals. *Proceedings of the 30th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2017)*, 2017, pp. 3751-3760.
28. Shamaei K., Khalife J., Kassas Z.M. Pseudorange and multipath analysis of positioning with LTE secondary synchronization signals. *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, 2018, pp. 1-6.
29. Shamaei K., Kassas Z. LTE receiver design and multipath analysis for navigation in urban environments. *NAVIGATION Journal of the Institute of Navigation*,2018, vol. 65, no. 4, pp. 655-675.
30. Shamaei K., Khalife J., Kassas Z.M. Exploiting LTE Signals for Navigation: Theory to Implementation. *IEEE Transactions on Wireless Communications*, 2018, vol. 17, no. 4, pp. 2173-2189.
31. Abdallah A.A., Shamaei K. Kassas Z.M. Performance characterization of an indoor localization system with LTE code and carrier phase measurements and an IMU. *2019 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, 2019, pp. 1-8.
32. Shamaei K., Morales J.J., Kassas Z.M. A framework for navigation with LTE time-correlated pseudorange errors in multipath environments. *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, 2019, pp. 1-6.
33. Kassas Z.M., Maaref M., Morales J.J., Khalife J.J., Shamei K. Robust Vehicular Localization and Map Matching in Urban Environments Through IMU, GNSS, and Cellular Signals. *IEEE Intelligent Transportation Systems Magazine*, 2020, vol. 12, no. 3, pp. 36-52.
34. Abdallah A.A., Shamaei K., Kassas Z.M. Assessing real 5G signals for opportunistic navigation. *In Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)*, 2020, pp. 2548-2559.
35. Shamaei K., Kassas Z.M. Receiver Design and Time of Arrival Estimation for Opportunistic Localization With 5G Signals. *IEEE Transactions on Wireless Communications*, 2021, vol. 20, no 7, pp. 4716-4731.
36. Shamaei K., Kassas Z.M. A joint TOA and DOA acquisition and tracking approach for positioning with LTE signals. *IEEE Transactions on Signal Processing*, 2021, vol. 69, pp.2689-2705.
37. Knutti F., Sabathy M., Driusso M., Mathis H., Marshall C. Positioning using LTE signals. *Proceedings of Navigation Conference in Europe*, 2015, pp. 1-8.
38. Driusso M., Babich F., Knutti F., Sabathy M., Marshall C. Estimation and tracking of LTE signals time of arrival in a mobile multipath environment. *2015 9th International Symposium on Image and Signal Processing and Analysis (ISPA)*, 2015, pp. 276-281.
39. Driusso M., Marshall C., Sabathy M., Knutti F., Mathis H., Babich F. Vehicular Position Tracking Using LTE Signals. *IEEE Transactions on Vehicular Technology*, 2017, vol. 66, no 4, pp. 3376-3391.
40. Xu W., Huang M., Zhu C., Dammann A. Maximum likelihood TOA and OTDOA estimation with first arriving path detection for 3GPP LTE system. *Transactions on Emerging Telecommunications Technologies*, 2016, vol. 27, no 3, pp. 339-356.
41. Fokin G.A., Volgushev D.B., Kharin V.N. Ispol'zovaniye SDR tekhnologii dlya zadach setevo-go pozitsionirovaniya. Formirovaniye opornykh signalov LTE [Using SDR technology for network positioning tasks. Formation of LTE reference signals]. *T-Comm: Telecommunications and transport*, 2022. vol. 16, no. 5, pp. 28-47.
42. Fokin G.A., Lavrukhin V.A., Volgushev D.A., Kireev A.V. Model'no-oriyentirovannoye pro-yektirovaniye na osnove SDR [Model-Based Design Based on SDR]. *Control Systems and Information Technologies*, 2015, no. 2 (60), pp. 94-99.
43. Fokin G.A. *Tekhnologii programmno-konfiguriruyemogo radio* [Software Defined Radio Technologies]. Moscow, Goryachaya liniya–Telekom, 2019, 316 p.
44. Fokin G.A. Metodika identifikatsii pryamoy vidimosti v radioliniyakh setey mobil'-noy svyazi 4-go pokoleniya s prostranstvennoy obrabotkoy signalov [Line-of-sight identification technique in radio links of 4th generation mobile communication networks with spatial signal processing]. *Proceedings of the Scientific Research Institute of Radio*, 2013, no. 3, pp. 78-82.
45. Fokin G.A. Imitatsionnoye modelirovaniye protsessa rasprostraneniya radiovoln v ra-dioliniyakh setey mobil'noy svyazi 4-go pokoleniya s prostranstvennoy obrabotkoy signalov [Simulation modeling of the process of propagation of radio waves in radio links of 4th generation mobile communication networks with spatial processing of signals]. *Proceedings of the Scientific Research Institute of Radio*, 2013, no. 3, pp. 83-89.

46. Fokin G.A. Kompleksnaya imitatsionnaya model' dlya pozitsionirovaniya istochnikov ra-dioizlucheniya v usloviyakh otsutstviya pryamoy vidimosti [Complex simulation model for positioning radio sources in the absence of line of sight]. *Proceedings of educational institutions of communication*, 2018, vol. 4, no. 1, pp. 85-101.
47. Fokin G.A. Stsenarii pozitsionirovaniya v setyakh 5G [Positioning scenarios in 5G networks]. *Vestnik svyazi*, 2020, no. 2, pp. 3-9.
48. Fokin G.A. Stsenarii pozitsionirovaniya v setyakh 5G [Positioning scenarios in 5G networks]. *Vestnik svyazi,* 2020, no. 3, pp. 13-21.
49. Fokin G.A., Kucheryavy A.E. Setevoye pozitsionirovaniye v ekosisteme 5G [Network positioning in the 5G ecosystem]. *Electrosvyaz*, 2020, no. 9, pp. 51-58.
50. Fokin G.A. Ispol'zovaniye metodov setevogo pozitsionirovaniya v ekosisteme 5G [Using network positioning methods in the 5G ecosystem], *Elektrosvyaz*, 2020, no. 11, pp. 29-37.
51. OpenCellid, available at: `https://opencellid.org/` (accessed 29.09.2022).
52. The Bonch-Bruevich Saint Petersburg State University of Telecommunications, available at: `https://www.sut.ru/` (accessed 29.09.2022).
53. Sivers M.A., Fokin G.A., Dukhovnitsky O.G. Pozitsionirovaniye abonentskikh stantsiy v setyakh mobil'noy svyazi LTE raznostno-dal'nomernym metodom [Positioning of subscriber stations in LTE mobile communication networks by difference-range method]. *Control systems and information technologies*, 2015, vol. 59, no. 1, pp. 55-61.
54. Aksenov V.O., Fokin G.A. *Programmnyy modul' kompleksa funktsiy predstavleniya i preobrazovaniya formatov otsenok koordinat pri pozitsionirovanii v setyakh mobil'nogo shirokopolosnogo bes-provodnogo dostupa (MSHBD)* [Software module for a set of functions for representing and converting formats of coordinate estimates for positioning in mobile broadband wireless access networks (MBBA)]. Certificate of state registration of the computer program No. 2022617912, 04/26/2022. Copyright holder LLC "Laboratory of infocommunication networks". Application No. 2022616360 dated 04/11/2022.
55. Dvornikov S.V., Fokin G.A., Al-Odkhari A.Kh., Fedorenko I.V. Otsenka vliyaniya svoystv signala PRS LTE na tochnost' pozitsionirovaniya [Evaluation of the influence of the properties of the PRS LTE signal on positioning accuracy]. *Problems of radio electronics. Series: TV Technique*, 2017, no. 4, pp. 94-103.
56. Dvornikov S.V., Fokin G.A., Al-Odkhari A.Kh., Fedorenko I.V. Issledovaniye zavisimo-sti geometricheskogo faktora topologii dlya raznostno-dal'nomernogo metoda pozitsionirovaniya [Investigation of the dependence of the geometric factor of topology for the difference-range method of positioning]. *Problems of radio electronics. Series: TV Technique*, 2017, no. 2, pp. 86-93.
57. Dvornikov S.V., Fokin G.A., Al-Odkhari A.Kh., Fedorenko I.V. Issledovaniye zavisimosti znacheniya geometricheskogo faktora snizheniya tochnosti ot topologii punktov priyema [Investigation of the dependence of the value of the geometric factor of accuracy reduction on the topology of reception points]. *Problems of radio electronics. Series: TV Technique*, 2018, no. 2, pp. 99–104.
58. Gelgor A.L., Pavlenko I.I., Gorlov A.I., Fokin G.A., Popov E.A., Lavrukhin V.A., Sivers M.A. Pervichnaya sinkhronizatsiya s bazovymi stantsiyami LTE [Primary synchronization with LTE base stations]. *Electromagnetic waves and electronic systems*, 2014, vol. 19, no. 7, pp. 54-62.
59. Gelgor A.L., Pavlenko I.I., Fokin G.A., Gorlov A.I., Popov E.A., Lavrukhin V.A., Sivers M.A. Pelengatsiya bazovykh stantsiy v setyakh LTE [Direction finding of base stations in LTE networks]. *Electrosvyaz*, 2014, no. 9, pp. 34-39.
60. Borisov E.G., Mashkov G.M., Fokin G.A. Eksperimental'nyy stend otsenki tochnosti po-zitsionirovaniya na osnove programmno-konfiguriruyemogo radio [Experimental stand for assessing positioning accuracy based on software-defined radio]. *Actual problems of infotelecommunications in science and education. collection of scientific articles of the V international scientific-technical and scientific-methodical conference*, 2016, pp. 120-125.
61. 3GPP TS 36.211 V16.7.0 (2021-12). Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation (Release 17).
62. 3GPP TS 36.212 V17.1.0 (2022-03). Evolved Universal Terrestrial Radio Access (E-UTRA); Multiplexing and channel coding (Release 17).
63. Drozdova V. G., Kalachikov A. A. SDR Based Evaluation of the Initial Cell Search In 5G NR OpenAir-Interface Implementation. *2021 XV International Scientific-Technical Conference on Actual Problems Of Electronic Instrument Engineering (APEIE)*, 2021, pp. 248-251.
64. Petrov V.P., Yakushev I.Yu. Sovremennyye tekhnologii v sisteme MIMO [Modern technologies in the MIMO system]. *Vestnik SibGUTI*, 2019, no. 2, pp. 94-108.

65. Kalachikov A.A., Bezgodkin R.O., Petrov I.A., Vinnikov A.A. Issledovaniye modeli kanala svyazi MIMO na osnove otkrytogo paketa modelirovaniya [Investigation of the MIMO channel model based on an open modeling package]. *Vestnik SibGUTI*, 2021, no. 4 (56), pp. 43-55.
66. van de Beek J.J., Sandell M., Borjesson P.O. ML estimation of time and frequency offset in OFDM systems. *IEEE Transactions on Signal Processing*, 1997, vol. 45, no. 7, pp. 1800-1805.
67. Fischer S. Observed time difference of arrival (OTDOA) positioning in 3GPP LTE. Qualcomm White Pap. July, 2014, pp.1-62.
68. Hofer M., McEachen J., Tummala M. Vulnerability Analysis of LTE Location Services. *2014 47th Hawaii International Conference on System Sciences*, 2014, pp. 5162-5166.
69. Speth M., Fechtel S.A., Fock G., Meyr H. Optimum receiver design for wireless broad-band systems using OFDM. I. *IEEE Transactions on Communications*, 1999, vol. 47, no. 11, pp. 1668-1677.
70. Speth M., Fechtel S.A., Fock G., Meyr H. Optimum receiver design for OFDM-based broadband transmission. II. A case study. *IEEE Transactions on Communications*, 2001, vol. 49, no 4, pp. 571-578.
71. Yang B., Letaief K.B., Cheng R.S., Cao Z. Timing recovery for OFDM transmission. *IEEE Journal on Selected Areas in Communications,* 2000, vol. 18, no. 11, pp. 2278-2291.

УДК: 378.14+004.056
DOI: 10.55648/1998-6920-2022-16-3-84-100

Кадровое обеспечение образовательных программ в области информационной безопасности: проблемы проектирования и развития[1]

Н. Л. Микиденко, С. П. Сторожева, Е. Г. Струкова

Развитие информационных технологий и возрастание цивилизационных рисков и угроз актуализируют вопросы информационной безопасности. Резко возрастает потребность в специалистах в области информационной безопасности. Это требует решения целого ряда управленческих, организационных, содержательных вопросов, связанных с организацией и реализацией образовательных программ по информационной безопасности, в том числе вопросов кадрового обеспечения. В таких условиях развитие кадрового потенциала преподавательского состава, формирование необходимых актуальных знаний и компетенций преподавателей для качественной подготовки будущих специалистов становятся актуальными и востребованными. Массовая переподготовка преподавателей становится важней задачей в обеспечении цифровой экономики специалистами по информационной безопасности. Методологической основой исследования приняты положения социологии образования, отражающие проблемы соответствия потребностей в кадрах для цифровой экономики, импортозамещения и национальной безопасности, количества и качества подготовки специалистов в образовательных организациях высшего профессионального образования. Цель исследования – выявить запросы работодателей на компетенции специалистов по информационной безопасности для формирования профессиональных образовательных программ и запросы преподавателей, занятых в подготовке специалистов по информационной безопасности, на актуальные знания, умения, навыки, наличие которых обеспечит инновационность в подготовке молодых специалистов. Гипотеза исследования: существует рассогласованность запросов со стороны субъектов внешней среды, прежде всего работодателей, и возможностей образовательной системы; существует острая необходимость наращивания кадрового потенциала преподавателей, занятых в подготовке специалистов в сфере информационной безопасности. Причины такого рассогласования связаны с (1) динамичным развитием технологий, появлением и нарастанием киберугроз и киберинцидентов, (2) наличием объективных проблем в развитии кадрового потенциала образовательных организаций (низкая доля молодых кадров, недостаточное взаимодействие образовательных организаций с производственными и научными центрами, недостаточная научная и образовательная мобильность научно-педагогических работников при повышении квалификации).
Запросы работодателей и преподавателей выявлены на основе проведенного авторами эмпирического исследования (осень 2021 г.). В социологическом исследовании, проведенном в форме анкетирования, приняли участие 103 преподавателя и 109 сотрудников предприятий, выполняющих функции по обеспечению информационной безопасности организаций и предприятий (преимущественно СФО). Результаты: выявлены запросы работодателей и преподавателей на актуальные для специалиста по информационной безопасности знания, умения навыки, актуальные программы повышения квалификации и профессиональной переподготовки. Практическая значимость результатов состоит в том, что исследование позволило выявить проблемы проектирования и дизайна образовательных программ по информационной безопасности, сформулировать рекомендации к проектированию.

[1] Исследование выполнено в рамках государственного задания № 071-03-2022-001.

Ключевые слова: информационная безопасность, кадровый потенциал, преподаватели высшей школы, образовательная программа.

1. Введение

Диверсификация экономики и переход на цифровую траекторию развития в ответ на технологические и цивилизационные вызовы актуализируют вопросы информационной безопасности. Существенная роль в обеспечении процессов цифровизации отводится сотрудникам информационной безопасности, способным работать в условиях высокой неопределенности, нестабильности, сложности, неясности. В докладе Е.Б. Белова (заместитель председателя ФУМО ВО ИБ), И.А. Волошиной (сотрудника ВНИИ труда, Минтруд России) в ходе XVII Всероссийской научно-практической конференции «Информационная безопасность цифровой экономики», проходившей в Новосибирске 12 – 15 октября 2021 г., была представлена ожидаемая среднегодовая потребность в специалистах в области информационной безопасности в 2022–2024 годах по субъектам Сибирского и Дальневосточного федеральных округов в объеме 15200 специалистов ежегодно, а также профессии будущего в сфере информационной безопасности [1].

Прогнозируемый рост потребности в специалистах информационной безопасности и недостаточность образовательных программ по подготовке специалистов в области информационной безопасности делает востребованными образовательные программы по направлению «Информационной безопасности» для преподавателей, которые будут обучать будущих специалистов по информационной безопасности. Массовая переподготовка преподавателей становится важной задачей в обеспечении цифровой экономики специалистами по информационной безопасности.

Исследования последних лет говорят «об острой нехватке кадров по направлению «информационная безопасность» [2, С. 987]. Специалисты отмечают, что «любая деятельность человека в цифровом бытие будь то производственная, социальная, политическая, просто бытовая, не может обойтись без надежной защиты информации и безопасных форм ее использования» [3, С. 697]. Подготовка кадров для сферы информационной безопасности широко обсуждается в профессиональном сообществе в разных аспектах: проектирование содержания образовательных курсов и программ [2, 4, 5, 6]; сравнение российских и международных подходов к стандартизации профессиональной и образовательной деятельности в сфере ИТ и основные принципы модели SFIA как наднационального инструмента для описания и управления компетенциями специалистов – разработчиков и эксплуатантов систем на базе ИКТ [7, С. 133]; подготовка педагогов для их реализации и востребованность программ повышения квалификации [8]. Отдельной проблемой обсуждаются компетенции специалистов по информационной безопасности [9], этические проблемы информационной безопасности и подготовка ИТ-специалистов, инновационно-профессионально-этическая проблематика информационной безопасности в VUCA-мире [10, 11, 12] и др. Подчеркивается, что «проблема защиты информации становится личным, деловым и национальным приоритетом и в той или иной мере затрагивает каждого члена общества» [13]. Потребность в кадрах в сфере информационной безопасности испытывается в экономике в целом [14] и в разных ее отраслях [15]. Отмечено, что зачастую «информационная безопасность отстает в развитии от других сфер экономики и в какой-то степени является ее тормозом» [16, С. 116]. Действующие специалисты по информационной безопасности, формулируя требования к профессиональным знаниям, умениям и навыкам будущего профессионала, помимо знаний программно-аппаратного обеспечения средств информационной защиты, нормативно-правовой базы, отмечают значимость таких составляющих, как управленческие и коммуникативные навыки, а также знания методов оценки и прогнозирования поведения человека [17].

На конференции «Кибербезопасность: защита информации как драйвер роста российского бизнеса», проведенной компанией Мегафон 21 июля 2022 года, отмечается, что в первые месяцы 2022 года число кибератак на российский бизнес выросло в четыре раза по сравнению с аналогичным периодом 2021 года, многие компании понесли финансовый и репутационный ущерб. «Задача обеспечения киберзащиты компаний вышла на первый план и напрямую влияет на экономику компаний и достижение бизнес-целей» [18].

В Решении XXVI Пленума ФУМО в системе высшего образования по УГСНП 10.00.00 «Информационная безопасность», прошедшего в рамках Форума информационной безопасности «Сибирь – Дальний Восток 2022» 28 июня – 2 июля 2022 года в Хабаровске, рекомендовано организовать в рамках ФУМО ВО ИБ с привлечением работодателей дискуссию по вопросам структуры и развития номенклатуры образовательных программ в области информационной безопасности, а также развития национальной системы подготовки кадров в области информационной безопасности [19].

Условием развития сферы информационной безопасности является создание специальных профессиональных образовательных программ. Их реализация напрямую зависит от готовности и квалификационных характеристик профессорско-преподавательского состава и актуализирует задачи профессиональной переподготовки и повышения квалификации в этой области.

2. Результаты исследования

2.1. Методология и методика исследования

Для выявления запроса со стороны преподавателей на программы повышения квалификации в сфере информационной безопасности проведено исследование (декабрь 2021 г.). Исследование проведено методом анкетирования с использованием электронной формы анкеты, включавшей три раздела и 30 вопросов. Дизайн анкеты включал следующие тематические блоки: социально-демографическая информация, оценка преподавателями и представителями образовательных организаций состояния рынка труда и востребованных компетенций в области «Информационная безопасность», оценки востребованности программ профессиональной переподготовки и повышения квалификации в области «Информационная безопасность».

2.2. Выборка исследования

Выборка исследования – целевая, неслучайная. В исследовании принимали участие преподаватели, работающие в высших и средних профессиональных образовательных организациях, преподающие дисциплины по образовательным программам в сфере информационной безопасности и проходившие курсы повышения квалификации и/или профессиональную переподготовку в период с сентября по ноябрь 2021 года. Опрос проводился в декабре 2021 года. В исследовании приняли участие 103 человека, среди которых мужчины составили 58.3 %, женщины – 41.2 %. В опросе приняли участие преподаватели 14 образовательных организаций высшего профессионального образования Сибирского федерального округа.

87.4 % участников опроса преподают учебные курсы по образовательным программам направления подготовки «Информационная безопасность». На рис. 1 отражено распределение преподавателей по дисциплинам, которые они преподают. Среди участников опроса более 60 % преподавателей по компьютерным и/или техническим наукам, 16.5 % преподавателей физико-математических дисциплин. В выборке представлены также преподаватели социальных (3.9 %), естественных (3.9 %), экономических (4.9 %) и юридических дисциплин (2.9 %) (рис. 1).

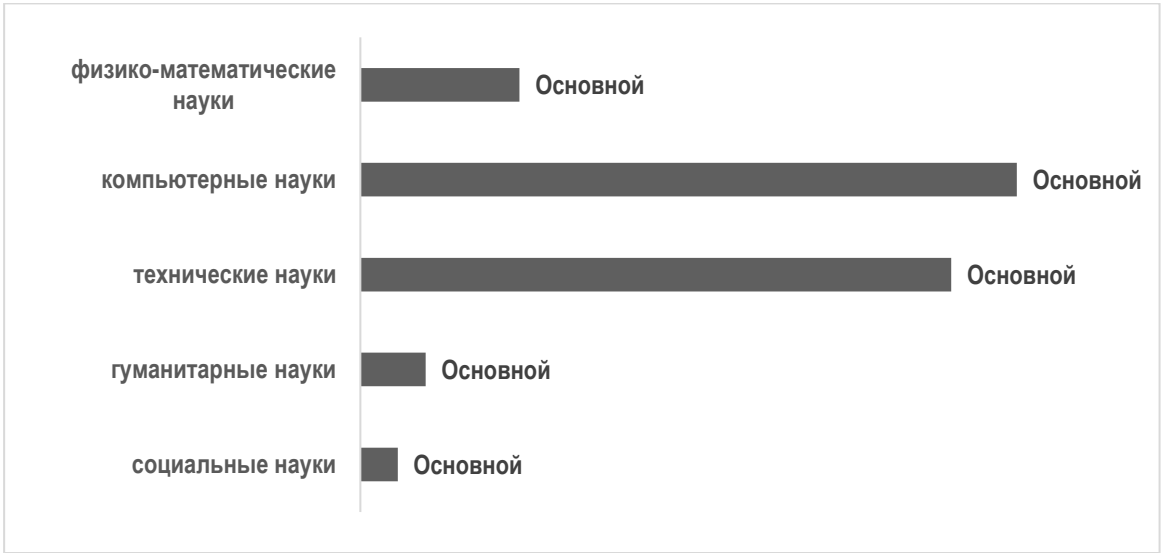

Рис. 1. Сферы науки, к которым относятся дисциплины, преподаваемые участниками опроса (вопрос с множественным выбором, допускается более одного ответа)

Преподаваемые дисциплины развивают разные типы компетенций. 43.7 % опрошенных преподают дисциплины, развивающие универсальные компетенции, 70.9 % – общепрофессиональные, 59.2 % – профессиональные. Распределение ответов отражено на рис. 2.

Рис. 2. Компетенции, формируемые дисциплинами преподавателей – участников опроса (% респондентов, вопрос с множественным выбором, допускается более одного ответа)

В опросе приняли участие разные группы преподавателей по стажу научно-педагогической деятельности. 58.3 % имеют стаж работы более 15 лет. Объем групп преподавателей по стажу работы представлен на рис. 3.

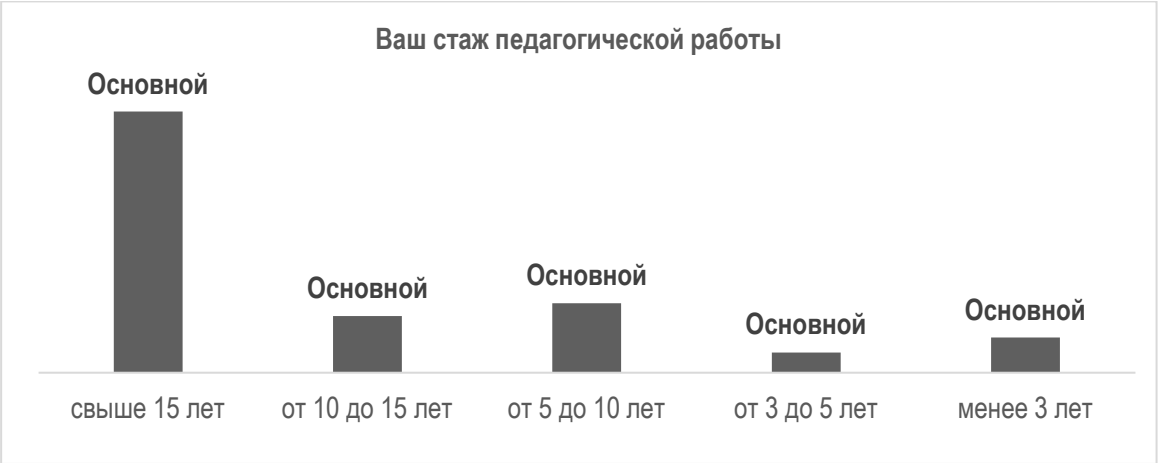

Рис. 3. Стаж педагогической работы респондентов (n = 103, %)

Респонденты, участвовавшие в опросе, участвуют в реализации разных направлений программ в сфере информационной безопасности (рис. 4):

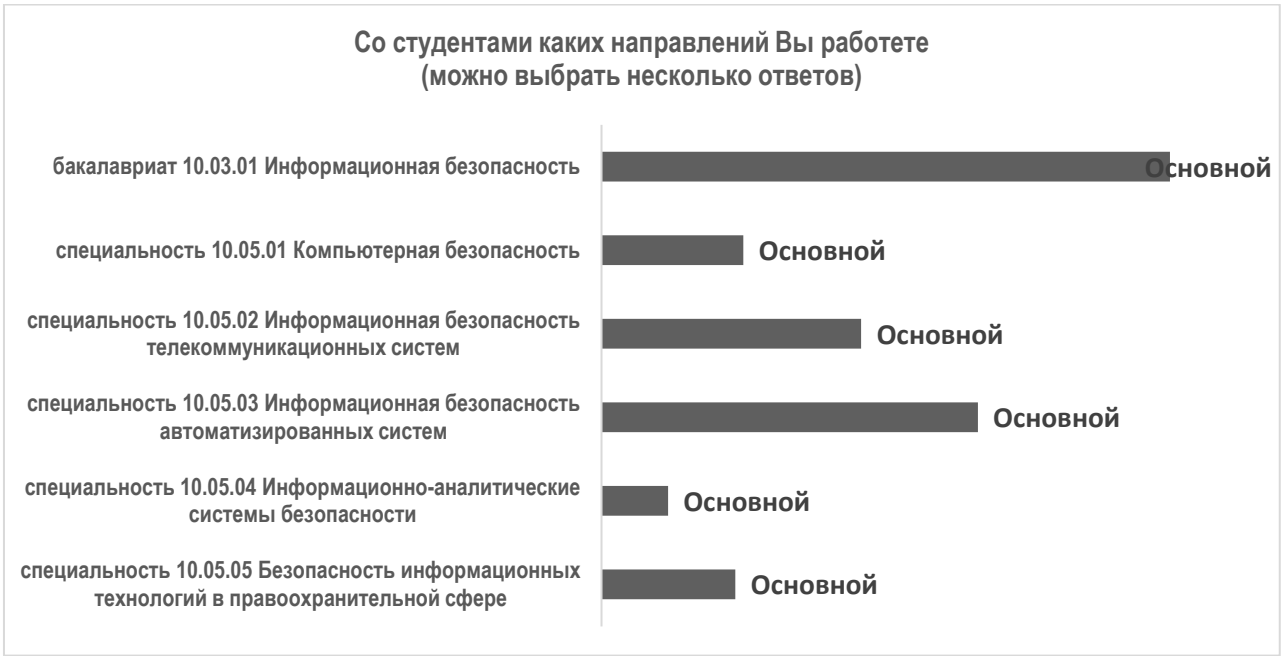

Рис. 4. Образовательные программы, в реализации которых участвуют респонденты (вопрос с множественным выбором, допускается более одного ответа) (%, n = 97)

Распределение групп респондентов по преподаваемым дисциплинам, формируемым компетенциям, стажу педагогической работы, региону работы и образовательным программам, в реализации которых они принимают участие, позволяет говорить о том, что в выборке представлены различные группы, что , в свою очередь, позволяет сделать заключение о довольно высокой репрезентативности результатов и целесообразности их использования при формировании предложения по программам повышения квалификации и переподготовки в области «Информационная безопасность».

2.3. Оценки работодателей и преподавателей востребованности компетенций специалиста по информационной безопасности

Преподаватели отмечают, что специалисты по информационной безопасности востребованы на рынке труда. Около 80 % полагают, что существует дефицит таких специалистов (рис. 5).

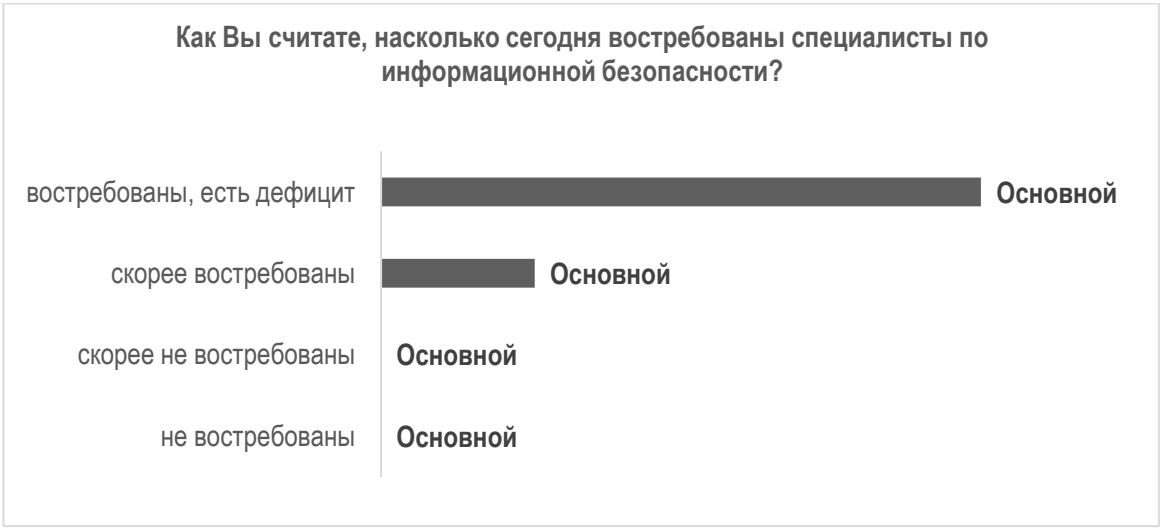

Рис. 5. Мнения преподавателей о востребованности специалистов в области информационной безопасности на рынке труда (%, *n* = 103)

30 % регулярно отслеживают изменения на рынке труда и еще 42 % отмечают, что обращают внимание на то, какие требования работодатели предъявляют к молодым специалистам в области информационной безопасности (рис. 6).

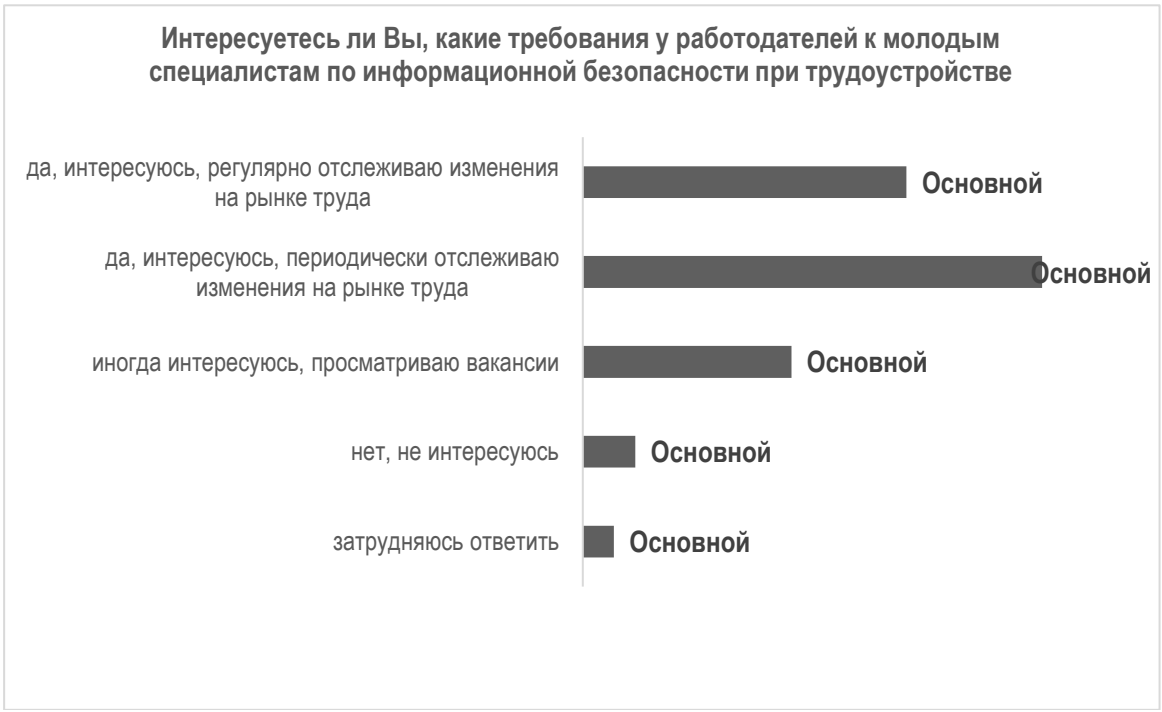

Рис. 6. Представления преподавателей о состоянии рынка труда в области информационной безопасности (%, *n* = 103)

Преподавателям было предложено оценить свои знания о трудовых функциях специалистов по информационной безопасности. Распределение оценок представлено на рис. 7.

Рис. 7. Представления преподавателей о трудовых функциях специалистов в сфере информационной безопасности (%, *n* = 103)

Также преподавателям было предложено ответить на вопрос о том, насколько достаточно их личных знаний, умений и навыков для организации профессиональной деятельности в подготовке специалистов информационной безопасности (распределение ответов – на рис. 8).

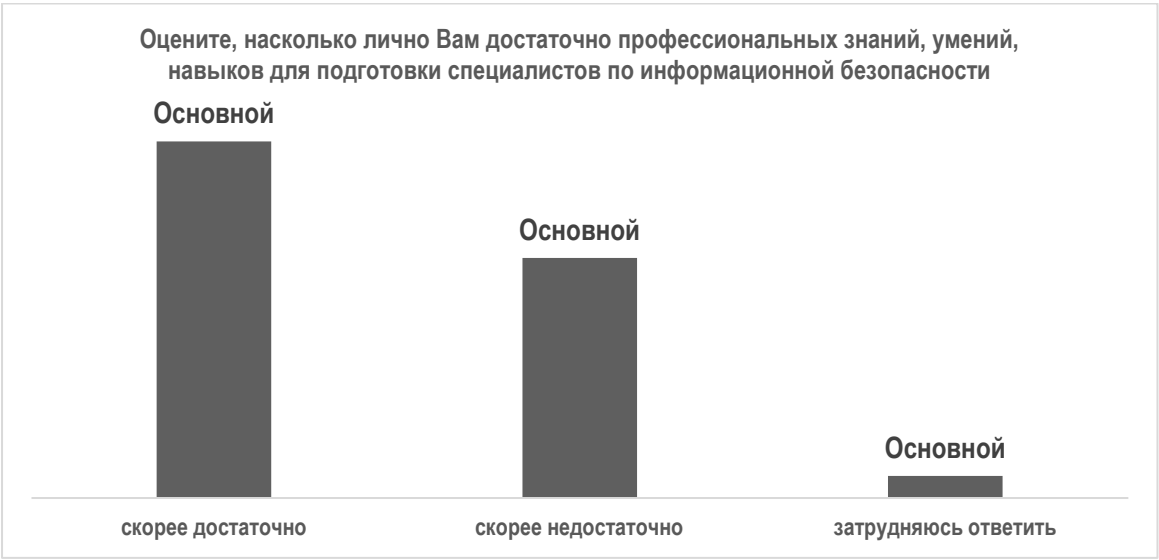

Рис. 8. Самооценка знаний, умений и навыков преподавателей, необходимых для подготовки специалистов по информационной безопасности (%, *n* = 103)

Почти 40 % участников опроса отметили, что им недостаточно знаний, умений и навыков для подготовки специалистов по информационной безопасности (рис. 8). Более 90 % хотели бы пройти повышение квалификации (рис. 9).

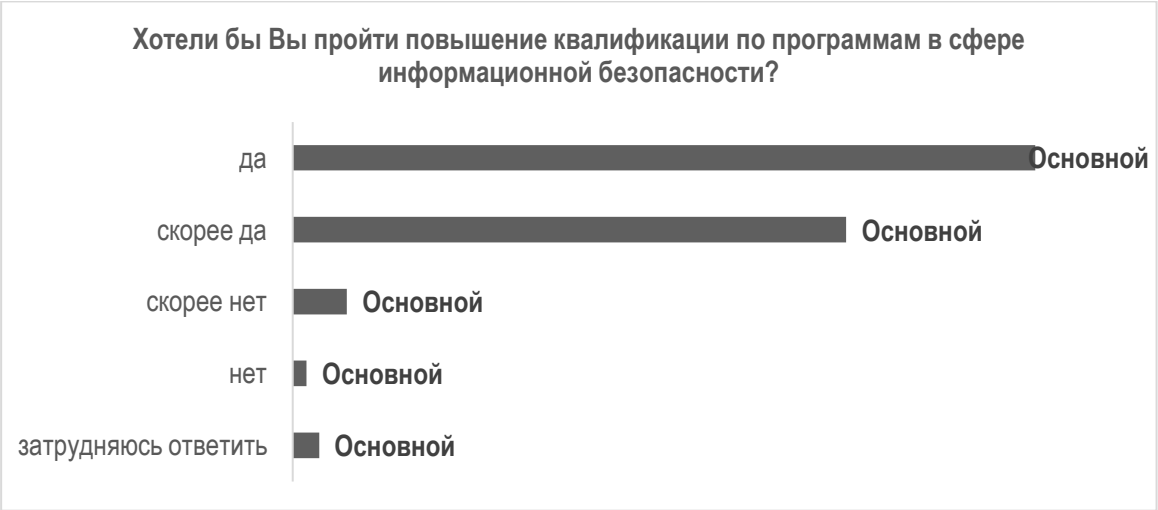

Рис. 9. Оценка потребности в обучении и/или повышении квалификации (%, *n* = 103)

В табл. 1 отражено распределение предпочтений преподавателей по продолжительности и формам программ обучения. Наибольший интерес представляют программы обучения продолжительностью 72 часа и мастер-классы по отдельным ситуациям в информационной безопасности.

Таблица 1. Предпочтения респондентов по программам повышения квалификации (вопрос с множественным выбором, допускается выбор более одного ответа)

	Программы повышения квалификации (по объему часов)	***N* (человек)**	**%**
1.	Повышение квалификации в объеме 36 ч.	30	29.1
2.	Повышение квалификации в объеме 72 ч.	57	55.3
3.	Повышение квалификации в объеме 144 ч.	30	29.1
4.	Программа профессиональной переподготовки в объеме более 250 ч.	26	25.2
5.	Мастер-классы по отдельным ситуациям в информационной безопасности	47	45.8
6.	Стажировка на предприятии	28	27.2

Высокий интерес преподаватели проявляют к краткосрочным видам обучения с участием отраслевых предприятий, а также к таким формам повышения квалификация, как тематические мастер-классы по отдельным ситуациям в информационной безопасности (45,8 %) и стажировка на предприятии (27.2 %). На развитие этих форм сотрудничества направлены н предложения по модернизации программ в области IT, где предлагается реализовать «возможности совместно с вузами модернизировать учебные программы, проводить совместные практики, привлекать к преподаванию представителей отрасли» (директор по развитию региональных образовательных проектов компании «Яндекс» С. Бражник); а также «участие работодателей в формировании образовательной повестки может проходить, во-первых, через их вовлечение в разработку и актуализацию ФГОС» и «развитие новых форматов партнерства», которые становятся возможны на основе Положения о практической подготовке обучающихся от 5 августа 2020 г. (заместитель министра науки и высшего образования РФ Д. Афанасьев) [20].

Для выявления востребованности тематики программ повышения квалификации по информационной безопасности респондентам предложен примерный перечень программ с возможностью выбрать все интересующие их программы. В табл. 2 отражена востребованность программ согласно предложенной примерной тематике.

Таблица 2. Востребованность у преподавателей программ повышения квалификации по информационной безопасности

Примерная тематика программ повышения квалификации по информационной безопасности	***N* респондентов, которые выразили интерес к программе**
10.03.01 Информационная безопасность. Базовые дисциплины	
1. Основы информационной безопасности	19
2. Сети и системы передачи информации	17
3. Программно-аппаратные средства защиты информации	27
4. Основы управления информационной безопасностью	30
5. Защита информации от утечки по техническим каналам	26
6. Методы и средства криптографической защиты информации	31
7. Организационное и правовое обеспечение информационной безопасности	24
8. Комплексная защита объектов информатизации	34
10.03.01 Информационная безопасность. Профессиональные дисциплины	
1. Безопасность операционных систем	21
2. Защита в операционных системах	19
3. Криптографические протоколы	20
4. Безопасность систем баз данных	20
5. Основы построения защищенных компьютерных сетей	20
6. Методы оценки безопасности компьютерных систем	35
7. Безопасность вычислительных сетей	16
8. Безопасность информационной инфраструктуры	20
9. Проектирование защищенных автоматизированных систем	28
10. Математическое моделирование систем и сетей телекоммуникаций	15
11. Проектирование элементов защищенных телекоммуникационных систем	10
12. Документоведение и конфиденциальное делопроизводство	16
13. Методы принятия организационно-технических решений	18
14. Моделирование процессов и систем защиты информации	21

15. Основы построения и функционирования специальных технических средств	6
16. Защита информации от несанкционированного доступа	30
17. Основы проектирования систем защиты объектов информатизации	22
10.05.01 Компьютерная безопасность. Базовые дисциплины	
1. Криптографические методы защиты информации	22
2. Защита в операционных системах	15
3. Основы построения защищенных баз данных	17
4. Защита программ и данных	18
5. Модели безопасности компьютерных систем	27
6. Криптографические протоколы	20
10.05.01 Компьютерная безопасность. Профессиональные дисциплины	
1. Анализ безопасности компьютерных систем	19
2. Математические методы защиты информации	18
3. Разработка защищенного программного обеспечения	17
4. Безопасность компьютерных систем и сетей (по отрасли или в сфере профессиональной деятельности)	15
5. Разработка систем защиты информации компьютерных систем объектов информатизации (по отрасли или в сфере профессиональной деятельности)	15
6. Информационно-аналитическая и техническая экспертиза компьютерных систем	28
10.05.02 Информационная безопасность телекоммуникационных систем. Базовые дисциплины	
1. Сети и системы передачи информации	14
2. Моделирование систем и сетей телекоммуникаций	13
3. Методы и средства криптографической защиты информации	15
4. Программно-аппаратные средства защиты информации телекоммуникационных систем	16
5. Комплексное обеспечение защиты информации телекоммуникационных систем	20
6. Проектирование защищенных телекоммуникационных систем	18
10.05.02 Информационная безопасность телекоммуникационных систем. Профессиональные дисциплины	
1. Информационная безопасность аэрокосмических ТКС	9
2. Разработка защищенных ТКС	14

3. Защита информации в радиосвязи и телерадиовещании	8
4. Управление безопасностью ТКСиС	7
5. Информационная безопасность мультисервисных телекоммуникационных сетей и систем на транспорте (по видам)	7
6. Системы подвижной цифровой защищенной связи	13
7. Техническая защита информации информационно-телекоммуникационных систем	19
10.05.03 Информационная безопасность автоматизированных систем. Базовые дисциплины	
1. Безопасность операционных систем	20
2. Безопасность вычислительных сетей	16
3. Безопасность систем баз данных	18
4. Управление информационной безопасностью	27
5. Разработка и эксплуатация автоматизированных систем в защищенном исполнении	24
6. Программно-аппаратные средства защиты информации	26
10.05.03 Информационная безопасность автоматизированных систем. Профессиональные дисциплины	
1. Безопасность открытых информационных систем	16
2. Безопасность автоматизированных систем в финансово-кредитной сфере	17
3. Анализ безопасности информационных систем	26
4. Разработка автоматизированных систем в защищенном исполнении	18
5. Безопасность автоматизированных систем на транспорте (по видам)	6
6. Безопасность автоматизированных систем управления технологическими процессами (по отрасли или в сфере профессиональной деятельности)	11
7. Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)	27
10.05.04 Информационно-аналитические системы безопасности. Базовые дисциплины	
1. Безопасность информационно-аналитических систем	11
2. Базы данных и экспертные системы	16
3. Распределённые информационно-аналитические системы	11
4. Моделирование автоматизированных информационно-аналитических систем	7
5. Технологии интеллектуальной обработки и анализа текстовых и мультимедийных данных	9
6. Обработка данных больших объемов	17

7. Принципы построения, проектирования и эксплуатации информационно-аналитических систем	13
10.05.04 Информационно-аналитические системы безопасности. Профессиональные дисциплины	
1. Автоматизация информационно-аналитической деятельности	16
2. Информационная безопасность финансовых и экономических структур	19
3. Технологии информационно-аналитического мониторинга	19
10.05.05 Безопасность информационных технологий в правоохранительной сфере. Базовые дисциплины	
1. Теория информационной безопасности и методология защиты информации	13
2. Информационное право	11
3. Защита и обработка документов ограниченного доступа	10
4. Организационная защита информации	13
5. Инженерно-техническая защита	8
6. Специальные информационные технологии в правоохранительной деятельности	14
7. Компьютерная криминалистика	30
10.05.05 Безопасность информационных технологий в правоохранительной сфере. Профессиональные дисциплины	
1. Компьютерная экспертиза	36
2. Организация и технологии обеспечения защиты информации	30

Ответы респондентов отражают востребованность широкого круга программ и дисциплин для бакалавриата и специалитета по базовым и профессиональным дисциплинам в области информационной безопасности.

Также преподавателям было предложено оценить востребованность дополнительных знаний, связанных с умением выстраивать педагогические и учебные процессы в цифровой образовательной среде, недостаточность которых остро ощущалась в период экстренного перехода в онлайн-формат обучения. Многочисленные исследования показывали серьезные сложности, которые возникли в организации учебных занятий, связанные именно с недостаточностью цифровых компетенций преподавателей. Так, в аналитическом докладе «Уроки стресс-теста» отмечено, что доля преподавателей, которые не смогли освоить цифровые инструменты работы, составила от 5 до 30 % в зависимости от вуза [21, С. 17]. При этом «дистанционный формат воспринимается как тотальное противопоставление традиционному по принципу «черное-белое». При жестком сравнении почти 90 % преподавателей отдают предпочтение традиционному формату с точки зрения качества образования, а 85 % считают традиционный формат более комфортным для себя» [21, С. 18]. Ответы преподавателей о востребованности обучения навыкам работы в цифровой образовательной среде представлены на рис. 10.

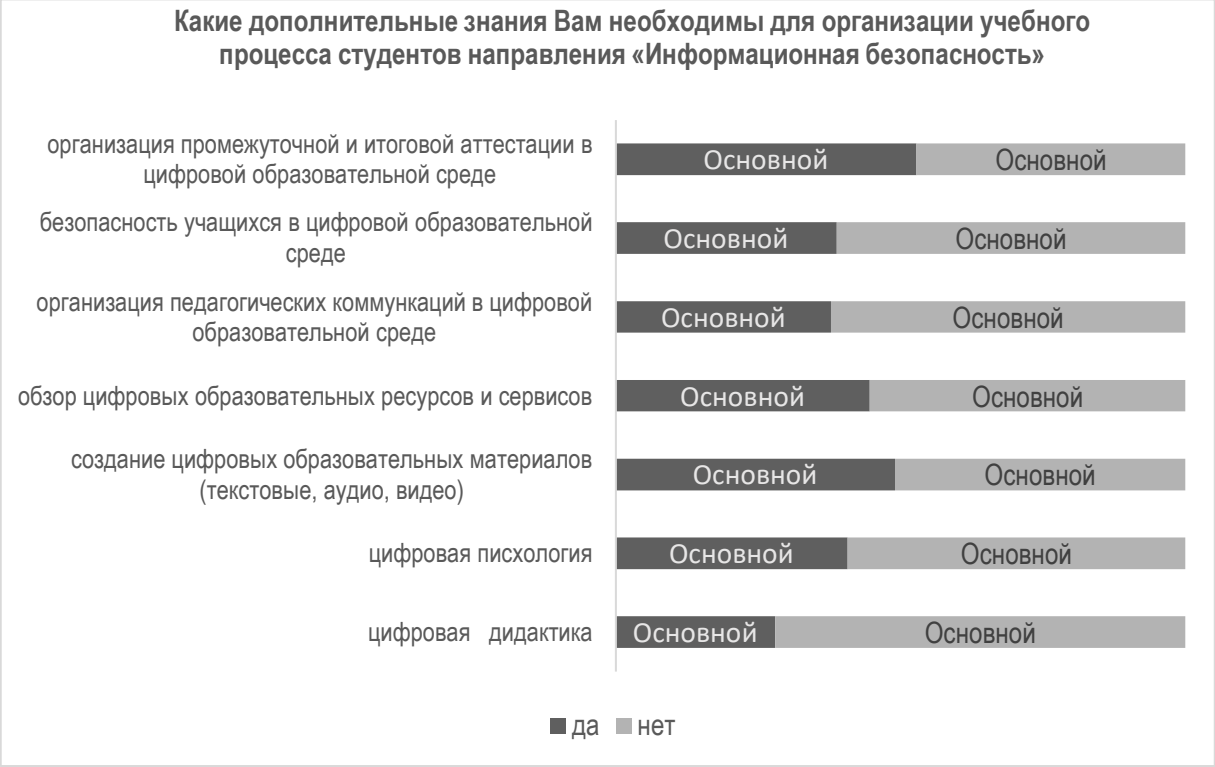

Рис. 10. Потребность в педагогических знаниях, необходимых для реализации учебного процесса для (%, n = 103)

Ответы отражают наличие потребности у преподавателей в развитии цифровых компетенций в организации педагогического и учебного процессов в цифровой образовательной среде, что выступает точкой роста педагогического сообщества. Подготовка специалистов по информационной безопасности без использования цифровых образовательных ресурсов и сервисов невозможна. Важны и востребованы также цифровые педагогические компетенции.

3. Заключение

Программы повышения квалификации по информационной безопасности по разной тематике востребованы. Преподаватели отдают предпочтение программам повышения квалификации в объеме 72 часов, мастер-классам и кейсам по отдельным ситуациям. Около 40 % респондентов отмечают недостаточность личных профессиональных знаний, умений и навыков, более 90 % выражают желание пройти повышение квалификации.

В целом преподаватели отмечают свою информированность о трудовых функциях специалистов по информационной безопасности (от 75 до 87 % в зависимости от специализации специалиста по информационной безопасности).

В условиях высокой востребованности специалистов по информационной безопасности и устаревания наличных компетенций необходима организация повышения квалификации преподавателей на регулярной основе при одновременном мониторинге сформированности цифровых компетенций и запросов преподавателей на повышение квалификации с целью выявления точек роста и организации опережающего обучения. Кроме того, необходим мониторинг запроса работодателя на компетенции выпускника образовательной программы.

Литература

1. Подведены итоги Пленума регионального отделения ФУМО по информационной безопасности. Режим доступа: https://sibsutis.ru/news/3701575/.
2. *Зива С. В., Захаров Д. И.* Принципы построения и опыт реализации учебного курса «Прикладные вопросы информационной безопасности» // Современные информационные технологии и ИТ-образование. 2020. Т. 16, № 4. С. 980–989. DOI 10.25559/SITITO. 16.202004.980-989.
3. *Сухомлин В. А., Белякова О. С., Климина А. С., Полянская М. С., Русанов А. А.* Модель цифровых навыков кибербезопасности 2020 // Современные информационные технологии и ИТ-образование. 2020. № 16 (3). С. 695–710. DOI 10.25559/ SITITO.16.202003.695-710.
4. *Авдеева Е. С., Миронова В. В.* Формирование групп стратегических профессий как один из инструментов достижения стратегической конкурентоспособности предприятий // Известия Юго-Западного государственного университета. Серия: Экономика. Социология. Менеджмент. 2017. Т. 7, № 2(23). С. 148–160.
5. *Цацкина Е. П., Ляхова Е. Г., Мороз Н. Ю.* О лингвистической подготовке кадров по информационной безопасности на этапе перехода к цифровой экономике // Обзор педагогических исследований. 2021. № 3 (6). С. 162–167.
6. *Сухомлин В. А., Белякова О. С., Климина А. С., Полянская М. С., Зубарева Е. В., Якушин А. В.* Архитектура и принципы разработки куррикулума для дисциплины «Кибербезопасность» // Современные информационные технологии и ИТ-образование. 2020. № 16(4). С. 927–939.
7. *Дрожжинов В. И.* SFIA-система профессиональных стандартов в сфере ИТ эпохи цифровой экономики // Современные информационные технологии и ИТ-образование. 2017. № 13 (1). С. 132–143.
8. *Цветкова О. Н.* Информационная безопасность в условиях цифровой экономики в России // Самоуправление. 2021. № 5 (127). С. 440–443.
9. *Малюк А. А., Полянская О. Ю.* Комментарии к Доктрине информационной безопасности Российской Федерации. М.: Горячая линия – Телеком, 2018. 102 с. ISBN 978-5-9912-0711-9.
10. *Малюк А. А., Полянская О. Ю.* Этика в сфере информационных технологий // Вестник Российского гуманитарного научного фонда. 2011. № 4 (65). С. 72–77.
11. Профессиональная этика инженера: Опыт коллективной рефлексии для магистр(ант)ов и профессоров: коллективная монография / под ред. В.И. Бакштановского; составители А. Ю. Согомонов, М. В. Богданова. Тюмень: НИИ ПЭ ТИУ, 2018. 246 с.
12. *Olifirov A. V., Makoveichuk K. A., Petrenko S. A.* Improving the courses of educational programs on information security smart grid // CEUR Workshop Proceedings: 4, Yalta, Crimea, 16–21 Sept. 2019, Yalta, Crimea, 2021. P. 340–350.
13. *Малюк А. А., Малюк З. П.* Актуальные вопросы создания системы массового обучения культуре информационной безопасности // Безопасность информационных технологий. 2021. № 28 (4). С. 6–21. DOI 10.26583/bit.2021.4.01.
14. *Бушуев А. Л., Деревцова И. В., Мальцева Ю. А., Терентьева В. Д.* Роль информационной безопасности в условиях цифровой экономики // Baikal Research Journal. 2020. № 11 (1). С. 6. DOI 10.17150/2411-6262.20.11(1).6.
15. *Пилипенко В. В., Кузнецова М. А.* Анализ российского рынка информационной безопасности в контексте развития цифровой экономики // Инновационная экономика. 2019. № 3 (20). С. 4–12.
16. *Антонова Н. Л., Бабикова И. И.* Информационная безопасность в условиях цифровой экономики // Заметки ученого. 2020. № 13. С. 111–117.
17. *Струкова Е. Г., Микиденко Н. Л, Сторожева С. П.* Взаимодействие с работодателем как инструмент формирования образовательной программы // Информационная безопасность цифровой экономики: Материалы XVII научно-теоретической конференции VIII Пленума регионального отделения Федерального учебно-методического объединения в системе

высшего образования по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» по Сибирскому и Дальневосточному федеральным округам (СибРОУМО), Новосибирск, 13–15 октября 2021 года. Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2021. С. 78–94.
18. Кибербезопасность: защита информации как драйвер роста бизнеса // Сайт: Мегафон (megafon.ru). URL: Кибербезопасность: защита информации как драйвер роста бизнеса (megafon.ru) (дата обращения: 28.08.2022).
19. В Хабаровске проходит форум информационной безопасности «Сибирь – Дальний Восток-2022» 30.06.2022 // Сайт: Министерство образования и науки Хабаровского края. URL: https://minobr.khabkrai.ru/events/Novosti/3606 (дата обращения: 28.08.2022).
20. *Батанов А., Брылякова М.* От цифровизации – к аккредитационной революции. Репортаж с парламентских слушаний в Комитете Госдумы РФ по образованию и науке. Апрель. 2022 // Сайт: Аккредитация в образовании. URL: https://akvobr.ru/new/publications/273 (дата обращения: 28.08.2022).
21. Аналитический доклад «Уроки стресс-теста: российские вузы в условиях пандемии и после нее». Июнь, 2020. URL: 003_Доклад.pdf (yandex.ru)(дата обращения: 28.08.2022).

Статья поступила в редакцию 08.08.2022;
переработанный вариант – 30.08.2022.

Микиденко Наталья Леонидовна
кандидат социологических наук, доцент кафедры социально-коммуникативных технологий, Сибирский государственный университет телекоммуникаций и информатики (630102, Новосибирск, ул. Кирова, 86), тел. (383) 2-693-929, e-mail: nl_nsk@mail.ru.

Сторожева Светлана Петровна
кандидат культурологии, доцент кафедры социально-коммуникативных технологий, Сибирский государственный университет телекоммуникаций и информатики, e-mail: s_storozheva@sibguti.ru.

Струкова Елена Геннадьевна
начальник управления маркетинга и развития образования, Сибирский государственный университет телекоммуникаций и информатики (630102, Новосибирск, ул. Кирова, 86), e-mail: strukova@sibguti.ru.

Staff assistance of educational programs in the sphere of information security: design and development problems

Natalia L. Mikidenko
Candidate of Sociology, Assistant Professor, Assistant Professor Department of Social and Communication Technology (SibSUTIS, Novosibirsk, Russia), nl_nsk@mail.ru.

Svetlana P. Storozheva
Candidate of Culturology, Assistant Professor, Assistant Professor Department of Social and Communication Technology (SibSUTIS, Novosibirsk, Russia), s_storozheva@sibguti.ru.

Elena G. Strukova
Head of Marketing and Education Development Department (SibSUTIS, Novosibirsk, Russia), strukova@sibguti.ru.

An increase in civilization risks and threats, and the development of information technologies actualize the questions of information security. The need for information security specialists is sharply increasing. This requires the solution of a number of managerial, organizational, substantive issues related to the organization and implementation of educational programs on information security including staffing issues. In such conditions the issues of teaching staff potential development, formation of the necessary up-to-date knowledge and competences of teachers for qualitative training of future specialists become urgent and in-demand. Mass retraining of teachers becomes the most important task in providing information security specialists for the digital economy. The methodological basis of the study is the provisions of education sociology reflecting the problems of matching the human resources needs for the digital economy, import substitution and national security with the quantity and quality of specialist training in higher educational institutions of vocational education.

The aim of the research is to identify employers' demands for information security specialists' competences for formation of professional educational programs and demands of teachers engaged in information training for actual knowledge, abilities, skills, which availability will ensure innovativeness in training of young specialists. The main hypothesis was that there is a mismatch between the demands of the external environment of higher education, above all, employers and the capabilities of the educational system, there is an urgent need to increase the capacity of teachers involved in training professionals in the field of information security. The reasons for this mismatch are (1) the dynamic development of technology, the emergence and increase of cyber threats and cyber incidents, (2) the presence of objective problems in the development of educational institutions staff capacity - the low proportion of young personnel, inadequate interaction between educational institutions and industrial and research centers, inadequate scientific and educational mobility of teaching staff for skills development.

The needs of employers and teachers have been identified on the basis of empirical research (autumn, 2021) conducted by the authors. 103 teachers and 109 employees of enterprises which carry out functions on maintenance of information security of organizations and enterprises (mainly SFD) participated in sociological research.

Results: requirements of employers and teachers on information security actual knowledge, abilities, actual programs of professional development and professional retraining were revealed. The practical significance of the results is that the study can reveal the problems of design and development of educational programs on information security and formulate recommendations for the design.

Keywords: information security, personnel potential, higher school teachers, educational program.

References

1. *Podvedeny itogi plenuma regional''nogo otdeleniya fumo po informatsionnoi bezopasnosti* [The results of the Plenum of the Regional Branch of the Information Security FUMO are summarized], available at: https://sibsutis.ru/news/3701575/ (accessed 05.07.2022).
2. Ziva S. V., Zakharov D. I. Printsipy postroeniya i opyt realizatsii uchebnogo kursa "Prikladnye voprosy informatsionnoi bezopasnosti" [Principles of construction and experience in the implementation of the training course "Applied issues of information security"]. *Sovremennye informatsionnye tekhnologii i IT-obrazovanie*, 2020, vol.16, no. 4, pp. 980-989. DOI 10.25559/SITITO.16.202004.980-989.
3. Sukhomlin V. A., Belyakova O. S., Klimina A. S., Polyanskaya M. S., Rusanov A. A. Model' tsifrovykh navykov kiberbezopasnosti 2020 [Model of digital cybersecurity skills 2020]. *Sovremennye informatsionnye tekhnologii i IT-obrazovanie*, 2020, vol.16, no. 3, pp. 695-710. DOI 10.25559/SITO.16.202003.695-710.
4. Avdeeva E. S., Mironova V. V. Formirovanie grupp strategicheskikh professii kak odin iz instrumentov dostizheniya strategicheskoi konkurentosposobnosti predpriyatii [Formation of groups of strategic professions as one of the tools for achieving the strategic competitiveness of enterprises]. *Izvestiya YUgo-Zapadnogo gosudarstvennogo universiteta. Seriya: EHkonomika. Sotsiologiya. Menedzhment*, 2017, vol. 7, no. 2(23), pp. 148-160.
5. Tsatskina E. P., Lyakhova E. G., Moroz N. Y. O lingvisticheskoi podgotovke kadrov po informatsionnoi bezopasnosti na etape perekhoda k tsifrovoi ekonomike [On linguistic training in information security at the stage of transition to digital economy]. *Obzor pedagogicheskikh issledovanij*, 2021, no. 3(6), pp. 162-167.

6. Sukhomlin V. A., Belyakova O. S., Klimina A. S., Polyanskaya M. S., Zubareva E. V., Yakushin A. V. Arkhitektura i printsipy razrabotki kurrikuluma dlya distsipliny «Kiberbezopasnost'» [Architecture and principles of curriculum development for the discipline of «Cybersecurity»]. *Sovremennye informatsionnye tekhnologii i IT-obrazovanie*, 2020, no. 16(4), pp. 927-939. DOI 10.25559/SITITO.16.202004.927-939
7. Drozhzhinov V. I. SFIA-sistema professional'nykh standartov v sfere IT epokhi tsifrovoi ekonomiki [SFIA-system of professional standards in IT in the era of digital economy]. *Sovremennye informatsionnye tekhnologii i IT-obrazovanie*, 2017, no. 13(1), pp. 132-143.
8. Tsvetkova O. N. Informatsionnaya bezopasnost' v usloviyakh tsifrovoi ekonomiki v Rossii [Information security in the conditions of digital economy in Russia]. *Samoupravlenie*, 2021, no. 5(127), pp. 440-443.
9. Malyuk A. A., Polyanskaya O. Yu. *Kommentarii k Doktrine informatsionnoj bezopasnosti Rossijskoj Federatsii* [Comments to the Doctrine of Information Security of the Russian Federation]. Moscow: Nauchno-tekhnicheskoe izdatel'stvo "Goryachaya liniya-Telekom", 2018, 102 p. ISBN 978-5-9912-0711-9.
10. Malyuk A. A., Polyanskaya O. Yu. Etika v sfere informatsionnykh tekhnologii [Ethics in the sphere of information technologies]. *Vestnik Rossijskogo gumanitarnogo nauchnogo fonda*, 2011, no. 4(65), pp. 72-77.
11. A.Yu. Sogomonov, M.V.Bogdanov *Professional'naya etika inzhenera* [Professional Ethics of Engineer]. Ed. V.I. Bakshtanovsky. Tyumen, Nauchno-issledovatel'skii institut politicheskoi ekonomiki Tyumenskogo issledovatel'skogo universiteta, 2018. 246 p.
12. Olifirov A. V., Makoveichuk K. A., Petrenko S. A. Improving the courses of educational programs on information security smart grid. *CEUR Workshop Proceedings*, 4, Yalta, Crimea, 16-21 September, 2019, Yalta, Crimea, 2021, pp. 340-350.
13. Malyuk A. A., Malyuk Z. P. Aktual'nye voprosy sozdaniya sistemy massovogo obucheniya kul'ture informatsionnoi bezopasnosti [Actual issues of creating a system of mass training culture of information security]. *Bezopasnost' informatsionnykh tekhnologij*, 2021, vol. 28, no.4, pp. 6-21. DOI 10.26583/bit.2021.4.01
14. Bushuyev A. L., Derevtsova I. V., Maltseva Yu. A., Terentyeva V. D. Rol' informatsionnoi bezopasnosti v usloviyakh tsifrovoi ekonomiki [The Role of Information Security in the Digital Economy]. *Baikal Research Journal*, 2020, no. 11(1), pp. 6-6. DOI 10.17150/2411-6262.20.11(1).6.
15. Pilipenko V. V., Kuznetsova M. A. Analiz rossiiskogo rynka informatsionnoi bezopasnosti v kontekste razvitiya tsifrovoi ekonomiki [Analysis of the Russian information security market in the context of digital economy development]. *Innovatsionnaya ehkonomika*, 2019, no. 3(20), pp. 4-12.
16. Antonova N.L., Babikova I.I. Informatsionnaya bezopasnost' v usloviyakh tsifrovoi ekonomiki [Information Security in the Digital Economy]. *Zametki uchenogo*, 2020, no. 13, pp. 111-117.
17. Strukova E. G., Mikidenko N. L., Storozheva S. P. Vzaimodeistvie s rabotodatelem kak instrument formirovaniya obrazovatel'noi programmy [Interaction with employer as a tool for educational program formation]. *Informatsionnaya bezopasnost' tsifrovoi ekonomiki XVII nauchno-teoreticheskaja konferentsija VIII Plenuma regional'nogo otdeleniya Federal'nogo uchebno-metodicheskogo ob"edineniya v sisteme vysshego obrazovaniya po ukrupnennoi gruppe spetsial'nostei i napravlenii podgotovki 10.00.00 "Informatsionnaya bezopas-nost'" po Sibirskomu i Dal'nevostochnomu federal'nym okrugam (SibROUMO)*, Novosibirsk, Sibirskii gosudarstvennyi universitet telekommunikatsii i informatiki, 13–15 October, 2021, pp. 78-94.
18. *Cybersecurity: information protection as a business growth driver*, available at: `Cyber security: information protection as a business growth driver (megafon.ru)` (accessed 05.07.2022).
19. *Khabarovsk hosts information security forum "Siberia Far East-2022" 30.06.2022*, available at: `https://minobr.khabkrai.ru/events/Novosti/3606` (accessed 05.07.2022).
20. Batanov A., Brylyakova M. From digitalization to accreditation revolution. Report from parliamentary hearings in State Duma Committee on Education and Science. April, 2022. Website: Accreditation in Education. available at: `https://akvobr.ru/new/publications/273` (accessed 05.07.2022).
21. *Uroki-stress-testa: rossijskie vuzy v usloviyakh pandemii i posle nee* [Analytical Report "Stress-Test Lessons: Russian Universities in Pandemic and Post-Pandemic Conditions"] June, 2020. available at: `003_Доклад.pdf (yandex.ru)` (accessed 05.07.2022).

УДК 519.86
DOI: 10.55648/1998-6920-2022-16-3-101-111

Прогнозирование местоположения мобильного абонента в сети Wi-Fi

Ю. С. Лизнева, Е. В. Кокорева, А. Е. Костюкович[1]

Для позиционирования в сети Wi-Fi наиболее распространён механизм трилатерации, основанный на измерении уровня мощности принимаемого сигнала RSSI и вычислении расстояний от абонентского устройства до видимых точек доступа. Применение этого механизма требует полного представления о конфигурации помещений, количестве и материале препятствий, разделяющих передающую и приёмную антенны, которое невозможно получить из значений RSSI. В данной статье исследуются возможности таксонометрического метода принятия решений для прогнозирования местоположения мобильных объектов в сети Wi-Fi внутри помещений с целью восполнения недостающих данных о параметрах помещений и препятствий, разделяющих точки доступа и мобильные объекты.

Ключевые слова: Wi-Fi, позиционирование, таксонометрический метод, принятие решений, квазирасстояние.

1. Введение

Для реализации системы определения местоположения, в частности, для повышения точности вычисления координат мобильного объекта необходимо тщательное территориально-частотное планирование сети Wi-Fi [1]. На сегодняшний день не имеется методики территориально-частотного планирования локальной беспроводной сети, которая подходила бы для эффективной работы системы определения местоположения, поскольку все существующие методики нацелены на построение сети Wi-Fi, предназначенной для доставки интернет-контента клиентам с заданной пропускной способностью.

Одним из наиболее точных методов определения местоположения мобильного объекта в сети Wi-Fi является метод трилатерации или мультилатерации [2–6]. Этот метод позволяет по расстояниям от мобильного объекта до каждой из трёх или более точек доступа AP (англ. *Access Point*) вычислять координаты местоположения этого объекта относительно конкретных помещений внутри зданий [7–8].

Расстояния от мобильного объекта до каждой из точек доступа определяются по результатам измерения уровня мощности сигнала на входе приёмного устройства RSSI (англ. *Received Signal Strength Indicator*) и последующего их вычисления с помощью моделей распространения радиоволн внутри помещений [9–12].

Для корректного применения моделей распространения радиоволн требуется полное представление о конфигурации помещений, количестве и материале препятствий, разделяющих передающую и приёмную антенны мобильных устройств и точек доступа. В большинстве случаев это невозможно, и измерение только уровня мощности не позволяет получить эти данные, поскольку множество случайных факторов влияют на уровень RSSI и все полу-

[1] Работа выполнена при поддержке Министерства цифрового развития, связи и массовых коммуникаций в рамках НИОКТР АААА-А20-120070290025-0.

чаемые оценки расстояний и координат объекта имеют статистический (вероятностный) характер [13–14]. Предлагается использовать для позиционирования комбинированную методику, включающую в себя методы интеллектуального анализа данных на карте измерения параметров сигнала и латерации.

Применение статистических или эвристических методов принятия решений в системах позиционирования позволяет частично преодолеть отсутствие необходимой для применения механизма латерации информации о параметрах помещения. Данные методы служат для того, чтобы получить грубую (предварительную) оценку местоположения мобильного клиента относительно каждой из видимых для него точек доступа, чтобы на этапах применения трилатерации можно было подобрать подходящие модели распространения радиоволн внутри помещений, а также параметры, входящие в математические выражения, описывающие эти модели [15].

Перед разработчиками стоит задача выбрать критерий принятия решений, позволяющий получить более достоверную оценку расстояний и местоположения мобильного клиента. В данной статье для получения такой оценки с заданной вероятностью рассмотрено применение *таксонометрического* метода [16–17].

Под термином таксонометрия в рамках данной статьи будем понимать математический метод ранжирования и группировки множества помещений по расстояниям до множества точек доступа в сети Wi-Fi и по уровням мощности радиосигнала RSSI. Таксонометрический метод позволяет ввести понятие квазирасстояний, используемых в качестве весовых коэффициентов при учёте уровней мощности радиосигнала RSSI, например, в центре каждого помещения относительно каждой точки доступа.

Таксонометрический анализ включает в себя совокупность математических методов, предназначенных для формирования относительно отдалённых друг от друга групп объектов, близко расположенных или тесно связанных между собой.

Далее рассматривается применение таксонометрического метода при прогнозировании местоположения точки приёма сигнала на основе экспериментально полученных уровней RSSI для конкретной конфигурации помещений.

2. Формирование матриц, содержащих параметры помещений

Таксонометрический метод опирается на работу с матрицами. В данном случае матрицы будут содержать различные параметры, являющиеся характеристиками зданий и помещений, внутри которых осуществляется процесс позиционирования, например, расстояния между центрами отдельных комнат здания и точками доступа сети Wi-Fi.

На рис. 1 представлен план конкретных помещений и размещения точек доступа, а также предварительно составленные тепловые карты радиопокрытия для этих помещений.

Для каждой комнаты, представленной на рис. 1, по теореме Пифагора рассчитывается расстояние между точками доступа AP и центром соответствующей комнаты:

$$R = \sqrt{\left(X_c - X_{AP}\right)^2 + \left(Y_c - Y_{AP}\right)^2}\,, \tag{1}$$

где X_c, Y_c – координаты центра комнаты, а X_{AP}, Y_{AP} – координаты точки доступа.

В табл. 1 представлены координаты AP. Координаты объекта задаются в метрах и измеряются относительно угла здания, который будем считать началом координат.

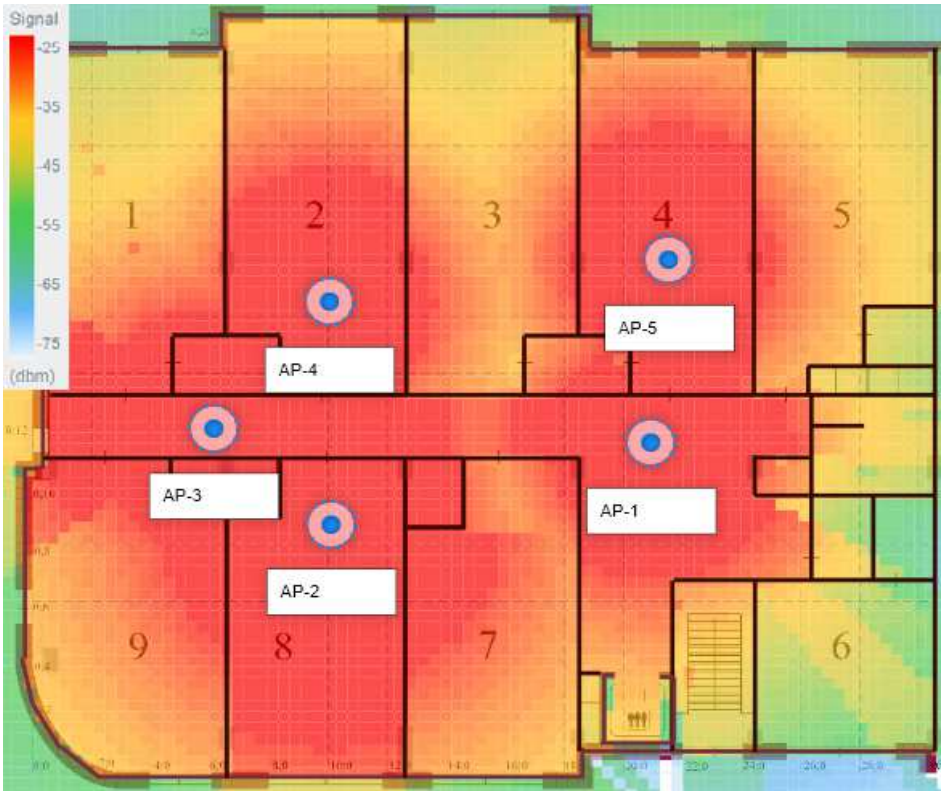

Рис. 1. План помещений и размещения точек доступа

Таблица 1. Координаты точек доступа

AP	X_{AP}, м	Y_{AP}, м
AP_1	20.0	11.5
AP_2	9.0	8.0
AP_3	5.8	12.2
AP_4	9.0	15.0
AP_5	22.0	17.5

В табл. 2 приведены координаты центров соответствующих комнат. Координаты также заданы относительно угла здания.

Таблица 2. Координаты центров комнат

Координаты / № комнаты	X_C, м	Y_{AP}, м
1	3.6	18.6
2	9.6	18.6
3	15.6	18.6
4	21.6	18.6
5	27.6	18.6
6	27.6	6.0
7	15.6	6.0
8	9.6	6.0
9	3.6	6.0

Табл. 3 содержит результаты вычисления расстояний между точками доступа и центрами помещений с помощью формулы (1).

На основании вычисленных расстояний, представленных в табл. 3, определяются весовые коэффициенты a_{ij} сравнительной значимости сигнала от AP_j в соответствующей комнате, здесь i – номер комнаты, j – номер точки доступа. При этом наименьшему расстоянию между точкой приёма и точкой доступа соответствует значение коэффициента 1, а наибольшему – 5. Полученное распределение весов сведено в табл. 4. В эксперименте были задействованы девять помещений и пять точек доступа.

Таблица 3. Результаты вычисления расстояний между точками доступа и центрами помещений

№ AP / № комнаты	AP_1	AP_2	AP_3	AP_4	AP_5
1	17.9	11.9	6.8	6.5	18.4
2	12.6	10.6	7.4	3.7	12.5
3	8.4	12.5	11.7	7.5	6.5
4	7.3	16.5	17.1	13.1	1.2
5	10.4	21.4	22.7	18.9	5.7
6	9.4	18.7	22.7	20.7	12.8
7	7.0	6.9	11.6	11.2	13.2
8	11.8	2.1	7.3	9.0	16.9
9	17.3	5.8	6.6	10.5	21.7

Таблица 4. Весовые коэффициенты, соответствующие расстояниям от центров комнат до точек доступа

№ AP / № комнаты	AP_1	AP_2	AP_3	AP_4	AP_5
1	4	3	2	1	5
2	5	3	2	1	4
3	3	5	4	2	1
4	2	4	5	3	1
5	2	4	5	3	1
6	1	3	5	4	2
7	2	1	4	3	5
8	4	1	2	3	5
9	4	1	2	3	5

3. Формирование образцовых карт помещений

На данном этапе по результатам экспериментальных данных измерений уровня RSSI необходимо сформировать образцовые карты для указанных на рис. 1 помещений.

В ходе эксперимента было проведено более 500 измерений в центре каждого помещения. Обработка экспериментальных результатов показала, что уровень RSSI, характеризующий радиообстановку помещений, описывается нормальным распределением, поэтому в табл. 5 для описания образцовой карты каждой комнаты достаточно двух параметров выборочной совокупности уровней сигнала:

– среднее арифметическое, или математическое ожидание (МО);
– среднеквадратическое отклонение (СКО).

Результаты расчета, которые можно наблюдать в табл. 5 и на рис. 2, представляют собой радиообразы, характеризующие электромагнитную обстановку в каждой комнате.

Таблица 5. Радиообразы комнат по уровню средней мощности принимаемого сигнала

№ комнаты	Показатель, дБм	AP_1	AP_2	AP_3	AP_4	AP_5
1	МО	–70.5	–59.9	–50.6	–51.2	–63.4
	СКО	3.1	3.7	3.8	2.7	3.4
2	МО	–66.9	–51.3	–51.8	–42.0	–56.5
	СКО	3.5	4.4	3.9	4.7	2.9
3	МО	–59.5	–62.2	–59.6	–48.4	–51.8
	СКО	2.9	4.3	3.4	5.7	4.9
4	МО	–52.3	–65.8	–69.0	–57.4	–40.0
	СКО	6.2	3.7	2.1	3.2	2.5
5	МО	–58.4	–74.7	–73.9	–64.9	–50.1
	СКО	3.6	3.3	3.4	4.3	2.6
6	МО	–54.3	–70.2	–75.8	–73.2	–60.6
	СКО	5.1	5.8	2.3	2.8	2.8
7	МО	–55.6	–50.8	–59.4	–57.8	–58.5
	СКО	4.4	4.5	4.3	5.6	3.5
8	МО	–62.6	–39.7	–51.3	–53.9	–68.7
	СКО	3.1	7.5	4.9	5.5	3.1
9	МО	–66.2	–49.1	–48.3	–64.2	–71.8
	СКО	2.8	2.6	4.5	2.8	3.9

4. Тестирование таксонометрического метода

Для тестирования таксонометрического метода были использованы данные об уровнях RSSI, полученные экспериментальным путём в конкретных помещениях здания, изображённого на рис. 1.

На рис. 2 приведена тепловая карта покрытия пяти точек доступа, совмещённая с диаграммами радиообразов помещений, полученными в результате статистической обработки экспериментальных данных.

Поскольку радиообразы комнат, выведенные из средних значений уровня RSSI относительно каждой из пяти точек доступа (табл. 5, рис. 2), уникальны, существует возможность однозначного определения каждого помещения. Однако, исходя из значений СКО (табл. 5), следует заметить, что нельзя полностью исключить ошибочное определение помещения.

Результаты тестирования метода в описанных помещениях приведены ниже.

4.1. Этапы реализации таксонометрического метода

На сервер определения местоположения мобильным клиентом был отправлен набор (вектор) измерений RSSI сигналов, полученных от всех видимых устройством точек доступа:

$$x_{Э} = \left| x_{AP_1} \;\; x_{AP_2} \;\; x_{AP_3} \;\; x_{AP_4} \;\; x_{AP_5} \right|.$$

Полученные сервером значения должны быть нормализованы относительно математического ожидания и среднеквадратического отклонения RSSI из табл. 5, вычисленных для каждой комнаты с использованием формулы:

$$z_{ij} = \frac{x_{APj} - \overline{X}_{ij}}{\sigma_{ij}}, \tag{2}$$

где $\overline{X}_{ij}$ – среднее арифметическое RSSI в i-й комнате от j-й АР;

σ_{ij} – среднеквадратическое отклонение.

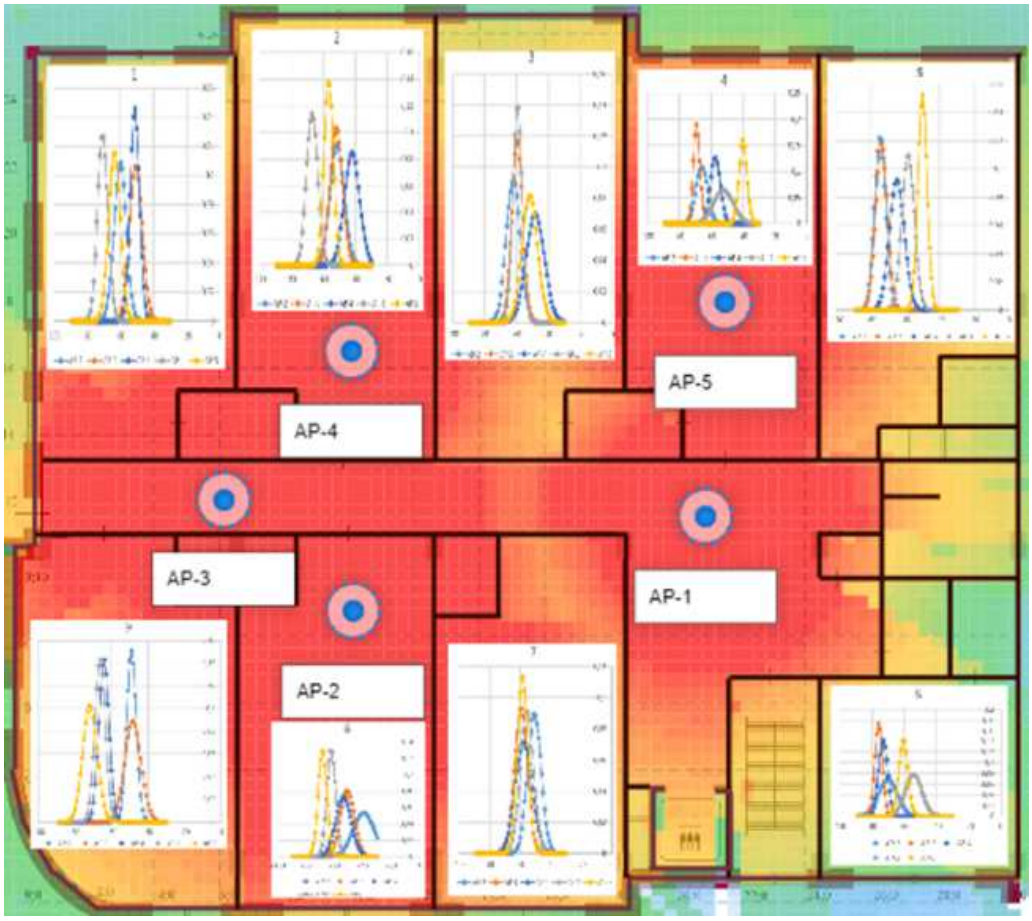

Рис. 2. Радиообразы помещений для пяти точек доступа

Проведение процедуры нормализации исключает влияние абсолютных величин и вариации значений самих показателей.

Из нормализованной матрицы производится формирование вектора эталонных или ближайших точек доступа, определённых по наименьшему нормированному значению в каждой строке, которое соответствует определённой комнате.

Вектор ближайших АР выглядит следующим образом:

$$Z = \begin{vmatrix} Z_1 \\ Z_2 \\ \vdots \\ Z_n \end{vmatrix}.$$

Все полученные результаты сводятся в таблицу, подобную табл. 6.

Таблица 6. Нормализованная матрица и вектор ближайших АР

№ АР / № комнаты	AP_1	AP_2	AP_j	AP_n	Z
1	z_{11}	z_{12}	…	z_{1n}	Z_1
2	z_{21}	z_{22}		z_{2n}	Z_2
i	…			…	…
4	z_{k1}	z_{k2}		z_{kn}	Z_k

Теоретическое определение комнаты, в которой находится мобильный абонент, осуществляется на основе расчёта квазирасстояний (рейтинговых значений комнаты относительно точки приёма сигнала) R_i по формуле:

$$R_i = \sum_{j=1}^{n} r_{ij}\,, \tag{3}$$

где

$$r_{ij} = a_{ij} \cdot \left(z_{ij} - Z_j\right)^2. \tag{4}$$

В формулах (3)–(4) r_{ij} – квазирасстояния относительно *j*-х точек доступа, а a_{ij} – весовые коэффициенты из табл. 4.

Полученное в результате наименьшее квазирасстояние R_i должно соответствовать местонахождению искомого объекта.

4.2. Результаты применения таксонометрического метода

Чтобы оценить достоверность результатов таксонометрического анализа, рассмотрены конкретные примеры статистической обработки параметров, измеренных в некоторой точке рассмотренного выше здания.

Например, сервером определения местоположения получен вектор измерений RSSI:

$$x_Э = \left|-68 \quad -52 \quad -58 \quad -45 \quad -55\right|.$$

Известно, что $x_Э$ – это результат измерений, произведённых в комнате № 2.

Элементы вектора нормируются относительно математических ожиданий и средних квадратических отклонений уровней мощности сигнала в каждой комнате, взятых из табл. 5.

Нормализованная матрица помещается в табл. 7, в последнем столбце которой располагается вектор эталонных АР, соответствующих минимальным значениям строк данной матрицы.

По формулам (3)–(4) рассчитываются квазирасстояния для нормализованных уровней сигнала от каждой точки доступа и общие квазирасстояния по всем комнатам. Результаты расчета сведены в табл. 8.

Анализ последней колонки табл. 8 показывает, что минимальное значение вектора квазирасстояний более всего соответствует комнате №2.

Таблица 7. Нормированные значения текущих измерений от всех точек доступа

AP / № комнаты	AP_1	AP_2	AP_3	AP_4	AP_5	Z
1	0.8	2.2	–2.0	2.3	2.5	–2.0
2	–0.3	–0.2	–1.6	–0.6	0.5	–1.6
3	–3.0	2.3	0.5	0.6	–0.7	–3.0
4	–2.5	3.7	5.3	3.9	–6.0	–6.0
5	–2.6	7.0	4.7	4.6	–1.9	–2.6
6	–2.7	3.1	7.8	10.0	2.0	–2.7
7	–2.8	–0.3	0.3	2.3	1.0	–2.8
8	–1.8	–1.6	–1.4	1.6	4.4	–1.8
9	–0.6	–1.1	–2.2	6.9	4.3	–2.2

Таблица 8. Вычисленные квазирасстояния
(рейтинговые значения относительно AP и точки приёма сигнала)

№ AP / № комнаты	r_{AP_1}	r_{AP_2}	r_{AP_3}	r_{AP_4}	r_{AP_5}	R_i
1	30.8	51.6	0.0	18.1	97.9	198.4
2	8.3	6.1	0.0	0.9	18.2	33.6
3	0.0	142.7	48.3	25.8	5.5	222.2
4	24.2	381.6	635.6	297.4	0.0	1338.9
5	0.0	370.4	270.2	157.7	0.6	798.9
6	0.0	102.0	548.3	647.7	44.3	1342.3
7	0.0	6.6	40.5	79.0	73.5	199.5
8	0.0	0.0	0.3	34.5	193.2	227.9
9	9.2	1.1	0.0	246.5	209.2	466.0

Так как исходные данные во время проведения эксперимента поступили из 2-й комнаты и решающее устройство также определило 2-ю комнату, то можно считать, что комната определена верно.

Теперь, зная, в каком помещении находится мобильный абонент, а также количество и материал перегородок, разделяющих приёмную и передающую антенны, можно подобрать параметры моделей распространения радиоволн таким образом, чтобы с помощью механизма латерации определить точные координаты объекта.

Аналогичным образом была проведена оценка работы таксонометрического метода для различных помещений. Результаты экспериментов с применением таксонометрического метода при прогнозировании местоположения мобильного клиента до уровня помещения показали, что более чем в 80 % случаев помещение было определено верно, что позволило корректно применять модели распространения радиоволн, соответствующие конфигурации препятствий между мобильным объектом и точками доступа при вычислении расстояний, используемых в методе трилатерации.

Однако приблизительно 20 % помещений были определены с ошибкой, особенно в тех местах, которых может достигать радиосигнал не более чем от двух AP, что можно объяс-

нить несовершенным территориально-частотным планированием при размещении точек доступа.

5. Заключение

В ходе экспериментальных и аналитических исследований применения таксонометрического метода принятия решений было установлено, что данный метод дает положительные результаты при обоснованном радиопланировании сети Wi-Fi.

Метод предоставляет предварительную грубую оценку местоположения мобильного клиента, которая в дальнейшем будет использоваться для определения его точных координат с помощью механизма трилатерации на основе измерения уровня принимаемого сигнала RSSI.

Таким образом, имея недостаточные знания о предмете исследований, в нашем случае – это местонахождение мобильного абонента внутри помещения со сложной конфигурацией, можно воспользоваться таксонометрическим методом принятия решений, который продемонстрировал приемлемые результаты с точки зрения достоверности, адаптивности и вычислительной сложности.

Выражение благодарности

Авторы выражают благодарность аспирантам Дощинскому И. В., Брагину А. С., Плужникову А. Ф и магистранту Шурыгиной К. И. за помощь в проведении и статистической обработке измерений, а также за разработку и тестирование необходимого программного обеспечения.

Литература

1. *Krzysztofik W. J.* Radio Network Planning and Propagation Models for Urban and Indoor Wireless Communication Networks. Wroclaw, Poland: IntechOpen, 2018. P. 77–114.
2. Wi-Fi Location-Based Services 4.1 Design Guide. San Jose, CA. Americas Headquarters Cisco Systems, Inc. 2008. 206 p.
3. *Bensky A.* Wireless Positioning Technologies and Applications. 2nd Ed. Boston. London: Artech House, 2016. 450 p.
4. *Кокорева Е. В., Костюкович А. Е., Дощинский И. В.* Оценка погрешности измерений местонахождения абонента в сети Wi-Fi // Программные системы и вычислительные методы. 2019. № 4. С. 30–38.
5. *Kokoreva E. V.*, *Kostyukovich A. E.*, *Doshchinsky I. V.* Analysis of the error in determining the location inside the logistics warehouse complexes // Advances in Intelligent Systems and Computing. Springer Verlag, TransSiberia, 2020.Vol. II.106. P. 1086–1094.
6. *Mukhopadhyay A.*, *Mallissery A.* TELIL: A Trilateration and Edge Learning based Indoor Localization Technique for Emergency Scenarios // Proc. International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2018. P. 6–10.
7. *Kokoreva*, *E. V.*, *Kostyukovich*, *A. E.*, *Doshchinsky*, *I. V.*, *Shurygina*, *K. I.* A Combined Location Method with Indoor Signal Strength Measurement // Proc. IEEE 1st International Conference Problems of Informatics, Electronics, and Radio Engineering (PIERE), 2021.
8. *Kostyukovich A. E.*, *Shurygina K. I.*, *Kokoreva E. V.*, *Doshchinsky I. V.* Locating an Object Inside a Room under Line-of-Sight Conditions Between Transmitter and Receiver // Proc. IEEE 15th International Conference of Actual Problems of Electronic Instrument Engineering (APEIE), 2021. P. 290–294.
9. *Andrade C. B.*, *Hoefel R. P. F.* IEEE 802.11 WLANs: A comparison on indoor coverage models [Электронный ресурс] // Proc. Canadian Conference on Electrical and Computer Engineering, 2010. URL: `https://www.researchgate.net/publication/221279961_IEEE_`

80211_WLANs_A_comparison_on_indoor_coverage_models/download (accessed on 10.07.2022).
10. *Saunders S. R.* Antennas and propagation for wireless communication systems. England: John Wiley & Sons Ltd, 2007. 554 p.
11. *Seidel S. H.*, *Rappaport T. S.* 914 MHz Path Loss Prediction Models for Indoor Wireless Communications in Multifloored Buildings / IEEE Transactions on Antennas and Propagation. 1992. V. 40, № 2. P. 207–217.
12. *Seybold J. S.* Introduction to RF Propagation // Hoboken, New Jersey: Wiley–Interscience, 2005. 349 p.
13. *Kokoreva E.*, *Kostyukovich A.*, *Shurygina K.*, *Doshchinsky I.* Experimental Study of the Positioning System in the Centralized Wi-Fi Network // Advances in Artificial Systems for Medicine and Education. Lecture Notes on Data Engineering and Communications Technologies. Springer, 2022. V. 107. P. 346–357.
14. *Kokoreva E. V.*, *Shurygina K. I.* An Assessment of the Local Positioning System Effectiveness // Lecture Notes in Networks and Systems. Springer, 2022. V. 246. P. 436–443.
15. *Roos T.*, *Myllymäki P.*, *Tirri H.*, *Misikangas P.* A Probabilistic Approach to WLAN User Location Estimation // International Journal of Wireless Information Networks. 2002. № 9 (3). P. 155–164.
16. *Лапченко Д. А.* Теория принятия решений. Минск: БНТУ, 2021. 62 с.
17. *Решетняк Е. И.*, *Лободин Р. О.* Методы многомерного сравнительного анализа при оценке конкурентоспособности предприятия // Бізнесінформ. 2016. № 9. С. 100–105.

Статья поступила в редакцию 13.08.2022;
переработанный вариант – 31.08.2022.

Лизнева Юлия Сергеевна
к.т.н., доцент кафедры инфокоммуникационных систем и сетей СибГУТИ (630102, Новосибирск, ул. Кирова, 86), тел. (383) 2-698-241, e-mail: ktm5r@rambler.ru.

Кокорева Елена Викторовна
к.т.н., доцент кафедры цифрового телерадиовещания и систем радиосвязи СибГУТИ (630102, Новосибирск, ул. Кирова, 86), тел. (383) 2-698-362, e-mail: kokoreva@sibguti.ru.

Костюкович Анатолий Егорович
к.т.н., доцент кафедры инфокоммуникационных систем и сетей СибГУТИ (630102, Новосибирск, ул. Кирова, 86), тел. (383) 2-698-379, e-mail: aek1954@gmail.com.

Predicting the location of the mobile subscriber in the Wi-Fi network

Lizneva Julia S.
Candidate of technical sciences, Assistant professor, Siberian State University of Telecommunications and Information Science (SibSUTIS, Novosibirsk, Russia), ktm5r@rambler.ru.

Kokoreva Elena V.
Candidate of technical sciences, Assistant professor, Siberian State University of Telecommunications and Information Science (SibSUTIS, Novosibirsk, Russia), kokoreva@sibguti.ru.

Kostyukovich Anatoliy E.
Candidate of technical sciences, Assistant professor, Siberian State University of Telecommunications and Information Science (SibSUTIS, Novosibirsk, Russia), aek1954@gmail.com.

A method of trilateration based on measuring the received signal's level RSSI and calculating the distance from the subscriber's device to the visible access points is the most common locating mechanism in the Wi-Fi network. The application of this mechanism requires a complete understanding of the premises configuration, the number and material of obstacles separating the transmitting and receiving antennas which is not possible to obtain from RSSI. In this paper, the capabilities of the taxonomic decision-making method for predicting the location of mobile objects in an indoor Wi-Fi network in order to fill in the missing data on the parameters of the premises and obstacles separating access points and mobile objects are considered.

Keywords: Wi-Fi, positioning, taxonomic method, decision-making, quasi-distance.

References

1. Krzysztofik W. J. Radio Network Planning and Propagation Models for Urban and Indoor Wireless Communication Networks. *Antennas and Wave Propagation*, 2018, pp. 77–114.
2. *Wi-Fi Location-Based Services 4.1 Design Guide*. San Jose, CA, Americas Headquarters Cisco Systems, Inc., 2008, 206 p.
3. Bensky A., *Wireless Positioning Technologies and Applications*. Boston, London, Artech House, 2016, 450 p.
4. Kokoreva E. V., Kostyukovich A. E., Doshchinsky I. V. Otsenka pogreshnosti izmerenii mestonakhozhdeniya abonenta v seti Wi-Fi [Estimation of the subscriber location measurement error in Wi-Fi network]. *Programmnye sistemy i vychislitel'nye metody*, 2019, no. 4, pp. 30-38.
5. Kokoreva E. V., Kostyukovich A. E., Doshchinsky I. V. Analysis of the error in determining the location inside the logistics warehouse complexes. *Advances in Intelligent Systems and Computing*, 2020, vol. II.106, pp. 1086-1094.
6. Mukhopadhyay A., Mallissery A. TELIL: A Trilateration and Edge Learning based Indoor Localization Technique for Emergency Scenarios. *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2018, pp. 6-10.
7. Kokoreva, E. V., Kostyukovich, A. E., Doshchinsky, I. V., Shurygina, K. I. A Combined Location Method with Indoor Signal Strength Measurement. *1st International Conference Problems of Informatics, Electronics, and Radio Engineering (PIERE)*, 2021, pp. 281-286.
8. Kostyukovich A. E., Shurygina K. I., Kokoreva E. V., Doshchinsky I. V. Locating an Object Inside a Room under Line-of-Sight Conditions Between Transmitter and Receiver. *IEEE 15th International Conference of Actual Problems of Electronic Instrument Engineering (APEIE)*, 2021, pp. 290-294.
9. Andrade C. B., Hoefel R. P. F. IEEE 802.11 WLANs: A comparison on indoor coverage models, available at: `https://www.researchgate.net/publication/221279961_IEEE_80211_WLANs_A_comparison_on_indoor_coverage_models/download` (accessed 10.07.2022).
10. Saunders S. R. *Antennas and propagation for wireless communication systems*. England, John Wiley & Sons Ltd, 2007, 554 p.
11. Seidel S. H., Rappaport T. S. 914 MHz Path Loss Prediction Models for Indoor Wireless Communications in Multifloored Buildings. *IEEE Transactions on Antennas and Propagation*, vol. 40, no. 2, 1992, pp. 207-217.
12. Seybold J. S. *Introduction to RF Propagation*. Hoboken, New Jersey, Wiley-Interscience, 2005, 349 p.
13. Kokoreva E., Kostyukovich A., Shurygina K., Doshchinsky I. Experimental Study of the Positioning System in the Centralized Wi-Fi Network. *Lecture Notes on Data Engineering and Communications Technologies*, vol. 107, 2022, pp. 346–357.
14. Kokoreva E. V., Shurygina K. I. An Assessment of the Local Positioning System Effectiveness. *Lecture Notes in Networks and Systems*, 2022, vol. 246, pp. 436-443.
15. Roos T., Myllymäki P., Tirri H., Misikangas P. A Probabilistic Approach to WLAN User Location Estimation. *International Journal of Wireless Information Networks*, 2002, no. 9(3), pp. 155-164.
16. Lapchenko D. A. *Teoriya prinyatiya reshenii* [Decision theory]. Minsk, Belorusskii natsional'nyi tekhnicheskii universitet, 2021, 62 p.
17. Reshetnyak O. I., Lobodin R. O. The Methods of Multidimensional Comparative Analysis in Evaluating Competitiveness of Enterprise. *Business Inform*, 2016, no. 9, pp. 100-105.