ISSN 2686-679X

ВЕСТНИК РГГУ

Серия
«Информатика.
Информационная безопасность.
Математика»

Научный журнал

RSUH/RGGU BULLETIN

"Information Science.
Information Security. Mathematics"
Series

Academic Journal

Основан в 2018 г.
Founded in 2018

1
2024

VESTNIK RGGU. Seriya “Informatica. Informacionnaya bezopasnost. Matematica”

RSUH/RGGU BULLETIN. “Information Science. Information Security. Mathematics” Series
Academic Journal

There are 4 issues of the printed version of the journal a year.

Founder and Publisher
Russian State University for the Humanities (RSUH)

RSUH/RGGU BULLETIN. “Information Science. Information Security. Mathematics” series is included: in the Russian Science Citation Index; in the List of leading scientific magazines journals and other editions for publishing PhD research findings peer-reviewed publications fall within the following research area:

1.1.6. Computational Mathematics (physical and mathematical sciences)

2.3.6. Information security methods and systems, information security (technical science)

2.3.8. Informatics and information processes (technical science)

Objectives and areas of research

RSUH/RGGU BULLETIN. “Information Science. Information Security. Mathematics” series publishes the results of research by scientists from RSUH and other universities and other Russian and foreign academic institutions. The areas covered by contributions include theoretical and applied computer science, up-to-date IT, means and technologies of information protection and information security as well as the issues of theoretical and applied mathematics including analytical and imitation models of different processes and objects. Special emphasis is put on articles and reviews covering research in indicated directions in the areas of social and humanitarian problems and also issues of personnel training for these directions.

RSUH/RGGU BULLETIN. “Information Science. Information Security. Mathematics” series is registered by Federal Service for Supervision of Communications Information Technology and Mass Media. 25.05.2018, reg. No. FS77-72977

Editorial staff office: 6, Miusskaya sq., Moscow, Russia, 125047
e-mail: grnat@rambler.ru

ВЕСТНИК РГГУ. Серия «Информатика. Информационная безопасность. Математика»
Научный журнал

Выходит 4 номера печатной версии журнала в год.

Учредитель и издатель – Российский государственный гуманитарный университет (РГГУ)

ВЕСТНИК РГГУ, серия «Информатика. Информационная безопасность. Математика», включен: в систему Российского индекса научного цитирования (РИНЦ); в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук по следующим научным специальностям и соответствующим им отраслям науки:

1.1.6. Вычислительная математика (физико-математические науки)

2.3.6. Методы и системы защиты информации, информационная безопасность (технические науки)

2.3.8. Информатика и информационные процессы (технические науки)

Цели и область

В журнале «Вестник РГГУ», серия «Информатика. Информационная безопасность. Математика», публикуются результаты научных исследований ученых и специалистов РГГУ, а также других университетов и научных учреждений России и зарубежных стран. Направления публикаций включают теоретическую и прикладную информатику, современные информационные технологии, методы, средства и технологии защиты информации и обеспечения информационной безопасности, а также проблемы теоретической и прикладной математики, включая разработку аналитических и имитационных моделей процессов и объектов различной природы. Особое внимание уделяется статьям и обзорам, посвященным исследованиям по указанным направлениям в области социальных и гуманитарных проблем, а также вопросам подготовки кадров по соответствующим специальностям для данных направлений.

ВЕСТНИК РГГУ. Серия «Информатика. Информационная безопасность. Математика», зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций 25.05.2018 г., регистрационный номер ПИ № ФС77-72977.

Адрес редакции: 125047, Россия, Москва, Миусская пл., 6

Электронный адрес: grnat@rambler.ru

Учредитель и издатель
Российский государственный гуманитарный университет (РГГУ)

Ответственный за выпуск:

Н.В. Гришина, кандидат технических наук, доцент,
Российский государственный гуманитарный университет (РГГУ)

CONTENTS

СОДЕРЖАНИЕ

УДК 004
DOI: 10.28995/2686-679X-2024-1-8-20

К вопросу разработки графических интерфейсов для управления БЛА

Александра С. Доброквашина
Казанский (Приволжский) федеральный университет, Казань, Россия, dobrokvashina@it.kfu.ru

Аннотация. В настоящее время сфера беспилотных летательных аппаратов быстро растет и развивается. Беспилотные системы активно интегрируются в повседневную жизнь. Однако с ростом количества БЛА значительно расширился объем программного обеспечения, появилось множество графических интерфейсов для управления. Сегодня известны различные решения для управления летательными аппаратами: как с помощью мобильных телефонов и устройств, так и с помощью персональных компьютеров и систем управления. Управление может осуществляться как для одного БЛА, так и для их групп и роев, а в некоторых случаях и для гетерогенных групп роботов, где БЛА могут применяться в связках с наземными, наводными или подводными роботами. В последнем случае комплексность графического интерфейса может вырастать в разы. На сегодняшний день нет четких способов классификации и упорядочивания графических интерфейсов для управления БЛА и их группами. В данной работе проводится аналитический обзор существующих графических интерфейсов, а ее целью является создание четкой классификации для возможности их распределения. Это позволит в дальнейшем предложить прототип универсального графического интерфейса для управления беспилотными летательными аппаратами и их группами, а также разработать методики для создания и тестирования ряда интерфейсов.

Ключевые слова: БЛА, графический интерфейс, БАС, обзор

Для цитирования: Доброквашина А.С. К вопросу разработки графических интерфейсов для управления БЛА // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 1. С. 8–20. DOI: 10.28995/2686-679X-2024-1-8-20

Development and testing of the graphical user interfaces for UAV

Aleksandra S. Dobrokvashina
Kazan Federal University, Kazan, Russia,
dobrokvashina@it.kfu.ru

Abstract. Currently, the field of unmanned aerial vehicles is growing and developing rapidly. Unmanned systems are being actively integrated into everyday life. However, with the increase in the number of UAVs, the volume of software has expanded significantly, and many graphical interfaces for control have appeared. Today, various solutions are known for controlling aircraft: both using mobile phones and devices, and using personal computers and control systems. Control can be carried out both for one UAV and for their groups and swarms, and in some cases for heterogeneous groups of robots, where UAVs can be used in conjunction with ground, surface or underwater robots. In the latter case, the complexity of the graphical interface can increase significantly. To date, there are no clear ways to classify and organize graphical interfaces for controlling UAVs and their groups. This work provides an analytical review of existing graphical interfaces, and its goal is to create a clear classification to enable their distribution. That will make it possible in the future to propose a prototype of a universal graphical interface for controlling unmanned aerial vehicles and their groups, as well as to develop methods for creating and testing a number of interfaces.

Keywords: UAV, graphical user interface, RPAS, review

For citations: Dobrokvashina, A.S. (2024), "Development and testing of the graphical user interfaces for UAV", *RSUH/RGGU Bulletin. "RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 1, pp. 8–20, DOI: 10.28995/2686-679X-2024-1-8-20

Введение

Беспилотные авиационные системы (БАС) активно набирают популярность [Новик, Кудряшов 2023] и все чаще применяются как в сельском хозяйстве [Айдаров, Горшенина, Боженко 2023], так и в спасательных операциях [Мостаков, Голобурдин, Анисимов, Бакаев, Кулагин 2022]. Растущий интерес к беспилотным летательным аппаратам (БЛА) влечет за собой увеличение не только количества производителей и разновидностей беспилотников, но и множащееся программное обеспечение (ПО) для них. Срели распространенного ПО: алгоритмы, создаваемые для автоматизации

процессов различного уровня сложности, а также системы управления [Чмелев, Калюка, Дмитренко 2022]. Графические интерфейсы являются одним из распространенных способов управления не только в сфере БАС [Dubelschikov, Tsoy, Bai, Svinin, Magid 2022], но и в робототехнической отрасли в целом [Магид, Лавренов, Маврин 2019; Mustafin, Chebotareva, Li, Magid 2023]. Они активно применяются для управления как отдельными дронами [Slingsby, Scott, Kregting, McIlvenny 2023], так и их группами [Terzi, Anastasiou, Kolios 2019]. В некоторых случаях система управления и графический интерфейс имеют соединение не только с одним и несколькими дронами, но и с роботами других типов [Shirakura, Kiyokawa, Takamatsu, Ogasawara 2021]. В таком случае можно говорить о комплексных системах управления для гетерогенных групп роботов. Стоит отметить, что несмотря на активно растущее количество графических интерфейсов, на сегодня не выявлено ни одного способа их классификации.

Данная работа содержит аналитический обзор существующих решений в вопросе управления БЛА с помощью графических интерфейсов. Также предлагается система классификации для самих графических интерфейсов. За основание для представленной классификации были использованы существующие классификации беспилотных летательных аппаратов и систем для их управления. В итоге классификация графических интерфейсов производится по нескольким типам, таким как уровень автономности систем, тип и количество управляемых аппаратов и т. д.

Благодаря полученным результатам возможна дальнейшая разработка унифицированного графического интерфейса для управления БЛА и их группами, а также создание и написание методик тестирования различных графических интерфейсов для управления.

Классификация интерфейсов

Классификация, предложенная для графических интерфейсов, базируется на классификации самих БЛА [Кузнецов, Горбоконенко 2023]. Тип и направленность работы БЛА, а также поставленная задача влияют на данные, необходимые оператору в процессе отслеживания или управления БЛА. По этой причине сложно использовать одну стандартную классификацию для всех интерфейсов. В этой работе предлагается определять тип графического интерфейса, базируясь на нескольких представленных ниже классификациях:

- тип БЛА;
- автономность;
- количество;
- управление;
- направленность.

Диаграмма классификаций графических интерфейсов представлена на рис. 1.

Рис.1. Диаграмма классификаций для графических интерфейсов

Классификация по типу БЛА

Для графических интерфейсов низкоуровневого управления (например управление отдельными моторами) стоит учитывать не только сторонние факторы, такие как задачи и цели вылета, но и конструкцию самого БЛА. Тип БЛА – первая классификация, которая будет рассмотрена. Классификация идет по двум основным группам:

– самолетные;
– винтокрылые.

Винтокрылые, в свою очередь, подразделяются на вертолетные – с одним винтом, и на мультироторные – в том числе квадро- и мультикоптеры [Хрунь, Хакимов 2021]. Различие в типах винтокрылых дронов заключается в количестве моторов и винтов, от чего напрямую зависит мощность и грузоподъемность аппарата. Различия конструкций самолетных и винтокрылых БЛА приводят к появлению специфических особенностей. Например, возможность удерживаться в одном положении в воздухе, необходимость взлетно-посадочной полосы, а также время автономной работы

и качества соединения между аппаратом и оператором. Все эти элементы влияют и на графический интерфейс, отражаясь на функционале и на алгоритме взаимодействия.

Классификация по уровню автономности

Следующая классификация зависит от степени автоматизации процессов и выполнения поставленных задач [Новик, Кудряшов 2023]. Чаще всего выделяют три уровня автономности систем:

– неавтономные;
– автономные;
– комбинированные.

При работе с неавтономными системами оператор управляет БЛА с помощью ручного управления. Примером неавтономной системы управления являются FPV-дроны, используемые в том числе в гонках [Пругер, Хмелик 2019]. Такой подход требует постоянного контроля со стороны оператора, интерфейсы стараются сохранять информативность при минимальной загруженности экрана. В полностью автономных системах оператор играет роль наблюдателя. Зачастую при работе с такими системами активное взаимодействие с интерфейсом происходит только при запуске системы. На этом этапе возможны проверка систем и корректировки параметров. После запуска оператор переходит в роль наблюдателя. На этом этапе возможно отслеживать процесс выполнения задачи, в некоторых случаях остановить его или скорректировать. Интерфейс при этом может иметь достаточно большое количество окон, содержащих информацию о ходе выполнения алгоритма, и небольшое количество интерактивных элементов, позволяющих взаимодействовать с БЛА. Последним пунктом в этой классификации выступают комбинированные системы управления, которые на сегодняшний день встречаются как среди любительских, так и среди профессиональных беспилотных систем. Как и в случае с неавтономными, оператор принимает активную роль в управлении БЛА, однако в таких системах подразумевается наличие частично автоматизированных процессов (например, автоматические взлет и посадка, следование за целью и т. д.). Интерфейс в таком случае может содержать большее количество различных окон и интерактивных элементов, позволяющих не только вручную управлять БЛА, но и контролировать работу автоматических алгоритмов.

Классификация по количеству

Следующая классификация связана с количеством и типами управляемых аппаратов:

– один БЛА;
– групповое взаимодействие:
  • гомогенные;
  • гетерогенные.

Классический случай – управление одним БЛА. Особенности можно найти в графических интерфейсах для управления группами роботов. Группы могут состоять из однотипных роботов (например, только БЛА) или различных (связки БЛА-БНА (беспилотные наземные аппараты), БЛА-БПА (беспилотные подводные аппараты) и т. д.). Если группа гомогенная, то на систему и графический интерфейс в том числе может влиять формат взаимодействия внутри. Это может быть рой, где в группе все дроны автономны, но выполняют одну задачу, либо группа с ведущим, где оператор управляет только ведущим, а остальная группа двигается вслед за ведущим.

Классификация по способу управления

Важным фактором при разработке графического интерфейса является устройство, на котором он будет запущен. В случае БЛА варианты управляющего устройства следующие:

– VR (FPV – First Person View);
– мобильное устройство;
– программное обеспечение для ПК;
– специализированные комплексы и системы управления.

Формат управления FPV набирает популярность среди операторов. При таком формате управления чаще всего используются VR-шлемы. Интерфейсы в них избегают интерактивных элементов, а экраны предоставляют максимум полезной информации с минимальной загрузкой экрана. Мобильные устройства, такие как дистанционные пульты, планшеты или смартфоны, в отличие от VR, дают больше свободы в отношении интерактивности. В них представлены различные выпадающие списки и дополнительные окна настроек, так как экраны этих устройств не могут вместить достаточно необходимой информации (например, приложение DJI GO). Следующим этапом идет программное обеспечение для ПК. При разработке ПО для персональных компьютеров пропадают

ограничения по производительности и количеству активных окон, что позволяет создавать комплексные архитектуры и решения. Специализированные комплексы и системы управления достаточно дорогостоящие проекты, поэтому чаще всего они находят свое применение в различных отраслевых решениях.

Классификация по направлению деятельности

Последняя классификация, которая будет рассмотрена в этой работе, базируется на сфере применения управляемого дрона, а именно:

– классическое управление;
– специализированные.

Классическое управление подразумевает собой стандартный подход к контролю БЛА. В качестве примера можно взять любой графический интерфейс, который идет в комплекте с дроном. В большинстве случаев это минимальный набор данных: картинка с камер, данные о заряде батареи, скорости и ориентации. Специализированные интерфейсы обычно идут в паре с доработанными дронами, оборудованными дополнительными сенсорами или креплениями, а интерфейс позволяет в большей мере взаимодействовать с имеющимися надстройками.

Примеры графических интерфейсов

При обзоре было рассмотрено множество различных систем управления как для одиночных БЛА [Peng, Turkmen, Eickhoff, Finta 2019; Slingsby, Scott, Kregting, McIlvenny 2023], так и для групп [Shirakura, Kiyokawa, Takamatsu, Ogasawara 2021; Terzi, Anastasiou, Kolios 2019]. Далее будут рассмотрены и классифицированы несколько графических интерфейсов для управления БЛА. На рис. 2 можно увидеть несколько вариаций графического интерфейса, используемого для управления FPV дроном [Kocer, Stedman, Kulik, Caves, Van Zalk, Pawar, Kovac 2022]. В интерфейсе отсутствуют интерактивные элементы, однако четко освещены основные аспекты состояния аппарата, а именно: информация о заряде батареи, скорости, местоположении и ориентации в пространстве. Графический интерфейс такого плана можно классифицировать как классический неавтономный VR интерфейс для управления одним БЛА мультироторного типа.

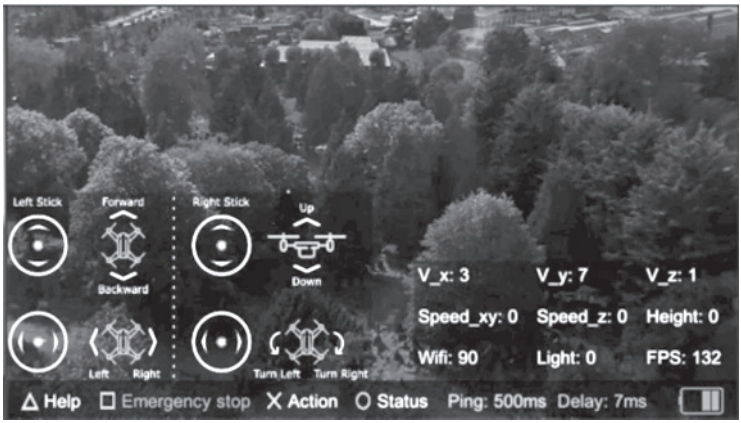


Рис. 2. Пример графического интерфейса FPV дрона [Kocer, Stedman, Kulik, Caves, Van Zalk, Pawar, Kovac 2022]

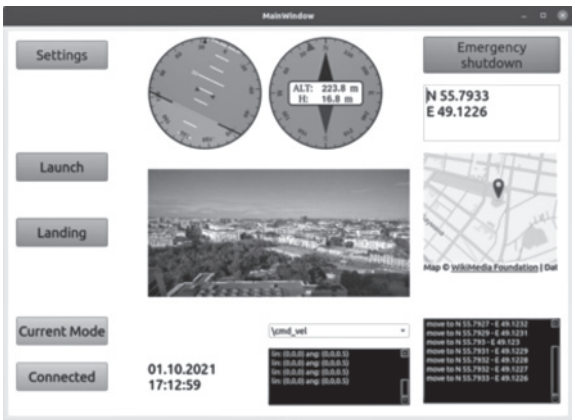


Рис. 3. Графический интерфейс системы управления для ПК [Lavrenov, Safin, Bai, Martinez-Gazrcia, Meshcheryakov 2022]

Рисунок 3 представляет собой пример универсального графического интерфейса для управления БЛА с использованием робототехнической операционной системы (ROS) [Lavrenov, Safin, Bai, Martinez-Gazrcia, Meshcheryakov 2022]. Интерфейс содержит стандартный набор элементов контроля полета: информация о

местоположении и ориентации дрона в пространстве, экран с видеопотоком, получаемым с камеры, и возможность запуска алгоритмов автономного полета и посадки. Присутствует также всплывающее окно настроек для оптимизации работы с БЛА. Данный интерфейс можно классифицировать как классический комбинированный интерфейс для ПК для управления одним БЛА мультироторного типа.

На рисунке 4 изображена система управления для модульного БЛА MQ-9 Reaper самолетного типа [Замятин 2020]. В отличие от предыдущих примеров данная СУ представлена крупным комплексом. Помимо стандартного набора элементов интерфейса, отображающих видео с камер и данные о местоположении и ориентации, здесь представлена расширенная информация о состоянии самого аппарата, а также имеется возможность более тонкой настройки систем БЛА и его алгоритмов. Классифицируя данный интерфейс, можно охарактеризовать его как специализированный профильный интерфейс системы управления для управления одним БЛА самолетного типа.

Рис. 4. Система управления MQ-9 Reaper [Замятин 2020]

Рассмотренные графические интерфейсы имеют несколько схожих черт, которые можно выделить как одни из часто встречаемых: данные с бортовой камеры, информация о заряде батареи, а также данные об ориентации дрона в пространстве (крен, тангаж и рыскание). Все эти элементы могут стать базовыми при дальнейшей разработке унифицированного графического интерфейса для БЛА.

Заключение

Активное развитие беспилотных авиационных систем (БАС) приводит к увеличению количества и разнообразия ПО для дронов. Среди прочего растет количество графических интерфейсов и систем управления как для одиночных и роев БЛА, так и гетерогенных групп роботов. Однако даже при таком активном росте отсутствует четкая система классификации для этих графических интерфейсов. В данной работе, базируясь на имеющихся классификациях БЛА и их направленности, был предложен новый способ классификации. Также были рассмотрены и классифицированы несколько примеров таких интерфейсов. Благодаря этому появилась возможность выделить общие элементы управления, что в дальнейшем позволит создать унифицированный графический интерфейс для управления БЛА и их группами. Полученные результаты могут стать основанием для создания методик тестирования графических интерфейсов для управления БЛА и их группами.

Литература

Айдаров, Горшенина, Боженко 2023 – *Айдаров А.В., Горшенина Е.Ю., Боженко В.О.* Разработка обучающего тренажера для работы с агроориентированными беспилотными летательными аппаратами // Проблемы и перспективы развития АПК: технические и сельскохозяйственные науки: Материалы Региональной научно-технической конференции, посвященной 110-летию Вавиловского университета. Саратов, 2023. С. 144–150.

Замятин 2020 – *Замятин П.А.* Системы управления беспилотными летательными аппаратами // Инновационная наука. 2020. № 4. С. 37–42.

Кузнецов, Горбоконенко 2023 – *Кузнецов Д.Ю., Горбоконенко В.Д.* Классификация беспилотных летательных аппаратов по летным характеристикам // Вузовская наука в современных условиях: Сборник материалов 57-й научно-технической конференции. Ульяновск: Ульяновский государственный технический университет, 2023. С. 87–89.

Магид, Лавренов, Маврин 2019 – *Магид Е.А., Лавренов Р.О., Маврин И.А.* Программное обеспечение с графическим интерфейсом для управления гусеничным роботом Сервосила Инженер. Свидетельство о государственной регистрации программы для ЭВМ. Номер свидетельства: RU 2019615855, 2019.

Мостаков, Голобурдин, Анисимов, Бакаев, Кулагин 2022 – *Мостаков Н.А., Голобурдин Н.В., Анисимов Р.О., Бакаев В.С., Кулагин К.А.* Система спасения утопающих с помощью беспилотного летательного аппарата // Конференция по компьютерной графике и зрению «Графикон». 2022. Т. 32. С. 1115–1122.

Новик, Кудряшов 2023 – *Новик А.В., Кудряшов А.С.* Беспилотные летательные аппараты, перспективы развития, классификация и способы борьбы с ними // Научные чтения имени профессора Н.Е. Жуковского: Сборник научных статей XIII Международной научно-практической конференции. Краснодар, 2023. С. 420–425.

Пругер, Хмелик 2019 – *Пругер И.Н., Хмелик О.Г.* Исследование применения квадрокоптеров для игровой индустрии // Электронные средства и системы управления. Материалы докладов XV Международной научно-практической конференции. Томск: Томский государственный университет систем управления и радиоэлектроники, 2019. С. 117–119.

Хрунь, Хакимов 2021 – *Хрунь В.Н., Хакимов Н.Т.* Обзор существующих типов беспилотных летательных аппаратов // Научные исследования: проблемы и перспективы: Сборник научных трудов по материалам XXXV Международной научно-практической конференции. Анапа, 2021. С. 147–151.

Чмелев, Калюка, Дмитренко 2022 – *Чмелев В.С., Калюка В.И., Дмитренко М.Е.* Обзор систем управления беспилотных летательных аппаратов общего пользования // Технологии. Инновации. Связь: Сборник материалов научно-практической конференции. СПб.: Военная академия связи, 2022. С. 279–286.

Dubelschikov, Tsoy, Bai, Svinin, Magid 2022 – *Dubelschikov A., Tsoy T., Bai Y., Svinin M., Magid E.* Intelligent System Concept of an IoT Cameras Network Application for an Unmanned Aerial Vehicle Control via a Graphical User Interface // 2022 International Conference on Information, Control, and Communication Technologies (ICCT). New York, NY: IEEE, 2022. P. 1–4.

Kocer, Stedman, Kulik, Caves, Van Zalk, Pawar, Kovac 2022 – *Kocer B.B., Stedman H., Kulik P., Caves I., Van Zalk N., Pawar V.M., Kovac M.* Immersive View and Interface Design for Teleoperated Aerial Manipulation // 2022 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS). New York, NY: IEEE, 2022. P. 4919–4926.

Mustafin, Chebotareva, Li, Magid 2023 – *Mustafin M., Chebotareva E., Li H., Magid E.* Experimental Validation of an Interface for a Human-Robot Interaction Within a Collaborative Task // International Conference on Interactive Collaborative Robotics. Cham: Springer, 2023. P. 23–35.

Lavrenov, Safin, Bai, Martinez-Gazrcia, Meshcheryakov 2022 – *Lavrenov R., Safin R., Bai Y., Martínez-García E.A., Meshcheryakov R.* Graphical User Interface Design for a UAV Teleoperation // Proceedings of International Conference on Artificial Life and Robotics. Kazan, 2022. P. 678–681.

Peng, Turkmen, Eickhoff, Finta 2019 – *Peng A.S., Turkmen A., Eickhoff B., Finta M., Gerads P.* Design of a Ground Sampling Distance Graphical User Interface for an Unmanned Aerial Vehicle System // 53rd Annual Conference on Information Sciences and Systems (CISS). New York, NY: IEEE, 2019. P. 1–6.

Shirakura, Kiyokawa, Takamatsu, Ogasawara 2021 – *Shirakura N., Kiyokawa T., Kumamoto H., Takamatsu J., Ogasawara T.* Collection of marine debris by jointly using uav-uuv with gui for simple operation // IEEE Access. 2021. Vol. 9. P. 67432–67443.

Slingsby, Scott, Kregting, McIlvenny 2023 – *Slingsby J., Scott B.E, Kregting L, McIlvenny J., Wilson J., Yanez M., Williamson B.J.* The bigger picture: developing a low-cost graphical user interface to process drone imagery of tidal stream environments // International Marine Energy Journal. 2023. Vol. 6 (1). P. 11–17.

Terzi, Anastasiou, Kolios 2019 – *Terzi M., Anastasiou A., Kolios P., Panayiotou C., Theocharides T.* SWIFTERS: A multi-UAV platform for disaster management // 2019 International conference on information and communication technologies for disaster management (ICT-DM). New York, NY: IEEE, 2019. P. 1–7.

References

Aidarov, A.V., Gorshenina, E.Yu. and Bozhenko, V.O. (2023), "Development of a training simulator for working with agro-oriented unmanned aerial vehicles", *Issues and Prospects of agro-industrial complex development. Technical and Agricultural Sciences. Proceedings of the Regional Scientific and Technical Conference Commemorating the 110th Anniversary of Vavilov University*, Saratov, Russia, pp. 144–150.

Chmelev, V.S., Kalyuka, V.I. and Dmitrenko, M.E. (2022), "Overview of the control systems of public unmanned aerial vehicles", *Technologies. Innovation. Communication. Proceedings of the Scientific and Practical. Conf.*, Military Telecommunication Academy, Saint Petersburg, Russia, pp. 279–286.

Dubelschikov, A., Tsoy, T., Bai, Y., Svinin, M. and Magid, E. (2022), "Intelligent system concept of an IoT cameras network application for an unmanned aerial vehicle control via a graphical user interface", *2022 International Conference on Information, Control, and Communication Technologies (ICCT)*, IEEE, New York, NY, USA, pp. 1–4.

Khrun', V.N. and Khakimov, N.T. (2021), "Overview of existing types of unmanned aerial vehicles", *Scientific Research. Issues and Prospects. Collection of scientific papers on the proceedings of the XXXV International Scientific and Practical Conference*, Anapa, Russia, pp. 147–151.

Kocer, B.B., Stedman, H., Kulik, P., Caves, I., Van Zalk, N., Pawar, V.M. and Kovac, M. (2022), "Immersive view and interface design for teleoperated aerial manipulation", *2022 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, IEEE, New York, NY, USA, pp. 4919–4926.

Kuznetsov, D.Y. and Gorbokonenko, V.D. (2023), "Classification of unmanned aerial vehicles by flight characteristics", *University Science in Current Environment. Sat. Art. by the Proceedings of the 57th Scientific and Practical. Conf.*, Ul'yanovsk State Technical University, Ul'yanovsk, Russia, pp. 87–89.

Lavrenov, R., Safin, R., Bai, Y., Martínez-García, E.A. and Meshcheryakov, R. (2022), "Graphical user interface design for a UAV teleoperation", *Proceedings of International Conference on Artificial Life and Robotics*, Kazan, Russia, pp. 678–681.

Magid, E.A., Lavrenov, R.O. and Mavrin, I.A. (2019), Software with graphical interface for controlling crawler robot Servosila Engineer. Certificate of the state registration of the computer program. Certificate number: RU 2019615855.

Mostakov, N.A., Goloburdin, N.V., Anisimov, R.O., Bakaev, V.S. and Kulagin, K.A. (2022), "A drowning rescue system using an unmanned aerial vehicle", *Graphicon – Conferences on Computer Graphics and Vision*, vol. 32, pp. 1115–1122.

Mustafin, M., Chebotareva, E., Li, H. and Magid, E. (2023), "Experimental validation of an interface for a human-robot interaction within a collaborative task", *International Conference on Interactive Collaborative Robotics*, Springer, Cham, Switzerland, pp. 23–35.

Novik, A.V. and Kudryashov, A.S. (2023), "Unmanned aerial vehicles, development prospects and ways to combat them", *Scientific Conference in honor of Professor N.E. Zhukovsky. Sat. Art. by the Proceedings of the 13th Scientific and Practical. Conf.*, Krasnodar, Russia, pp. 420–425.

Peng, A.S., Turkmen, A., Eickhoff, B., Finta, M. and Gerads, P. (2019), "Design of a ground sampling distance graphical user interface for an unmanned aerial vehicle system", *53rd Annual Conference on Information Sciences and Systems (CISS)*, IEEE, New York, NY, USA, pp. 1–6.

Pruger, I.N. and Khmelik, O.G. (2019), "Research on the use of quadrocopters for the gaming industry", *Electronic Means and Control Systems. Proceedings of XV International Scientific and Practical Conference*, Tomsk State University of Control Systems and Radioelectronics, Tomsk, Russia, pp. 117–119.

Shirakura, N., Kiyokawa, T., Kumamoto, H., Takamatsu, J. and Ogasawara, T. (2021), "Collection of marine debris by jointly using uav-uuv with GUI for simple operation", *IEEE Access*, vol. 9, pp. 67432–67443.

Slingsby, J., Scott, B.E., Kregting, L., McIlvenny, J., Wilson, J., Yanez, M. and Williamson, B.J. (2023), "The bigger picture: developing a low-cost graphical user interface to process drone imagery of tidal stream environments", *International Marine Energy Journal*, vol. 6 (1), pp. 11–17.

Terzi, M., Anastasiou, A., Kolios, P., Panayiotou, C. and Theocharides, T. (2019), "SWIFTERS: A multi-UAV platform for disaster management", *2019 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)*, IEEE, New York, NY, USA, pp. 1–7.

Zamyatin, P.A. (2020), "Control systems for unmanned aerial vehicles", *Innovative Science*, vol. 4, pp. 37–42.

Информация об авторе

Александра С. Доброквашина, аспирант, Казанский (Приволжский) федеральный университет, Казань, Россия; 420008, Россия, Казань, Кремлевская ул., д. 35; dobrokvashina@it.kfu.ru

Information about the author

Aleksandra S. Dobrokvashina, postgraduate student, Kazan Federal University, Kazan, Russia; 35, Kremlevskaya Str., Kazan, 420008, Russia; dobrokvashina@it.kfu.ru

УДК 519+004.42
DOI: 10.28995/2686-679X-2024-1-21-35

Анализ моделей адаптивных нейро-нечетких систем

Андрей П. Титов
Российский технологический университет МИРЭА, Москва, Россия, titov_and@mail.ru

Аннотация. Статья посвящена исследованию основных методов для моделей адаптивных нейро-нечетких систем. На основе проведенного анализа найдены сильные стороны нейронных сетей и нечеткой логики, которые стали мощными инструментами для решения сложных задач моделирования и прогнозирования. Изучена и проанализирована адаптивная нейронная сеть, представляющая собой класс нейронных сетей, которые обладают способностью изменять свою структуру и параметры в процессе обучения и адаптации к новым данным и условиям. Изучена Гауссовская функция принадлежности, также известная как нормальная функция принадлежности или функция принадлежности типа Гаусса, которая представляет собой ценный инструмент в области нечеткой логики и нечетких систем. Проанализирована обобщенная функция принадлежности Белл, также известная как функция принадлежности типа Белл или функция Белла, которая играет важную роль в области нечеткой логики и нечетких систем. Проанализирована модель Цукамото, которая является одной из основных моделей нечеткой логики. Выбрана модель Co-Active Neuro-Fuzzy Inference System, которая представляет собой адаптивную нейро-нечеткую систему, которая сочетает в себе нейронные сети и нечеткую логику для обработки данных с неопределенностью и нечеткостью. При дальнейшей реализации комбинированной модели на основе выше перечисленных моделей на основе STL языка C++ получим модель нейронной сети, обладающую универсальностью, которая достигается за счет использования комбинации этих моделей. Это позволит легко модифицировать и адаптировать ее под различные задачи.

Ключевые слова: нейронные сети, адаптивная нейронная сеть, Гауссовская функция принадлежности, модель Цукамото, обобщенная функция принадлежности Белл

Для цитирования: Титов А.П. Анализ моделей адаптивных нейро-нечетких систем // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 1. С. 21–35. DOI: 10.28995/2686-679X-2024-1-21-35

Analysis of models of adaptive neuro-fuzzy systems

Andrei P. Titov
Russian Technological University MIREA, Moscow, Russia, titov_and@mail.ru

Abstract. The article deals with the study of basic methods for models of adaptive neuro-fuzzy systems. Based on the analysis, the strengths of neural networks and fuzzy logic were found, that became powerful tools for solving complex modeling and forecasting issues. There is studying and analyzing the adaptive neural network, which is a class of neural networks that have the ability to change their structure and parameters in the process of learning and adaptation to new data and conditions and besides the article studies the Gaussian membership function, also known as the normal membership function or the Gauss-type membership function, which is a valuable tool in the field of fuzzy logic and fuzzy systems.

The paper provides as well an analysis of the generalized Bell membership function, also known as the Bell type membership function or Bell function, which plays an important role in the field of fuzzy logic and fuzzy systems. Furthermore it analyzes the Tsukamoto model, which is one of the main models of fuzzy logic. The author opted to choose the Co-Active Neuro-Fuzzy Inference System model, which is an adaptive neuro-fuzzy system that combines neural networks and fuzzy logic for processing data with uncertainty and fuzziness. With the further implementation of the combined model based on the above-listed models based on the STL of the C++ language, thus the neural network model is obtained, the model with versatility, that is achieved by using a combination of those models. That will facilitate its easy modification and adaptation to various tasks.

Keywords: neural networks, adaptive neural network, Gaussian membership function, Tsukamoto model, generalized Bell membership function

For citation: Titov, A.P. (2024), "Analysis of models of adaptive neuro-fuzzy Systems", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series,* no. 1, pp. 21–35, DOI: 10.28995/2686-679X-2024-1-21-35

Введение

Быстро развивающийся мир информационных технологий включает в себя множество задач, требующих эффективной обработки и анализа данных. В этом контексте нейро-нечеткие системы,

сочетающие в себе сильные стороны нейронных сетей и нечеткой логики, стали мощными инструментами для решения сложных задач моделирования и прогнозирования.

Нечеткая логика (англ. fuzzy logic), основы которой заложил Л. Заде в 60-х годах прошлого столетия, за несколько десятилетий превратилась в мощный инструмент для построения моделей приближенных рассуждений человека в задачах принятия решений в условиях неопределенности, классификации и анализа данных. Математический аппарат теории нечетких множеств позволяет построить модель объекта, основываясь на нечетких рассуждениях и правилах [Андрейчиков, Андрейчикова 2000].

Нечеткие модели описывают явления и процессы реального мира на естественном языке при помощи лингвистических переменных, а механизм нечеткого вывода прозрачен и понятен человеку. Эти преимущества обусловили широкое применение нечеткой логики для решения задач автоматического управления, принятия решений, прогнозирования в различных прикладных областях науки, техники и экономики [Алтунин, Семухин 2000].

Выделяют три периода в развитии нечеткой логики и нечетких систем.

Первый период (конец 60-х начало 70-х гг.) характеризуется развитием теоретического аппарата нечетких множеств (Л. Заде, Е. Мамдани, Беллман) [Борисов, Крумберг, Федоров 1990].

Во втором периоде (70–80-е годы) появляются первые практические результаты в области нечеткого управления техническими системами (поршневой двигатель). Одновременно ученые коллективы стали уделять внимание вопросам построения экспертных систем, основанных на нечеткой логике, разработке нечетких контроллеров [Борисов, Алексеев, Крумберг 1982].

В третьем периоде, который длится с конца 80-х годов и продолжается в настоящее время, появляются пакеты программ для построения нечетких экспертных систем, а области применения нечеткой логики заметно расширяются. Она применяется в автомобильной, аэрокосмической и транспортной промышленности, в области изделий бытовой техники, в сфере финансов, анализа и принятия управленческих решений и многих других [Кравченко 2002].

Нечеткие нейронные сети

Нечеткие нейронные сети (ННС) представляют собой методологию, основанную на использовании нейронных сетей для решения разных задач с помощью нечеткого логического вывода.

В отличие от традиционных двоичных нейронных сетей, ННС работают с нечеткими значениями вместо жестких бинарных состояний, что позволяет учитывать неопределенность и нечеткость входных данных. Они находят применение в моделировании нечеткого мышления и логического вывода, что позволяет эффективно решать задачи классификации, прогнозирования, управления и принятия решений, связанные с нечеткими и неопределенными данными. Нечеткие нейронные сети демонстрируют способность наиболее эффективно обрабатывать размытые концепты, что делает их ценным инструментом в области искусственного интеллекта и машинного обучения [Поспелов 1986].

Положительные стороны нечетких нейронных сетей	Недостатки нечетких нейронных сетей
1. Обработка размытых данных. Данные с нечеткостью и неопределенностью обрабатываются нечеткими нейронными сетями наиболее эффективно. Это и делает их весьма важными инструментами при анализе сложных систем, где важны точные значения, которые могут быть недоступными или неясными.	1. Вычислительная сложность. При работе с большими объемами данных нечеткие нейронные сети могут быть более восприимчивы к вычислительной мощности и медленнее за счет дополнительных вычислений и операций. Обработка таких данных нуждается в дополнительных вычислительных мощностях по сравнению с обычными методами обработки информации.
2. Учет неопределенности. Если информация содержит некоторые степени неопределенности, то с ней способны работать только нечеткие нейронные сети, что делает их адаптивными и гибкими при работе с данными, содержащими шумы, неточности и неоднозначности.	2. Зависимость от экспертных знаний. К ошибочным результатам и понижению эффективности модели может привести ошибочное определение нечетких функций принадлежности или правил. Именно поэтому при создании эффективных нечетких нейронных сетей требуется глубинное понимание и знание предметной области, а также должны быть привлечены экспертные знания.
3. Интуитивный подход. Интерпретация данных и принятие решений будет более понятными и интуитивными при использовании нечетких нейронных сетей, которые моделируют человеческое мышление, содержащее нечеткие концепции и логику.	3. Интерпретируемость. Зачастую сложно понять, какие условия влияют на итоги конкретной модели и как модель принимает эти конкретные решения. Именно поэтому такие сети могут быть сложными для исполнения исходного кода программы и объяснения результатов.

Окончание

Положительные стороны нечетких нейронных сетей	Недостатки нечетких нейронных сетей
4. Адаптивность и обучаемость. Нечеткие нейронные сети способны находить закономерности в неупорядоченных данных, что делает их полезными для анализа сложных систем и прогнозирования. Сети обучаются на основе имеющихся данных и адаптируются к изменяющимся условиям.	

Адаптивные нейронные сети

Нейронные сети, которые обладают свойством гибкости и могут автоматически настраивать свою архитектуру и менять вес, чтобы получать более достоверные и точные результаты, называются адаптивными нейронными сетями. Они представляют собой новый класс нейронных сетей, который в процессе обучения и адаптации к новым данным и условиям обладает способностью изменять свои параметры и структуру [Паклин 2003].

За счет добавления, удаления или изменения нейронов, а также связей между ними адаптивные нейронные сети способны изменять свою структуру. Это позволяет им эффективно приспосабливаться к различным задачам и переменным условиям. Они могут обучаться на основе имеющихся данных и опыта, а также использовать обратную связь для корректировки своих параметров и повышения качества решений.

Положительные стороны адаптивных нейронных сетей	Отрицательные стороны, или недостатки, адаптивных нейронных сетей
1. Гибкость и адаптивность. Адаптивные нейронные сети обладают способностью изменять свою структуру и параметры в зависимости от изменяющихся условий и требований задач. Это позволяет им эффективно приспосабливаться к новым ситуациям и достигать более точных результатов.	1. Вычислительная сложность. Обучение и использование адаптивных нейронных сетей может требовать значительных вычислительных ресурсов и времени. Большие и сложные модели могут быть особенно требовательными к вычислительной мощности.

Окончание

Положительные стороны адаптивных нейронных сетей	Отрицательные стороны, или недостатки, адаптивных нейронных сетей
2. Обучение на основе данных. Адаптивные нейронные сети способны изучать информацию из имеющихся данных и извлекать из них закономерности и шаблоны. Они могут прогнозировать, классифицировать и принимать решения на основе полученных знаний, что делает их мощными инструментами для анализа и обработки данных.	2. Зависимость от данных. Качество работы адаптивных нейронных сетей непосредственно зависит от доступных данных. Если данных недостаточно или если данные содержат шум или ошибки, это может негативно сказаться на точности и надежности модели.
3. Автоматическая оптимизация. Адаптивные нейронные сети могут автоматически настраивать свои параметры и веса, чтобы достичь наилучших результатов. Это позволяет им эффективно использовать имеющиеся ресурсы и обеспечивает высокую производительность в различных задачах.	3. Интерпретируемость. Адаптивные нейронные сети могут быть сложными для понимания и объяснения, особенно когда они имеют большое количество нейронов и слоев. Иногда сложно определить, какие именно факторы влияют на принятие решений моделью.

Гауссовская функция принадлежности

Гауссовская функция принадлежности, также известная как нормальная функция принадлежности или функция принадлежности типа Гаусса, представляет собой ценный инструмент в области нечеткой логики и нечетких систем. Ее форма, похожая на колокол или кривую Гаусса, позволяет определить степень принадлежности элемента к нечеткому множеству [Горбаченко, Ахметов, Кузнецова 2023].

Суть гауссовской функции принадлежности заключается в определении, насколько близок элемент к пиковому значению функции. График функции представляет собой симметричную кривую, с параметрами μ и σ, определяющими положение и ширину функции соответственно.

Основные преимущества гауссовской функции принадлежности заключаются в ее гибкости и применимости к различным типам данных. Можно настраивать параметры функции, чтобы адекватно отражать поведение и характеристики конкретных явлений или переменных.

Гладкая и плавная форма гауссовской функции позволяет ей ловко отслеживать даже незначительные изменения и переходы между различными степенями принадлежности. Это особенно полезно в ситуациях, где требуется учесть плавный переход или учесть малые вариации в данных.

Гауссовская функция принадлежности также обладает математической интерпретируемостью. Ее параметры μ и σ могут быть легко связаны с понятными лингвистическими терминами, что облегчает общение с экспертами в соответствующей области и интерпретацию результатов.

Кроме того, гауссовская функция принадлежности демонстрирует хорошие свойства при выполнении нечетких операций, таких как объединение и пересечение нечетких множеств. Она сохраняет свои математические характеристики при применении этих операций, что гарантирует точные и надежные результаты при работе с нечеткими множествами.

В итоге гауссовская функция принадлежности представляет собой ценный инструмент для анализа и моделирования нечетких данных. Ее способность адаптироваться к различным формам данных, гладкость и плавность, интерпретируемость и совместимость с нечеткими операциями делают ее неотъемлемой частью нечеткой логики и нечетких систем.

Обобщенная функция принадлежности Белл

Обобщенная функция принадлежности Белл, также известная как функция принадлежности типа Белл или функция Белла, играет важную роль в области нечеткой логики и нечетких систем. Она используется для определения степени принадлежности элемента к нечеткому множеству [Воронов, Пименов, Небаев 2023].

Названная в честь Джона Белла, который внес существенный вклад в развитие нечеткой логики, обобщенная функция принадлежности Белл характеризуется параметрами, включающими ширину, симметрию и положение пика функции.

Графическое представление обобщенной функции принадлежности Белл является симметричной кривой, которая начинается с нулевого значения, достигает пикового значения и снова снижается до нуля. Форма этой кривой зависит от значений параметров, определяющих ее свойства.

Настройка параметров обобщенной функции принадлежности Белл позволяет создавать различные формы и типы функций, соответствующие разнообразным данным. Например, увеличение

ширины кривой делает ее более плоской, а изменение симметрии и положения пика позволяет адаптировать функцию к конкретным требованиям.

Одно из преимуществ обобщенной функции принадлежности Белл заключается в ее гладкой и непрерывной форме. Это особенно важно при анализе данных, где нужно учесть плавные переходы и тонкие изменения. Такая форма функции обеспечивает точное отображение степени принадлежности в различных ситуациях.

Параметры обобщенной функции принадлежности Белл могут быть легко интерпретированы с помощью лингвистических терминов, что облегчает общение и понимание результатов. Они могут быть связаны с понятиями, такими как ширина, смещение и пиковое значение функции, что упрощает их использование в практических приложениях.

Обобщенная функция принадлежности Белл широко применяется в области нечеткой логики и нечетких систем, включая управление, прогнозирование и принятие решений. Ее гибкость и адаптивность к различным типам данных делают ее незаменимым инструментом в моделировании нечеткости и обработке неопределенности.

В итоге обобщенная функция принадлежности Белл представляет собой мощный инструмент, который позволяет описывать степень принадлежности элементов к нечетким множествам. Ее параметры и гладкая форма обеспечивают гибкость и точность при работе с различными данными, что делает ее незаменимой в нечеткой логике и нечетких системах.

Модель Цукамото

Модель Цукамото является одной из основных моделей нечеткой логики. Эта модель была разработана Лотфи А. Заде и его коллегами в 1970-х годах и широко применяется в различных областях, включая системы управления, прогнозирование, принятие решений и другие [Бессмертный 2023].

Основными компонентами модели Цукамото являются база знаний, набор нечетких правил и механизм вывода. База знаний содержит правила, которые определяют связь между входными переменными и выходными значениями. Каждое правило состоит из условий (антецедентов) и действий (консеквентов), которые определяют значения входных переменных и соответствующие выходные значения.

Механизм вывода модели Цукамото основан на нечеткой логике и использует принципы индуктивного и нечеткого вывода. Вход-

ные нечеткие переменные преобразуются в нечеткие множества с помощью функций принадлежности. Затем применяются нечеткие правила из базы знаний для определения выходных значений. Это осуществляется путем комбинирования и агрегации нечетких правил на основе степени принадлежности входных переменных к условиям правил.

Одной из особенностей модели Цукамото является процесс дефаззификации, который преобразует нечеткие выходные значения в конкретные числовые значения или действия. Для этого используются различные методы, такие как метод центра тяжести, метод максимума или метод среднего значения.

Модель Цукамото предлагает множество преимуществ, включая способность работать с нечеткими данными, учет неопределенности и нечеткости при принятии решений, а также простоту интерпретации результатов. Она является мощным инструментом для моделирования и анализа систем, где применение точных числовых моделей может быть ограничено.

Помимо основных компонентов, модель Цукамото имеет возможность расширяться и адаптироваться для решения более сложных задач. Например, она может быть расширена для работы с нечеткими числовыми переменными, что позволяет учесть нечеткость как в значениях переменных, так и в их числовых диапазонах.

Другое расширение модели Цукамото включает использование различных методов агрегации для объединения нечетких правил и определения выходных значений. Некоторые из наиболее распространенных методов включают метод максимума, метод среднего значения и метод центра тяжести. Каждый из этих методов предоставляет свои преимущества и может быть выбран в зависимости от конкретных потребностей и характеристик задачи.

Модель Цукамото также может быть расширена для работы с нечеткими временными рядами, что позволяет учитывать неопределенность и нечеткость в данных, связанных с изменением во времени. Это открывает дополнительные возможности для прогнозирования и анализа временных рядов в условиях неопределенности.

Важно отметить, что модель Цукамото имеет свои ограничения. Например, при использовании большого числа нечетких правил и переменных возникает проблема комбинаторного взрыва, что может сказаться на вычислительной сложности модели. Кроме того, правильное определение нечетких правил и выбор подходящих функций принадлежности требует экспертного знания и опыта.

Модель Цукамото представляет собой мощный инструмент в области нечеткой логики, способный моделировать и анализировать системы с учетом нечеткости и неопределенности. Ее возмож-

ность расширения и адаптации делает ее гибким инструментом для различных задач прогнозирования, управления и принятия решений в различных областях применения.

Модель TSK

Модель TSK, известная как модель Такаги-Сугено-Канг, представляет собой разновидность нечетких моделей, разработанных для анализа данных, прогнозирования и систем управления. Она состоит из трех ключевых компонентов: базы правил, базы данных и механизма вывода [Колесникова 2023].

В базе правил содержится набор нечетких правил, которые связывают входные переменные с выходными значениями модели. Каждое правило состоит из условий (антецедентов), определяющих значения входных переменных, и действий (консеквентов), определяющих выходные значения.

База данных представляет собой набор данных, используемых для определения параметров модели. Эти параметры включают коэффициенты функций принадлежности и линейных функций активации. Они определяют форму функций принадлежности и линейные соотношения между входными и выходными переменными.

Механизм вывода модели TSK основан на комбинации нечетких правил и агрегации выходных значений. В отличие от других нечетких моделей, где выходные значения представлены нечеткими множествами, в модели TSK выходные значения представляются линейными функциями от входных переменных. Это делает модель TSK более подходящей для решения задач аппроксимации и регрессии.

Основным преимуществом модели TSK является ее способность захватывать нелинейные зависимости между входными и выходными переменными с помощью линейных функций активации. Каждое нечеткое правило в модели TSK имеет свою собственную линейную функцию активации, которая определяет, как входные переменные влияют на выходные значения. Коэффициенты функций активации вычисляются на основе данных из базы данных модели.

Несмотря на преимущества, модель TSK имеет свои ограничения. Например, при использовании большого количества правил может возникнуть проблема переобучения. Также важно правильно выбрать количество правил и определить соответствующие функции активации, что требует опыта и экспертного знания.

В итоге модель TSK представляет собой мощный инструмент для анализа данных и прогнозирования на основе нечеткой логики.

Благодаря базе правил, базе данных и механизму вывода она обладает гибкостью и способностью эффективно решать разнообразные задачи аппроксимации и моделирования данных.

Модель CANFIS (Co-Active Neuro-Fuzzy Inference System)

Модель Co-Active Neuro-Fuzzy Inference System (CANFIS) представляет собой адаптивную нейро-нечеткую систему, которая сочетает в себе нейронные сети и нечеткую логику для обработки данных с неопределенностью и нечеткостью [Новиков 2023].

CANFIS использует нечеткие правила и механизмы вывода для преобразования входных данных в выходные значения. Она состоит из нескольких слоев, включая входной слой, скрытые слои и выходной слой, где каждый слой содержит нейроны, выполняющие нечеткую активацию и вывод результатов.

Особенностью модели CANFIS является ее способность к активному сотрудничеству (коактивации), когда каждый нейрон в сети влияет на активность других нейронов в процессе вывода. Это позволяет модели адаптивно обучаться на основе обратного распространения ошибки и оптимизировать ее параметры для достижения желаемых результатов.

CANFIS находит применение в различных задачах, таких как аппроксимация функций, классификация данных, прогнозирование временных рядов, а также в системном управлении и принятии решений на основе нечеткой информации.

Модель CANFIS (Co-Active Neuro-Fuzzy Inference System) представляет собой гибкую адаптивную сеть, основанную на нечетком выводе, которая применяется для прогнозирования и моделирования сложных систем. Она объединяет преимущества нечеткой логики и нейронных сетей, создавая мощный инструмент для анализа и решения сложных задач.

CANFIS состоит из двух ключевых компонентов: нечеткой сети и адаптивной сети. Нечеткая сеть отвечает за обработку нечетких правил и логического вывода, а адаптивная сеть выполняет обучение и адаптацию модели на основе имеющихся данных.

Главная цель этой модели заключается в создании адаптивной модели, способной моделировать системы с неопределенностью и размытостью. Она способна обрабатывать данные и принимать решения на основе нечетких правил. CANFIS находит применение в различных областях, включая прогнозирование, управление, классификацию и анализ данных.

Преимущества модели CANFIS заключаются в ее способности обучаться на основе имеющихся данных, адаптироваться к изменяющимся условиям и учитывать неопределенность и размытость в данных. Она позволяет учесть сложные и нечеткие концепции, что делает ее полезной для решения реальных задач, где точные значения могут быть неизвестны или приближенны. Эта модель обладает большим потенциалом в области анализа данных и принятия решений в условиях неопределенности [Новиков 2023].

Процесс работы модели CANFIS включает следующие основные шаги.

1. *Инициализация модели*. Начальная структура модели создается путем определения числа нечетких наборов правил и функций принадлежности для каждой входной переменной. Это может быть выполнено путем предварительного определения или с использованием алгоритмов конструкции, таких как алгоритм кластеризации данных или генетический алгоритм.

2. *Фаззификация*. Входные данные преобразуются в нечеткие значения с использованием функций принадлежности. Функции принадлежности определяют степень принадлежности каждого входного значения к различным нечетким множествам, которые описывают лингвистические переменные. Это позволяет учесть неопределенность и размытость входных данных.

3. *Процесс вывода*. На основе нечетких правил, определенных в базе знаний модели, происходит процесс вывода, который определяет связь между входными и выходными переменными. Каждое правило имеет условие (IF-часть), которое проверяет значения входных переменных, и результат (THEN-часть), который определяет значение выходной переменной. Процесс вывода использует функции принадлежности и операции нечеткой логики для комбинирования правил и получения выходных значений.

4. *Агрегация*. Выходные значения, полученные из различных правил, агрегируются для получения единого выходного значения модели. Это может быть выполнено с помощью различных методов агрегации, таких как взвешенная сумма или центр тяжести нечетких значений.

5. *Дефаззификация*. Полученное агрегированное выходное значение преобразуется обратно в определенное числовое значение путем процесса дефаззификации. Это может быть выполнено с использованием методов, таких как центр тяжести, средневзвешенное значение или другие методы нечеткого вывода.

6. *Обучение и адаптация*. Модель CANFIS может быть обучена на основе тренировочных данных для настройки параметров мо-

дели и достижения желаемых результатов. Это может включать оптимизацию параметров функций принадлежности, весов правил и других параметров модели. Обучение может быть выполнено с использованием методов градиентного спуска, эволюционной оптимизации или других алгоритмов.

7. *Тестирование и оценка.* После обучения модель проверяется на тестовых данных для оценки ее производительности и точности предсказания. Это позволяет оценить эффективность модели и ее способность обобщать новые данные.

8. *Адаптация модели.* В случае необходимости модель может быть адаптирована к новым условиям или изменяющимся требованиям путем повторного обучения или регуляризации параметров.

Процесс работы модели CANFIS может быть гибким и настраиваемым в зависимости от конкретной задачи и требований. Он объединяет преимущества нечеткой логики и искусственных нейронных сетей, что делает его мощным инструментом для моделирования сложных систем и решения разнообразных задач.

Заключение

В статье проведена обзорная аналитика существующих методов и подходов к моделированию и прогнозированию с использованием нейро-нечетких систем. Выбор для дальнейшей работы пал на модель Co-Active Neuro-Fuzzy Inference System (CANFIS), которая представляет собой адаптивную нейро-нечеткую систему, сочетающую в себе нейронные сети и нечеткую логику для обработки данных с неопределенностью и нечеткостью.

CANFIS использует нечеткие правила и механизмы вывода для преобразования входных данных в выходные значения. Она состоит из нескольких слоев, включая входной слой, скрытые слои и выходной слой, где каждый слой содержит нейроны, выполняющие нечеткую активацию и вывод результатов.

CANFIS находит применение в различных задачах, таких как аппроксимация функций, классификация данных, прогнозирование временных рядов, а также в системном управлении и принятии решений на основе нечеткой информации.

Модель CANFIS (Co-Active Neuro-Fuzzy Inference System) представляет собой гибкую адаптивную сеть, основанную на нечетком выводе, которая применяется для прогнозирования и моделирования сложных систем. Она объединяет преимущества нечеткой логики и нейронных сетей, создавая мощный инструмент для анализа и решения сложных задач.

Литература

Алтунин, Семухин 2000 – *Алтунин А.Е., Семухин М.В.* Модели и алгоритмы принятия решений в нечетких условиях. Тюмень: ТГУ, 2000. 352 с.

Андрейчиков, Андрейчикова 2000 – *Андрейчиков А.В., Андрейчикова О.Н.* Анализ, синтез и планирование решений в экономике. М.: Финансы и статистика, 2000. 363 с.

Бессмертный 2023 – *Бессмертный И.А.* Системы искусственного интеллекта: Учеб. пособ. для среднего профессионального образования. М.: Юрайт, 2023. 157 с.

Борисов, Алексеев, Крумберг 1982 – *Борисов А.Н., Алексеев А.В., Крумберг О.А.* Модели принятия решений на основе лингвистической переменной. Рига: Зинатне, 1982. 256 с.

Борисов, Крумберг, Федоров 1990 – *Борисов А.Н., Крумберг О.А., Федоров И.П.* Принятие решений на основе нечетких моделей: примеры использования. Рига: Зинатне, 1990. 184 с.

Воронов, Пименов, Небаев 2023 – *Воронов М.В., Пименов В.И., Небаев И.А.* Системы искусственного интеллекта: Учеб. и практикум для вузов. М.: Юрайт, 2023. 268 с.

Горбаченко, Ахметов, Кузнецова 2023 – *Горбаченко В.И., Ахметов Б.С., Кузнецова О.Ю.* Интеллектуальные системы: нечеткие системы и сети: Учеб. пособие для вузов. М.: Юрайт, 2023. 105 с.

Колесникова 2023 – *Колесникова С. М.* Когнитивная лингвистика: Учеб. для вузов. М.: Юрайт, 2023. 192 с.

Кравченко 2002 – *Кравченко Ю.А.* Перспективы развития гибридных интеллектуальных систем // Перспективные информационные технологии и интеллектуальные системы. 2002. № 3. С. 34–38.

Новиков 2023 – *Новиков Ф.А.* Символический искусственный интеллект: математические основы представления знаний: Учеб. пособие для вузов. М.: Юрайт, 2023. 278 с.

Паклин 2003 – *Паклин Н.Б.* Адаптивные системы нечеткого логического вывода и их приложения // Интеллектуальные системы в производстве. 2003. № 2. С. 138–151.

Поспелов 1986 – *Поспелов Д.А.* Нечеткие множества в моделях управления и искусственного интеллекта. М.: Наука, 1986. 311 с.

References

Altunin, A.E. and Semukhin, M.V. (2000), *Modeli i algoritmy prinyatiya reshenii v nechetkikh usloviyakh* [Models and algorithms for decision making in fuzzy conditions], TSU, Tyumen, Russia, 352 p.

Andreichikov, A.V. and Andreichikova, O.N. (2000), *Analiz, sintez i planirovanie reshenii v ekonomike* [Analysis, synthesis and planning of decisions in economics], Finansy i statistika, Moscow, Russia, 363 p.

Bessmertnyi, I. A. (2023), *Sistemy iskusstvennogo intellekta: ucheb. posob. dlya srednego professional'nogo obrazovaniya* [Artificial intelligence systems. A study guide for secondary vocational education, Yurait, Moscow, Russia, 157 p.

Borisov, A.N., Alekseev, A.V. and Krumberg, O.A. (1982), *Modeli prinyatiya reshenii na osnove lingvisticheskoi peremennoi* [Models of decision making based on linguistic variables], Zinatne, Riga, Latvia, 256 p.

Borisov, A.N., Krumberg, O.A. and Fedorov, I.P. (1990), *Prinyatie reshenii na osnove nechetkikh modelei: primery ispol'zovaniya* [Decision making based on fuzzy models: examples of use], Zinatne, Riga, Latvia, 184 p.

Gorbachenko, V.I., Akhmetov, B.S., and Kuznetsova, O.Yu. (2023), *Intellektual'nye sistemy: nechetkie sistemy i seti: ucheb. posobie dlya vuzov* [Intelligent systems: fuzzy systems and networks. A study guide for universities], Yurait, Moscow, Russia, 105 p.

Kolesnikova, S.M. (2023), *Kognitivnaya lingvistika: uchebnik dlya vuzov* [Cognitive linguistics. A textbook for universities], Yurait, Moscow, Russia, 192 p.

Kravchenko, Yu.A. (2002), "Prospects for the development of hybrid intelligent systems", *Perspective information technologies and intelligent systems*, no. 3, pp. 34–38.

Novikov, F.A. (2023), *Simvolicheskii iskusstvennyi intellekt: matematicheskie osnovy predstavleniya znanii: ucheb. posobie dlya vuzov* [Symbolic artificial intelligence: mathematical foundations of knowledge representation. A study guide for universities], Yurait, Moscow, Russia, 278 p.

Paklin, N.B. (2003), "Adaptive systems of fuzzy logical inference and their applications use", *Intelligent systems in production*, no. 2, pp. 138–151.

Pospelov, D.A. (1986), *Nechetkie mnozhestva v modelyakh upravleniya i iskusstvennogo intellekta* [Fuzzy sets in control and artificial intelligence models], Nauka, Moscow, 311 p.

Voronov, M.V., Pimenov, V.I. and Nebaev, I.A. (2023), *Sistemy iskusstvennogo intellekta: ucheb. i praktikum dlya vuzov* [Artificial intelligence systems. A textbook and workshop for universities], Yurait, Moscow, Russia, 268 p.

Информация об авторе

Андрей П. Титов, кандидат технических наук, доцент, Российский технологический университет МИРЭА, Москва, Россия; 107076, Россия, Москва, ул. Стромынка, д. 20, titov_and@mail.ru

Information about the author

Andrei P. Titov, Cand. of Sci. (Computer Science), associate professor, Russian Technological University MIREA, Moscow, Russia; 20, Stromynka Str., Moscow, 107076, Russia; titov_and@mail.ru

УДК 004.421
DOI: 10.28995/2686-679X-2024-1-36-50

Потенциал генетических алгоритмов в задачах покрытия территории группой БЛА

Рамиль Ф. Файзуллин
Казанский (Приволжский) федеральный университет, Казань, Россия, fzllnrml@gmail.com

Аннотация. Беспилотные летательные аппараты (БЛА) стали ключевыми средствами в задачах автоматизированного покрытия территорий благодаря тому, что они не ограничены препятствиями на земле и способны быстро выполнять задачи. Однако при планировании маршрутов для БЛА при охвате территории возникают сложности в поиске оптимальных решений из-за вычислительной сложности задачи. Поэтому при решении задач с группой БЛА на больших территориях используются эвристические алгоритмы для поиска путей охвата, близких к оптимальным. Одним из популярных алгоритмов для этого является генетический алгоритм. Статья исследует потенциал применения генетических алгоритмов в контексте решения задачи покрытия территории с использованием группы БЛА. В статье проведен обзор методов разработки и оптимизации модифицированных генетических алгоритмов, учитывающих уникальные особенности задачи охвата. Анализируются характеристики генетического алгоритма и представления хромосом при решении задачи охвата, в зависимости от разного вида представления территорий. Рассматриваются особенности применения генетических операций к хромосомам, отражающим траекторию движения БЛА, а также особенности задачи при работе с группой БЛА. Кроме того, обсуждаются методы предотвращения столкновений в миссиях с группой БЛА, их преимущества и ограничения.

Ключевые слова: генетический алгоритм, планирование пути покрытия, оптимизация пути

Для цитирования: Файзуллин Р.Ф. Потенциал генетических алгоритмов в задачах покрытия территории группой БЛА // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 1. С. 36–50. DOI: 10.28995/2686-679X-2024-1-36-50

Potential of genetic algorithms in tasks of the territory coverage by a group of UAVs

Ramil F. Faizullin
Kazan (Volga region) Federal University, Kazan, Russia,
fzllnrml@gmail.com

Abstract. Unmanned aerial vehicles (UAVs) have become key tools in automated area coverage tasks due to the fact that they are not limited by obstacles on the ground and are able to quickly complete tasks. However, when planning routes for UAVs covering an area, difficulties arise in finding optimal solutions due to the computational complexity of the problem. Therefore, when solving problems with a group of UAVs over large areas, heuristic algorithms are used to find coverage paths that are close to optimal. One popular algorithm for that is the genetic algorithm. The article studies the potential of using genetic algorithms in the context of solving the problem of covering an area using a group of UAVs. The article provides a review of methods for developing and optimizing modified genetic algorithms that take into account the unique features of the coverage problem. The characteristics of the genetic algorithm and the representation of chromosomes when solving the coverage problem are analyzed, depending on the different types of representation of territories. The article considers features of applying genetic operations to chromosomes that reflect the trajectory of the UAV, as well as the features of the task when working with a group of UAVs. In addition, it also discusses collision avoidance techniques in UAV swarm missions, their advantages and limitations.

Keywords: genetic algorithms, coverage path planning, path optimization

For citation: Faizullin, R.F. (2024), "Potential of genetic algorithms in tasks of the territory coverage by a group of UAVs", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series,* no. 1, pp. 36–50, DOI: 10.28995/2686-679X-2024-1-36-50

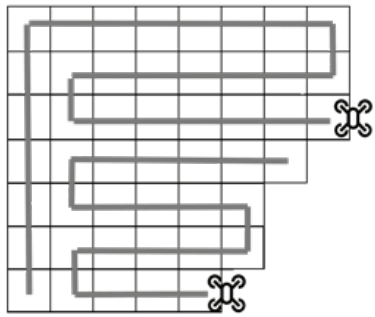
Введение

В мобильной робототехнике часто возникает необходимость в решении задачи планирования пути покрытия для мобильных роботов. Основной целью этой задачи является поиск оптимального пути, который позволит мобильному роботу посетить все точки заранее заданной области, избегая при этом столкновений с препятствиями [Galceran, Carreras 2013].

На данный момент беспилотные летательные аппараты (БЛА) наиболее часто используются в области автоматизированного покрытия территорий. БЛА стали популярными в современной робототехнике по множеству причин. Они не ограничены препятствиями на земле, способны быстро перемещаться в труднодоступных местах, выполняя различные задачи за короткое время [Denisov, Sagitov, Yakovlev, Su, Svinin, Magid 2019]. Эти преимущества делают БЛА важными инструментами в задачах покрытия и придают им конкурентное преимущество перед другими мобильными роботами. Поэтому они применяются для разведки [Park, Choi 2020], мониторинга [Ren, Zhao, Xiao, Hu 2019], военных операций и поисково-спасательных миссий [Martinez-Alpiste, Golcarenarenji, Wang, Alcaraz-Calero 2021], повышая безопасность и снижая риски для человеческой жизни. Развитие технологий и постоянное совершенствование беспилотных систем значительно расширяют функциональные возможности таких аппаратов, а также повышают их надежность. Эти факторы подчеркивают актуальность и значимость задачи использования БЛА для автоматизированного покрытия.

Задача покрытия территории группой БЛА представляет собой задачу поиска траектории движения для каждого БЛА таким образом, что БЛА посещают все точки заданной территории и при этом не сталкиваются между собой [Петренко, Тебуева, Павлов, Гурчинский 2022]. Данная задача может иметь вводимые ограничения, например, ограничение на время выполнения всей миссии, ограничения по безопасности, связанные с минимальным расстоянием сближения для БЛА, ограничение на дальность полета для каждой БЛА, связанное с конечной емкостью батареи БЛА, и иные ограничения, требуемые на практике.

В задачах покрытия важно учесть представление территории и вид ее декомпозиции. Декомпозиция разбивает территорию на простые, непересекающиеся ячейки, легкие для охвата. Одним из популярных вариантов декомпозиции является декомпозиция на основе сетки. Территория разделяется на одинаковые по размеру прямоугольные элементы сетки. Каждый элемент нумеруется. Траекторию движения БЛА в таком случае отражает последовательность чисел, обозначающая номера ячеек сетки, по которым двигался БЛА. Обычно ячейка сетки выбирается квадратной и равной размерам охвата территории датчиком, установленной на БЛА.



41	42	43	44	45	46	47	48
33	34	35	36	37	38	39	40
25	26	27	28	29	30	31	32
18	19	20	21	22	23	24	
12	13	14	15	16	17		
6	7	8	9	10	11		
1	2	3	4	5			

Рис. 1. Пример охвата территории с наложенной сеткой с помощью двух БЛА

Всю территорию, подлежащую охвату, обозначим через M. Предположим, что M разбито на n одинаковых ячеек $M = \{m_1, m_2, ... m_n\}$. В группе U имеется k БЛА: $U = \{U_1, U_2, ... U_k\}$. Тогда траекторию каждой i-й БЛА – $T(U_i)$ можно обозначить как последовательность $T(U_i) = \{m_{1i}, m_{2i}, m_{3i} ... m_{si}\}$, где $m_{ij} \in M$. БЛА на каждом шаге может передвигаться на соседнюю ячейку в сетке. Длину траектории обозначим $|T(U_i)|$, она будет включать число охваченных ячеек для $БЛА_i$ при движении по траектории $T(U_i)$. При этом не должно оставаться неохваченных ячеек, поэтому $\cup_i T(U_i) = M$, то есть объединение всех траекторий БЛА составляет территорию, подлежащую охвату. Для предотвращения столкновений будем предполагать, что ячейку может посещать только единственная БЛА. Также будем предполагать, что БЛА двигаются равномерно с одинаковой скоростью, и время пролета траектории БЛА пропорционально ее длине. Поэтому время миссии будет равно времени полета БЛА с самой длинной траекторией. Тогда задача покрытия территории для заданной территории M и группы БЛА U сводится к поиску траектории $T(U_i)$ для каждого БЛА.

К данной задаче могут накладываться дополнительные условия. Например, ограничение по времени на всю миссию можно ввести как: $\max_i(|T(U_i)|) < W$, где W обозначает максимальную длину траектории, которую может пройти БЛА за заданное ограниченное время.

Задача поиска пути покрытия для мобильного робота является NP-трудной [Arkin, Fekete, Mitchell 2000] в связи с необходимостью анализа всего множества возможных решений, число которых экспоненциально возрастает с увеличением сложности и размера

территории, подлежащей покрытию. Поэтому для данного класса задач не существует универсальных алгоритмов, способных находить оптимальное решение за полиномиальное время от размера входных данных. Для поиска решений на практике используют эвристические алгоритмы. Они не находят гарантированно оптимальное решение, однако позволяют достаточно быстро приближаться к данному решению.

Одним из популярных эвристических алгоритмов являются генетические алгоритмы. Они обладают рядом преимуществ при решении задач поиска. При сравнительно простой реализации алгоритма выполнение генетического алгоритма легко распараллелить, что особенно важно при работе с обширными пространствами решений. Генетические алгоритмы также позволяют находить решения в задачах с множеством критериев для оптимизации, что часто встречается на практике. Они предоставляют метод для исследования всего пространства решений с целью поиска глобального оптимума, что полезно в задачах со множеством локальных экстремумов. Генетические алгоритмы легко адаптировать под различные задачи, потому что они способны работать со множеством представлений для решений, включая целые и вещественные числа, а также бинарные строки. Все это делает генетические алгоритмы эффективными для решения задач поиска пути покрытия для мобильных роботов.

Целью данной статьи является обзор методов разработки модифицированных генетических алгоритмов, специально адаптированных для решения задачи покрытия территории группой БЛА. В статье рассматриваются классические одноцелевые генетические алгоритмы. В случае многоцелевой оптимизации в задаче охвата территории подразумевается, что все цели могут быть объединены в единую целевую функцию.

Генетические алгоритмы

Генетические алгоритмы, опираясь на принципы биологической эволюции, часто применяются для решения задач поиска [Katoch, Chauhan, Kumar 2021]. Они моделируют процесс естественного отбора с целью нахождения оптимальных решений. Эти алгоритмы взаимодействуют с популяцией потенциальных решений, каждое из которых называется индивидуумом. Путем последовательной оценки множества решений создается новое поколение, где наилучшие решения имеют более высокие шансы передать свои характеристики следующему поколению. Со временем решения в популяции становятся более адаптированными к поставленной задаче.

Генетический алгоритм на первом этапе создает начальную популяцию, которая чаще всего состоит из случайных хромосом. Каждая хромосома – это возможное решение задачи. Определяется целевая функция, которая присваивает каждой хромосоме числовое значение, отражающее эффективность данной хромосомы в решении задачи. Далее из популяции отбираются фиксированным способом индивидуумы для создания следующего поколения. Индивидуумы, демонстрирующие более высокую пригодность к окружающей среде, имеют больший шанс на выживание и передачу своих характеристик следующему поколению, что ведет к улучшению популяции с течением времени. Происходит операция кроссовера для образования новых хромосом потомков, это позволяет новым индивидуумам наследовать лучшие характеристики от своих родителей, сохраняя их для будущих поколений. Мутации – это случайные изменения в характеристиках индивидуумов, которые поддерживают генетическое разнообразие и периодически способствуют значительным рывкам в развитии популяции. После кроссовера с некоторой вероятностью применяется операция мутации, которая незначительно изменяет хромосомы потомка.

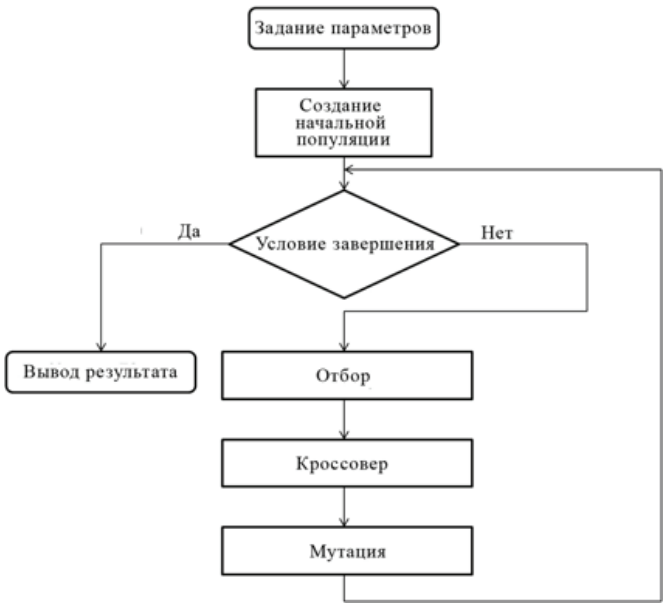


Рис. 2. Этапы генетического алгоритма

В задаче охвата территории для БЛА необходимо найти оптимальную траекторию, при которой БЛА посещает все заданные точки на территории. Поэтому каждая хромосома будет кодировать траекторию движения БЛА. В контексте использования генетического алгоритма для решения задачи охвата популяция будет представлять собой множество потенциальных траекторий БЛА. Способ кодирования траектории в хромосому может быть произвольным. На практике обычно хромосомы представляют собой последовательности целых чисел [Tuncer, Yildirim 2011].

Рис. 3. Пример хромосомы в генетическом алгоритме

Особенности применения генетических операторов в задаче покрытия территории

Важной особенностью применения генетического алгоритма в задаче поиска пути покрытия является то, что даже после операций кроссовера или мутации хромосома должна кодировать некоторую траекторию для БЛА. Поэтому на операции кроссовера и мутации должны накладываться определенные ограничения.

В случае применения классических операций кроссовера и мутации хромосома может перестать отражать траекторию движения БЛА, то есть перестать быть решением задачи.

На рис. 4 представлена классическая операция одноточечного кроссовера, при котором образуются два потомка. Хромосома в данном алгоритме представляет собой порядок посещения ячеек, свободных от препятствий, при охвате территории БЛА. Если родители представляют собой допустимые для задачи хромосомы, то потомки содержат одинаковые гены и не представляют собой решения задачи обхода траектории. Например, первый потомок содержит одинаковые гены 1 и 3, поэтому, согласно хромосоме, траектория БЛА дважды проходит через области 1 и 3, но при этом не покрывает области 2 и 8.

Одним из вариантов решения является модификация операции кроссовера. Например, использование двухточечного кроссовера от одного родителя [Pham, Bestaoui, Mammar 2017].

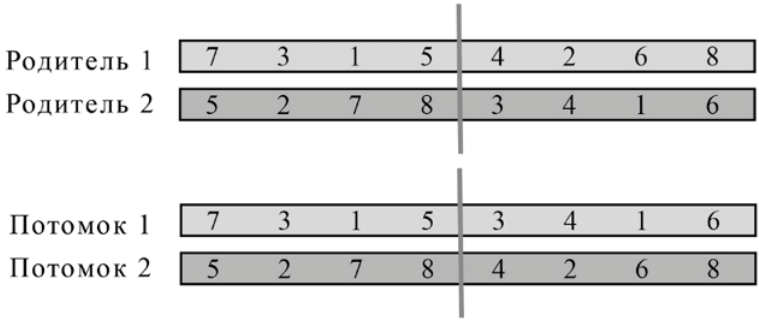


Рис. 4. Пример операции кроссовера,
при котором потомки перестают отражать траекторию движения

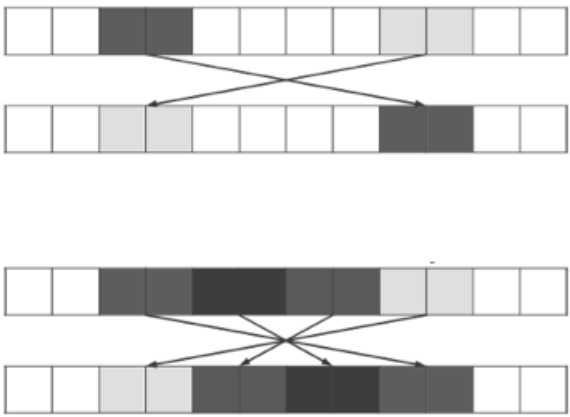


Рис. 5. Пример двухточечного кроссовера от одного родителя

При таком способе кроссовера от одного родителя образуется много потомков, и далее выбираются два с наибольшим значением целевой функции. При этом можно быть уверенным, что каждый потомок отражает некую траекторию для обхода территории. Согласно статье [Pham, Bestaoui, Mammar 2017], при симуляции работы генетического алгоритма с предложенным методом кроссовера удалось добиться ускорения вычислений более чем в 4 раза.

Задачи покрытия
для одного БЛА и группы БЛА

На практике задачу охвата территории более эффективно решать с привлечением группы БЛА. Это необходимо не только для повышения скорости охвата, так как несколько БЛА могут работать одновременно и тем самым сократить время выполнения задачи, но и для обеспечения надежности. В случае, если один из БЛА выходит из строя, другие могут завершить выполнение миссии. Особенно это актуально при работе на больших территориях, где ограничены временные рамки для завершения задачи [Maza, Ollero 2007].

БЛА является движущимся препятствием для остальных БЛА, и нельзя планировать его маршрут в отрыве от остальной группы [Bai, Wang, Svinin, Magid, Sun 2022]. Поэтому генетический алгоритм должен учитывать маршруты всех БЛА в совокупности.

Решением задачи охвата территории группой БЛА является траектория для каждого БЛА, при которой они совместно покрывают заданную территорию и не сталкиваются между собой. В этом случае решение должно объединять траектории всех БЛА в одну хромосому.

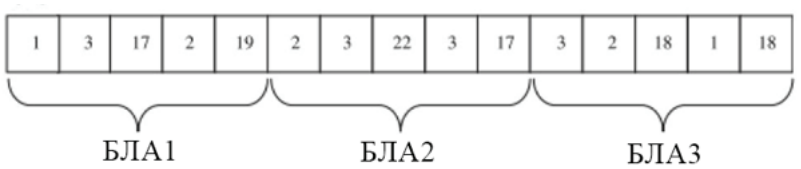


Рис. 6. Пример хромосомы,
объединяющей траектории движения трех БЛА

Использование группы БЛА для охвата территории способно не только сократить время выполнения задачи, но также влечет потенциальные риски столкновения БЛА во время выполнения миссии. Для предотвращения столкновений существуют различные стратегии планирования пути группы БЛА. Рассмотрим эти стратегии применительно к генетическим алгоритмам.

Стратегии предотвращения столкновений группы БЛА при охвате территории

1. Выделение для каждого БЛА своей области для охвата.

Для предотвращения сталкивания в воздухе БЛА можно разделить территорию на равные области и каждому БЛА поручить для охвата свою область [Almadhoun, Taha, Seneviratne, Zweiri 2019]. Данный метод упростит задачу, и можно будет перейти к задаче с одним БЛА. Для каждого БЛА при этом запускается свой генетический алгоритм, и выполняется поиск пути охвата для выделенной ему области.

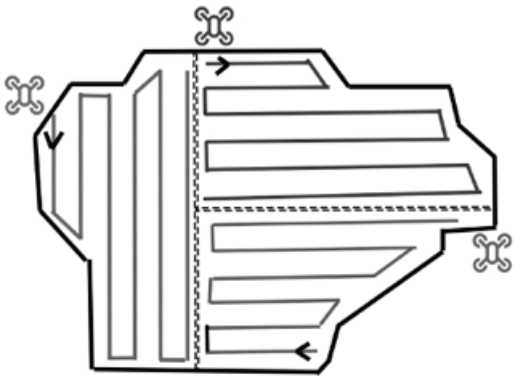


Рис. 7. Пример разделения территории для охвата на отдельные области для каждого БЛА

Преимущества данной стратегии:
- возможность легкого распараллеливания вычислений для каждого БЛА, потому что их траектории никак не зависят друг от друга;
- модель генетического алгоритма остается простой и не требует дополнительных модификаций.

Недостатки данной стратегии:
- эффективность итогового охвата группой БЛА сильно зависит от эффективности разделения на области для каждого отдельного БЛА;
- если группа БЛА вылетает из единой точки, следует учесть предотвращение столкновений при движении БЛА к своим областям;

– если территория для охвата имеет разный приоритет обследования, то это сложнее учесть при разделении территории на области.

2. Штраф за приближение БЛА друг к другу.

В задаче покрытия территории хромосома в генетическом алгоритме задает траекторию движения группы БЛА. На каждом этапе работы генетического алгоритма происходит оценка каждой хромосомы популяции с помощью целевой функции, которая ставит в соответствие хромосоме число, которое отражает, насколько успешно данная хромосома решает задачу. Чем выше это значение, тем лучше данные траектории БЛА выполняют охват. Если в момент охвата территории БЛА подлетали слишком близко друг к другу, то можно ввести функцию штрафа, которая будет уменьшать значение целевой функции [Nazarahari, Khanmirza, Doostie 2019].

Для этого введем понятие безопасного расстояния между двумя БЛА. Обозначим его Sd. Через $l_{(i,j)}$ обозначим минимальное расстояние между $БЛА_i$ и $БЛА_j$. Тогда функцию штрафа $F_{penalty}(БЛА_i)$ можно определить следующим образом:

$$F_{penalty}(БЛА_i) = \begin{cases} 0, \text{ если } \forall j: i \neq j \Rightarrow \min(l_{(i,j)}) > Sd \\ \frac{1}{l_{(i,j)}}, \text{ если } \exists j: i \neq j, \min\left(l_{(i,j)}\right) < Sd \end{cases}$$

Сумма штрафов для всех БЛА $\sum F_{penalty}(БЛА_i)$ вычитается из значения целевой функции потенциального решения.

Преимущества данной стратегии:

– гибкий способ влиять на генетический алгоритм через целевую функцию. Позволяет в зависимости от целей задачи использовать разные штрафные функции. Например, экспоненциально возрастающие для задач, в которых фактор безопасности является критически важным.

Недостатки данной стратегии:

– требуется попарное сравнение минимального расстояния между каждой парой БЛА. При увеличении количества БЛА сложность сравнений возрастает экспоненциально.

Заключение

В контексте задачи покрытия известной территории с использованием группы беспилотных летательных аппаратов приходим к выводу о необходимости адаптации классических генетических алгоритмов к уникальным требованиям этой задачи. Использование стандартных операторов классического генетического алгоритма в данном контексте может вызвать разрушение структуры, где каждая хромосома представляет собой траекторию движения группы БЛА. В зависимости от метода представления и декомпозиции территории, а также от наложенных ограничений и требований к итоговым траекториям БЛА, требуется модификация генетического алгоритма. Следует также учесть стратегии предотвращения столкновений группы БЛА в период выполнения миссии.

Разработка генетических алгоритмов, адаптированных к характеристикам задачи охвата территории с помощью БЛА, предоставляет значительные перспективы для увеличения эффективности данного процесса.

Литература

Петренко, Тебуева, Павлов, Гурчинский 2022 – *Петренко В.И., Тебуева Ф.Б., Павлов А.С., Гурчинский М.М.* Метод распределения и планирования выполнения задач агентами роевых робототехнических систем в условиях недетерминированной среды // Прикаспийский журнал: управление и высокие технологии. 2022. № 3 (59). С. 25–43.

Almadhoun, Taha, Seneviratne, Zweiri 2019 – *Almadhoun R., Taha T., Seneviratne L., Zweiri Y.* A survey on multi-robot coverage path planning for model reconstruction and mapping // SN Applied Sciences. 2019. Vol. 1, no. 8. P. 847.

Arkin, Fekete, Mitchell 2000 – *Arkin E.M., Fekete S.P., Mitchell J.S.B.* Approximation algorithms for lawn mowing and milling // Computational Geometry. 2000. Vol. 17, no. 1–2. P. 25–50.

Bai, Wang, Svinin, Magid, Sun 2022 – *Bai Y., Wang Y., Svinin M., Magid E., Sun R.* Adaptive Multi-Agent Coverage Control With Obstacle Avoidance // IEEE Control Systems Letters. 2022. Vol. 6. P. 944–949.

Denisov, Sagitov, Yakovlev, Su, Svinin, Magid 2019 – *Denisov E., Sagitov A., Yakovlev K., Su K.-L., Svinin M., Magid E.* Towards Total Coverage in Autonomous Exploration for UGV in 2.5 D Dense Clutter Environment // Proceedings of the XVI International Conference on Informatics in Control, Automation and Robotics, Prague, Czech Republic. Montreal: SCITEPRESS – Science and Technology Publications, 2019. P. 409–416.

Galceran, Carreras 2013 – *Galceran E., Carreras M.* A survey on coverage path planning for robotics // Robotics and Autonomous Systems. 2013. Vol. 61, no. 12. P. 1258–1276.

Katoch, Chauhan, Kumar 2021 – *Katoch S., Chauhan S.S., Kumar V.* A review on genetic algorithm: past, present, and future // Multimedia Tools and Applications. 2021. Vol. 80 no. 5, pp. 8091–8126.

Martinez-Alpiste, Golcarenarenji, Wang, Alcaraz-Calero 2021 – *Martinez-Alpiste I., Golcarenarenji G., Wang Q., Alcaraz-Calero J.M.* Search and rescue operation using UAVs: A case study // Expert Systems with Applications. 2021. Vol. 178. P. 114–937.

Maza, Ollero 2007 – *Maza I., Ollero A.* Multiple UAV cooperative searching operation using polygon area decomposition and efficient coverage algorithms // Distributed Autonomous Robotic Systems 6, Japan, Tokyo. Cham: Springer, 2007. P. 221–230.

Nazarahari, Khanmirza, Doostie 2019 – *Nazarahari M., Khanmirza E., Doostie S.* Multi-objective multi-robot path planning in continuous environment using an enhanced genetic algorithm // Expert Systems with Applications. 2019. Vol. 115. P. 106–120.

Park, Choi 2020 – Park S., Choi Y. Applications of Unmanned Aerial Vehicles in Mining from Exploration to Reclamation: A review // Minerals. 2020. Vol. 10, no. 8. P. 663.

Pham, Bestaoui, Mammar 2017 – *Pham T.H., Bestaoui Y., Mammar S.* Aerial robot coverage path planning approach with concave obstacles in precision agriculture // Education and Development of Unmanned Aerial Systems RED-UAS, Linkoping, Sweden. New York, NY: IEEE, 2017. P. 43–48.

Ren, Zhao, Xiao, Hu 2019 – *Ren H., Zhao Y., Xiao W., Hu Z.* A review of UAV monitoring in mining areas: current status and future perspectives // International Journal of Coal Science & Technology. 2019. Vol. 6, no. 3. P. 320–333.

Tuncer, Yildirim 2011 – *Tuncer A., Yildirim M.* Chromosome Coding Methods in Genetic Algorithm for Path Planning of Mobile Robots // XXVI International Symposium on Computer and Information Sciences, London, United Kingdom. Cham: Springer, 2011. P. 377–383.

References

Almadhoun, R., Taha, T., Seneviratne, L. and Zweiri, Y. (2019), “A survey on multi-robot coverage path planning for model reconstruction and mapping”, *SN Applied Sciences*, vol. 1, no. 8, pp. 847.

Arkin, E.M., Fekete, S.P. and Mitchell, J.S.B. (2000), “Approximation algorithms for lawn mowing and milling”, *Computational Geometry*, vol. 17, no. 1–2, pp. 25–50.

Bai, Y., Wang, Y., Svinin, M., Magid, E. and Sun, R. (2022), "Adaptive Multi-Agent Coverage Control with Obstacle Avoidance", *IEEE Control Systems Letters*, vol. 6, pp. 944–949.

Denisov, E., Sagitov, A., Yakovlev, K., Su, K.-L., Svinin, M. and Magid, E. (2019), "Towards total coverage in autonomous exploration for UGV in 2.5 D Dense clutter environment", *Proceedings of the 16th International Conference on Informatics in Control, Automation and Robotics, Prague, Czech Republic*, SCITEPRESS – Science and Technology Publications, Montreal, Canada, pp. 409–416.

Galceran, E. and Carreras, M. (2013), "A survey on coverage path planning for robotics", *Robotics and Autonomous Systems*, vol. 61, no. 12, pp. 1258–1276.

Katoch, S., Chauhan, S.S. and Kumar, V. (2021), "A review on genetic algorithm: past, present, and future", *Multimedia Tools and Applications*, vol. 80, no. 5, pp. 8091–8126.

Martinez-Alpiste, I., Golcarenarenji, G., Wang, Q. and Alcaraz-Calero, J.M. (2021), "Search and rescue operation using UAVs: A case study", *Expert Systems with Applications*, vol. 178, p. 114–937.

Maza, I. and Ollero, A. (2007), "Multiple UAV cooperative searching operation using polygon area decomposition and efficient coverage algorithms", *Distributed Autonomous Robotic Systems 6, Japan, Tokyo*, Springer, Cham, Switzerland, pp. 221–230.

Nazarahari, M., Khanmirza, E. and Doostie, S. (2019), "Multi-objective multi-robot path planning in continuous environment using an enhanced genetic algorithm", *Expert Systems with Applications*, vol. 115, pp. 106–120.

Park, S. and Choi, Y. (2020), "Applications of unmanned aerial vehicles in mining from exploration to reclamation: A review", *Minerals*, vol. 10, no. 8, p. 663.

Petrenko, V.I., Tebueva, F.B., Pavlov, A.S. and Gurchinskii, M.M., (2022), "Method for the allocations and scheduling of task execution by agents of swarm robotics systems under uncertainty", *Prikaspiiskii zhurnal: upravlenie i vysokie tekhnologii*, vol. 3 (59), pp. 25–43.

Pham, T.H., Bestaoui, Y. and Mammar, S. (2017), "Aerial robot coverage path planning approach with concave obstacles in precision agriculture", Education and Development of Unmanned Aerial Systems RED-UAS, Linkoping, Sweden, IEEE, New York, NY, USA, pp. 43–48.

Ren, H., Zhao, Y., Xiao, W. and Hu, Z. (2019), "A review of UAV monitoring in mining areas: current status and future perspectives", *International Journal of Coal Science & Technology*, vol. 6, no. 3, pp. 320–333.

Tuncer, A. and Yildirim, M. (2011), "Chromosome Coding Methods in Genetic Algorithm for Path Planning of Mobile Robots", *26*th International Symposium on Computer and Information Sciences, London, UK, Springer, Cham, Switzerland, pp. 377–383.

Информация об авторе

Рамиль Ф. Файзуллин, аспирант, Казанский (Приволжский) федеральный университет, Казань, Россия; 420008, Россия, Казань, ул. Кремлевская, д. 18; fzllnrml@gmail.com

Information about the author

Ramil F. Faizullin, postgraduate student, Kazan (Volga region) Federal University, Kazan, Russia; 18, Kremlevskaya Str., Kazan, 420008, Russia; fzllnrml@gmail.com

УДК 327:004.056(470)
DOI: 10.28995/2686-679X-2024-1-51-64

Обеспечение информационной безопасности России в рамках реализации Концепции внешней политики

Дмитрий Н. Баранников
Российский государственный гуманитарный университет, Москва, Россия, d.2006@mail.ru

Анастасия И. Мартынова
Российский государственный гуманитарный университет, Москва, Россия, anastasia.martynova2004@mail.ru

Аннотация. Статья посвящена анализу положений новой Концепции внешней политики РФ 2023 г. в контексте обеспечения информационной безопасности страны в современных условиях. В статье показано, как этот документ может конкретизировать отдельные положения Стратегии национальной безопасности Российской Федерации, в том числе в информационной сфере. Автор показывает, как рассматриваемая Концепция может позволить выстраивать в том числе перспективные международные взаимоотношения, обеспечивающие информационную безопасность России, опираясь на концептуальную основу. Уделяется внимание проблемам обеспечения национальной безопасности государства в рамках проведения процессов расширения взаимоотношений со странами, позитивно настроенными в отношении Российской Федерации, стиранию разграничительных линий, становлению долгосрочных отношений с учетом современных реалий. В статье подчеркивается и развивается положение о том, что приоритетным направлением для России является обеспечение глобальной безопасности, основанной на принципе уважения требований обеспечения национальной безопасности разных стран, в том числе в информационной сфере, а миссией Российской Федерации является поддержание глобального баланса сил. Автор анализирует применительно к вопросам обеспечения информационной безопасности РФ положение Концепции, касающееся того, что Россия не противопоставляет себя США и ее союзникам, но в то же время предусматривается возможность применения вооруженных сил в случае гипотетического нападения на Россию или ее союзников с целью сохранения сбалансированного и справедливого мира.

Ключевые слова: Концепция внешней политики РФ, национальная безопасность, информационная безопасность, внешнеполитический курс, информационный терроризм, гибридная война

Для цитирования: Баранников Д.Н., Мартынова А.И. Обеспечение информационной безопасности России в рамках реализации Концепции внешней политики // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 1. С. 51–64. DOI: 10.28995/2686-679X-2024-1-51-64

Ensuring the information security of Russia within the framework of the implementation of the Foreign Policy Concept

Dmitrii N. Barannikov
Russian State University for the Humanities, Moscow, Russia, d.2006@mail.ru

Anastasiya I. Martynova
Russian State University for the Humanities, Moscow, Russia, anastasia.martynova2004@mail.ru

Abstract. The article deals with the analysis of the provisions of the new Foreign Policy Concept of the Russian Federation in 2023 concerning ensuring the country's information security in modern conditions. The article shows how this document can specify certain provisions of the National Security Strategy of the Russian Federation, including in the information sphere. The author shows how the Concept under consideration can make it possible to build, among other things, promising international relations that ensure the information security of Russia, based on a conceptual framework. Attention is paid to the issues of ensuring the national security of the state in the framework of the processes of expanding relations with countries that are positively disposed towards the Russian Federation, erasing dividing lines, and establishing long-term relations, taking into account modern realities. The article emphasizes and develops the position that the priority for Russia is to ensure global security, based on the principle of respect for the requirements of ensuring the national security of different countries, including in the information sphere, and the mission of the Russian Federation is to maintain a global balance of power. The author analyzes, in relation to the issues of ensuring the information security of the Russian Federation, the provision of the Concept regarding the fact that Russia does not oppose itself to the United States and its allies, but at the same time it provides for the possibility of using armed forces in

the event of a hypothetical attack on Russia or its allies in order to maintain a balanced and just world.

Keywords: the concept of foreign policy of the Russian Federation, national security, information security, foreign policy course, information terrorism, hybrid war

For citation: Barannikov, D.N. and Martynova, A.I. (2024), "Ensuring the information security of Russia within the framework of the implementation of the Foreign Policy Concept", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 1. pp. 51–64, DOI: 10.28995/2686-679X-2024-1-51-64

Введение

Внешнеполитические межгосударственные взаимоотношения между Россией и странами, входящими в блок НАТО, осуществляют движение по синусоидальной кривой. И, к сожалению, в век, когда имеющиеся на вооружение средства нападения способны нанести непоправимый урон всей планете, движущий вектор направлен не на военно-политическое сдерживание. Группировки НАТО сплотили мощный альянс, осуществляют совершенствование военной инфраструктуры около границ с Российской Федерацией и поддерживают все больше и больше разгорающийся конфликт между странами, имеющими родственные связи (Россия – Украина).

Со стороны западной части государственной границы Российской Федерации усиливается военная инфраструктура альянса.

За последние два года выросли расходы на оборону у стран Североатлантического альянса, отмечается усиленная активность проведения странами НАТО военных учений различного уровня вблизи границ Российской Федерации. В приграничных странах усилена группировка альянса, переброшена тяжелая техника. К неблагоприятным факторам стоит отнести и тот факт, что страны, некогда соблюдавшие нейтральную позицию, в настоящее время меняют свою позицию и изъявляют желание стать участниками-партнерами стран НАТО. Формируются передовые командно-штабные подразделения, а также усиливается группировка в морской акватории вблизи границ РФ. Осуществляется финансовая и военно-техническая поддержка группировок, осуществляющих недружественные действия по отношению к Российской Федерации. Безосновательно военные корабли нечерноморских государств, входящих в блок НАТО, длительное

время пребывают в акватории Черного моря, осуществляют ведение различных видов разведки. В том числе увеличилось количество полетов самолетов как пилотируемых, так и беспилотных, имеющих на борту разведывательную аппаратуру. Беспилотная техника используется вооруженными силами стран, проводящих недружественную политику по отношению к Российской Федерации, для совершения террористических атак по объектам гражданской инфраструктуры. Интенсивность ведения всех видов разведки увеличилась в десятки раз, если сравнивать период до 2023 г. Самолеты, входящие в состав ВКС России, перехватываются и сопровождаются на всех участках полета, даже если осуществляются плановые учебно-тренировочные полеты в нейтральном воздушном пространстве [Митюшин 2022].

Методично реализуются планы по увеличению контингента размещения военнослужащих США на территории Польши. По данным СМИ, в Польше продолжается реконструкция инфраструктуры для размещения бронетанковой бригады США, завершается создание противоракетного комплекса «Иджис Эшор». Данные действия ставят под сомнение выполнение странами, входящими в блок НАТО, Основополагающего акта Россия–НАТО от 1997 г., который призывает обеспечивать военную стабильность в Европе.

Дипломатическое сообщество озабочено молчаливым согласием большинства государств, входящих в альянс и видящих, как происходит отказ от ключевых договоренностей по обеспечению военной сдержанности. На глазах у всего мира планомерно разрушается когда-то эффективно выстроенная и действовавшая архитектура европейской безопасности, а также нормы международного права. Несмотря на неоднократные попытки представителей дипломатического корпуса возобновить диалог для обсуждения взаимовыгодных вопросов по урегулированию активности в военной сфере, особенно касающихся территорий, непосредственно граничащих с Российской Федерацией, совершенствования механизма предотвращения опасной военной деятельности и инцидентов в воздушном пространстве и на море, положительных реакций со стороны стран НАТО не получено. Таким образом страны, входящие в блок НАТО, подчеркивают свое решение о замораживании плодотворного сотрудничества с Российской Федерацией. Отсутствие шагов во встречном направлении по поиску решений, удовлетворяющих принципам миропорядка, не способствует решению проблем, а приводит к дестабилизирующим последствиям. В связи с этим странам Запада необходимо взять курс на поддержание мира и стабильности, прекратить недружественные шаги навстречу Российской Федерации. В мире достаточно угроз, которые

требуют сплочения в их решении, например, по противодействию международному терроризму, распространению оружия массового уничтожения, наркоторговле, пиратству. Россия готова к диалогу. Однако не видно готовности со стороны альянса учитывать законные интересы России и развивать отношения на основе равноправия и всеобщей безопасности.

Международные отношения Россия строит в соответствии с нормами и принципами международного права, в рамках которого договоры, противоречащие Конституции РФ, не подлежат исполнению. Также регуляция внешнеполитических решений с недавнего времени определяется Концепцией внешней политики, утвержденной Указом Президента Российской Федерации от 31 марта 2023 г. № 229[1].

Целью данной статьи является анализ положений Концепции внешней политики РФ 2023 г. в контексте обеспечения информационной безопасности России в современных условиях.

Обеспечение информационной безопасности РФ в контексте приоритетов России в развитии международных отношений

Из текста Концепции внешней политики, утвержденной Указом Президента Российской Федерации от 31 марта 2023 г. № 229, следует, что этот документ призван конкретизировать отдельные положения Стратегии национальной безопасности Российской Федерации. Россия не противопоставляет себя странам, придерживающимся иных политических взглядов, не изолируется при решении спорных вопросов, а также несет миролюбивые и равноправные подходы, не остаются без внимания подходы урегулирования доминирующего влияния Соединенных Штатов в мире. Приоритетным направлением для России является обеспечение глобальной безопасности, основанной на принципе взаимности. Миссией Российской Федерации является поддержание глобального баланса сил, а внешняя политика страны «...носит миролюбивый, открытый, предсказуемый, последовательный, прагматичный характер». В отличие от американской Стратегии национальной безопасности, где США как выступали, так и продолжают высту-

[1] Концепция внешней политики Российской Федерации (утверждена Президентом Российской Федерации В.В. Путиным 31 марта 2023 г.) // Министерство иностранных дел Российской Федерации. URL: https://www.mid.ru/ru/detail-material-page/1860586/ (дата обращения 17.05.2023).

пать с позиций глобализации, политический подход Российской Федерации признает реалии многополярного мира, предполагает уважение к международным институтам и праву.

Подходы равноправия и взаимоуважения являются главным утверждением в Концепции: «Россия не считает себя врагом Запада». Из заявлений политических деятелей США также следует готовность «поддерживать и развивать прагматичные формы взаимодействия для решения вопросов, по которым сотрудничество с Россией может быть взаимовыгодным»[2]. Однако это заявление о готовности сотрудничества перечеркивается контекстуальным обликом России, созданным в документе Соединенных Штатов Америки. В контексте Стратегии национальной безопасности США (далее – СНБ США) Российская Федерация являет собой пример автократии, которая угрожает демократическим государствам. Ее агрессивные действия стали причиной продовольственного кризиса, роста цен на энергоносители и, как следствие, усугубили проблему бедности. Напрашиваются лишь вопросы: на каких условиях разработанные США модели прагматичного взаимодействия с РФ будут осуществляться? Не противоречит ли в целом российско-американское сотрудничество миссии США, согласно СНБ, – охране демократии в международном масштабе?

Стоит отметить, что хотя в СНБ США однокоренные слова и производные от «демократия» упоминаются 99 раз, США, придерживаясь своих традиций, спонсируют военные конфликты по всему миру[3]. В современных реалиях конфронтация приобретает черты гибридной войны нового типа с применением достижений в сфере технологий. Гибридные войны являются непосредственной угрозой для информационной безопасности государства. Таким образом, лишь за 2022 г. количество кибератак, направленных на госсектор, увеличилось до 80%[4].

---

[2] Biden-Harris Administration's National Security Strategy // The White House 12.10.2022. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/12/fact-sheet-the-biden-harris-administrations-national-security-strategy/ (дата обращения 17.05.2023).

[3] Полный перечень войн, вооруженных конфликтов, развязанных США за свою историю // Международная жизнь. URL: https://interaffairs.ru/news/show/35248 (дата обращения 12.05.2023).

[4] *Сыромолотов О.В.* Интервью заместителя Министра иностранных дел Российской Федерации О.В. Сыромолотова МИА «Россия сегодня», 28 декабря 2022 года // Министерство иностранных дел Российской Федерации 28.12.2022. URL: https://www.mid.ru/ru/foreign_policy/news/1845853/ (дата обращения 18.05.2023).

В частности следует отметить помощь иностранных коллег, к примеру со стороны Великобритании, украинским спецслужбам в сфере информационной безопасности: специальной структуре Сил специальных операций Украины – Центрам информационно-психологических операций (далее – ЦИПсО). Направлением деятельности ЦИПсО служила агитация, распространение заведомо ложной информации через каналы массовой информации, социальные сети: как пример действий на территории Украины следует привести пример из Доктрины информационной безопасности Украины, утвержденной еще в 2016 году, где одним из приоритетов государственной политики в сфере информационной безопасности было «обеспечение полного покрытия территории Украины цифровым вещанием, прежде всего пограничных и временно оккупированных территорий»[5]. Также с ЦИПсО связаны хакерские атаки на закрытые информационные ресурсы, распространение ложной информации о готовящихся терактах[6]. Действия ЦИПсО гражданское население могло ощутить еще в 2020 г. во время массовых звонков, то есть телефонного терроризма[7].

Последняя активность со стороны коллективного Запада и Украины несет прямую угрозу безопасности жизни и здоровья граждан РФ.

Вопрос эффективности переговоров по той или иной проблеме при участии международных организаций являет собой отдельный блок для исследований специалистов по международным отношениям и праву, но недавние заявления официальных лиц западных стран ставят под сомнение ответ на него в пользу РФ. Одним из последних и ярких стало высказывание министра обороны Германии Бориса Писториуса, который увидел необходимость ударов ВСУ по гражданскому населению России: «До тех пор пока не проводятся нападения на города, гражданских и гражданские районы, это приходится принимать как необходимость.

---

[5] Обзор законодательства Украины в сфере информационной безопасности // Digital.Report. URL: https://digital.report/zakonodatelstvo-ukrainyi-informatsionnaya-bezopasnost/ (дата обращения 12.05.2023).

[6] *Рябов К.* Центры информационно-психологических операций ССО Украины. Разгром близок // Военное обозрение 03.03.2022. URL: https://topwar.ru/192979-centry-informacionno-psihologicheskih-operacij-sso-ukrainy-razgrom-blizok.html (дата обращения 12.05.2023).

[7] *Лазаренко Н.* Инфодиверсанты. Как действовал Центр инфопсихологических операций ВСУ // РИА Новости 13.05.2022. URL: https://ria.ru/20220513/tsipso-1788372942.html (дата обращения 14.05.2023).

Не то чтобы с удовольствием, но, к примеру, для отрезания путей снабжения»[8].

Официальный представитель МИД РФ Мария Захарова неоднократно высказывалась о недопустимости поддержки террористической активности. Было озвучено обращение в Совет безопасности ООН: «Мы будем привлекать внимание Совбеза в ходе официальных заседаний, консультаций Совета безопасности к террористической активности киевского режима на постоянной основе»[9]. Данное заявление являет собой очередной пример линии внешней политики против классификации России как врага мировой стабильности в СНБ США 2022 года.

По сегодняшний день преградой для успешного сотрудничества является конфронтационная политика США, осознание бесперспективности которой может стать началом прагматичных контактов с Россией[10].

В условиях нарастания угрозы международного информационного терроризма, которому коллективный Запад не только не желает противостоять, но и в открытую спонсирует его, также осуществляются мероприятия по милитаризации. Генеральный секретарь НАТО делает открытые заявления о необходимости крупных инвестиций в вооруженные силы, что позволит результативно конкурировать в условиях вооруженного противоборства. Йенс Столберг не скрывает и того, что наравне с политическими и экономическими подходами для регулирования обстановки не исключается и силовой характер достижения приоритетных целей альянса. И как показывает практика, военная сила является первостепенной частью в решении вопросов. Россия же в этих непростых условиях сталкивается с острой потребностью в обеспечении безопасности, защите государственного информационного суверенитета. Попытки призвать международную общественность

---

[8] *Нармания Д.* Украине разрешили бить вглубь России // РИА Новости. 23.04.2023. URL: https://ria.ru/20230423/razreshenie-1867094922.html?in=t (дата обращения 12.05.2023).

[9] МИД: Россия будет обращать внимание ООН на террористические атаки Украины // РИА Новости. 10.05.2023. URL: https://ria.ru/20230510/aktivnost-1870867837.html (дата обращения 12.05.2023).

[10] *Лавров С.В.* Выступление Министра иностранных дел Российской Федерации С.В. Лаврова на Совещании с постоянными членами Совета Безопасности Российской Федерации, Москва, 31 марта 2023 года // Министерство иностранных дел Российской Федерации 31.03.2023. URL: https://www.mid.ru/ru/foreign_policy/news/1861005/ (дата обращения 19.05.2023).

бороться совместно с данной проблемой не находят поддержки со стороны ЕС, англосаксонских стран, которые игнорируют в ущерб себе значимость России как постоянного члена ведущих международных организаций.

Внешнеполитический курс Российской Федерации направлен на открытость и уважение общепризнанных норм и правил, равноправное международное сотрудничество и миролюбивость. Поэтому Российской Федерации пока остается, опираясь на основополагающие документы, создавать систему, позволяющую выстраивать отношения с перспективой долгосрочного развития внешней политики, и оказывать содействие в сохранении баланса сил многополярной международной системы[11].

Учитывая то, что взгляды стран Запада и России на внешнеполитический курс неоднозначны, тем не менее Российская Федерация направила вектор усилий принимаемых мер на повышение объективности, укрепление позитивного имиджа в мире, а также перевод международных отношений в плоскость доверия. Ко всем странам Россия не настроена враждебно, не изолирует себя на международной арене и не собирается себя противопоставлять странам Запада, демонстрируя враждебные намерения.

Но шаги, предпринимаемые странами под руководством США, заставили осуществить переоценку внешнеполитических подходов.

Специальная военная операция по «демилитаризации и денацификации территории Украины» направлена на решение задач по созданию нейтрального статуса территории Украины без ударных комплексов НАТО, имеющих целью удара объекты России, а также признанию территории Крыма российской принадлежностью. Сложившиеся условия, усугубившиеся санкционным давлением, создали благоприятную почву для утверждения Президентом Российской Федерации Концепции внешней политики[12].

В сложившихся реалиях международных отношений в концепции дается понятие «великая держава», подчеркивающее имеющиеся ресурсы, которые способны оказывать влияние во всех сферах жизнедеятельности. Россия является участником в ведущих межгосударственных организациях и представляет собой крупнейшую

---

[11] *Мездриков Е.* Россия представила новую концепцию внешней политики // Ведомости. 31.03.2023. URL: https://www.vedomosti.ru/politics/articles/2023/03/31/969022-rossiya-predstavila-kontseptsiyu-vneshnei-politiki?ysclid=lm1pd6rzha380644804 (дата обращения 12.05.2023).

[12] *Жильцов С.* Россия расставила приоритеты во внешней политике // Международная жизнь. 03.04.2023. URL: https://interaffairs.ru/news/show/39727 (дата обращения 19.05.2023).

ядерную державу, обеспечивающую глобальный баланс сил в многополярном мире.

Принятая концепция позволяет без оглядки на кого-либо выражать свое мнение о разногласиях в политических взглядах, выстраивать отношения как нейтральные, так и конструктивные, но что еще важно – адекватно реагировать на различные недружественные позиции в отношении России. С учетом отношения стран будут формироваться новые сферы военных действий, а также внешнеполитического реагирования. Впервые изменение политических реалий допускает использование Вооруженных сил Российской Федерации в качестве убедительного довода, для предупреждения и предотвращения агрессивных действий в отношении Российской Федерации или ее союзников, разрешения кризисов, сохранения и стабилизации мира на основании решений СБ ООН, организаций коллективной безопасности, обеспечения безопасности своих граждан и, конечно, предотвращения действий международных террористических организаций.

Национальному интересу также придается значительное место в стратегическом планировании. Данная форма стратегического планирования будет являться начальным рубежом при постановке задач[13].

Преобразуется политическое устройство широкомасштабных приоритетов. Например, подчеркивается актуальная область, относящаяся к обеспечению национальных ориентиров Российской Федерации в актуальных областях, к которым принадлежат космическое, морское и воздушное пространства. Расширяются возможности защиты законных интересов и прав граждан России в развитии международных отношений. Теперь странам, которые осмеливаются осуществлять «русофобские» высказывания, будет оказываться противодействие.

В Концепции внешней политики Российской Федерации 2023 г. трансформируются региональные границы. С 2023 г. вводятся в обращение понятия, не использовавшиеся ранее, такие как «Исламский мир» и «Евразийский континент». Данные понятия могут употребляться как самостоятельные территориальные ориентиры внешней политики России. Уделяется немало внимания и разви-

[13] *Лебедева О., Бобров А.* Концепция внешней политики России 2023: стратегия многополярного мира // Российский Совет по международным делам. 2 мая 2023 г. URL: https://russiancouncil.ru/analytics-and-comments/analytics/kontseptsiya-vneshney-politiki-rossii-2023-strategiya-mnogopolyarnogo-mira/?ysclid=lm1pcbvo3i120013227 (дата обращения 10.05.2023).

тию Арктики. Несмотря на существующую конфликтогенность этого региона, создаются условия для развития Северного морского пути, а также по недопущению милитаризации Арктического региона [Жильцов 2023].

Но не только Арктике уделяется внимание, в числе приоритетных регионов находится и Антарктика. Как и в Арктическом регионе, приоритетным направлением для России является недопущение милитаризации, а также вопросы экологической безопасности. В данном вопросе большая роль отводится взаимодействию со странами АТР, Африки, Латинской Америки и т. д.

Африканские государства впервые носят ярко выраженный приоритет внешний политики. В укреплении многосторонних отношений принимают участие ряд структур, с которыми развивается взаимодействие по различным направлениям.

Форматом двусторонних международных отношений являются развивающиеся направления внешний политики взаимодействия со странами Латинской Америки и Карибского бассейна. Подчеркивается содействие латиноамериканским государствам, испытывающим диктатуру США, и их союзникам в поддержке суверенитета и независимости.

В то же время Россия не отвергает отношения с европейскими государствами, Соединенными Штатами Америки, а также Канадой, Австралией и Новой Зеландией. Эти отношения находятся в непосредственной зависимости от предпринимаемых данными странами шагов по отношению к России. Позиция России развивается в направлении недопущения нарушения международных договоров, создания условий для взаимовыгодного сотрудничества, исключения проявления агрессивной политики и роста угроз национальным интересам. Также Россия не поддерживает позицию получения односторонних экономических преимуществ реализацией недружелюбной политики [Подберезкин 2023].

Заключение

Политические взгляды государственных лидеров в мире и политическое влияние очень многообразны: кто-то придерживается демократических идеалов, обеспечивая рациональную международную атмосферу «демократической солидарности», кто-то акцентирует внимание на выходе из кризисного состояния, кто-то меняет статус развивающейся страны на экономически независимую и заявляет о своем присутствии на мировой политической арене, а кто-то продолжает свое притязание на роль мирового

политического лидера, промышленной и финансовой державы мира. Процесс глобализации необратим, а технические прорывы в различных областях значительно сокращают трансграничные коммуникации, упрощая обмен научно-техническими достижениями.

На примере Соединенных штатов Америки хорошо виден процесс приобретения статуса великой державы, начинающийся с завоевания военной мощи и переходящий к формированию международной системы, оказывающей влияние на межгосударственные отношения. Наличие ресурсов, влияющих на решение национальных интересов, позволяет обеспечивать научно-технический потенциал, стабильность политической структуры и географической целостности.

Попытки США по реализации монополярного мира претерпевают очередной крах. Несмотря на то, что после принятия в Союзе Советских Социалистических Республик решений, отрицательно сказавшихся на военном потенциале, официально США являются наиболее могущественной сверхдержавой, выкроить мировой порядок по своим шаблонам у них не получается.

Возврат к позиции многополярности мирового влияния возродился благодаря усилиям российских политиков. Благодаря поддержке Российской Федерации Китай и Индия заняли свои геополитические полюсы. Китай по торговым показателям приближается к Соединенным Штатам и имеет внушительный золотовалютный резерв. Несмотря на развивающееся многостороннее взаимодействие, многие вопросы требуют взвешенного и более сдержанного решения политических трений, особенно касающихся территориальных споров, так как существует экономическая взаимозависимость стран с высокоразвитым индустриальным сектором. Однако США, гордясь достаточной экономической состоятельностью, демократическими принципами, активно занимаются приумножением своих преимуществ, увеличивая результативность экономического и политического секторов и часто пренебрегая интересами других стран. Такой подход вносит дисбаланс в мировой порядок, нарушая права слаборазвитых стран.

С целью обеспечения безопасности на основе принципа взаимности для всех стран президент Российской Федерации утвердил своим Указом от 31 марта 2023 г. № 229 Концепцию внешней политики Российской Федерации.

Одним из ключевых аспектов этого документа является обеспечение информационной безопасности России в сфере внешней политики, которая определяется безопасностью трех субъектов информационного пространства: государства, общества и личности. Рассмотренные положения концепции позволяют выявить

и оценить основные принципы и проблемы обеспечения информационной безопасности перечисленных субъектов.

При этом наиболее актуальными проблемами и направлениями для проведения научных исследований в области обеспечения информационной безопасности при реализации внешней политики России являются:

- анализ долгосрочных тенденций в сфере внешней политики, влияющих на состояние информационной безопасности личности, общества и государства;
- исследование подходов к укреплению международной безопасности и стабильности;
- анализ принципов и методов создания информационного пространства, безопасного для государства в целом, общественных структур и граждан;
- изучение направлений содействия развитию российской экономики в сфере современных информационных технологий и др.

Инновационная направленность Концепции внешней политики не умаляет сложности толкования разработанного документа. Вследствие нормативно-правовой направленности отдельные положения являются руководством к реализации для государственных органов и подведомственных организаций на ближайшую и дальнейшую перспективы. Это касается и положений Концепции, связанных с обеспечением информационной безопасности РФ. В частности, ее положения уже нашли выражение в Федеральном законе от 04.08.2023 № 432-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации», который определяет новые положения законодательства в области защиты сведений, составляющих государственную тайну и других документах.

Веяния современного мира диктуют задачи, которые необходимо решать быстро, четко и своевременно. Одной из задач принятой Концепции внешней политики Российской Федерации является обеспечение информационной безопасности как во внутренних делах РФ, так и во взаимоотношениях с мировым сообществом. Это задача не выживать в глобальном беспорядке, а выстраивать четкую концепцию при расстановке приоритетов.

Литература

Жильцов 2023 – *Жильцов С.С.* Арктика в Концепции внешней политики России 2023 года: основные направления и вызовы // Вестник Дипломатической академии МИД России. Россия и мир. 2023. № 3 (37). С. 6–19.

Митюшин 2022 – *Митюшин Д.А.* Использование беспилотных летательных аппаратов в ОРМ «Наблюдение»: модель угроз безопасности информации // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2022. № 3. С. 43–65.

Подберезкин 2023 – *Подберезкин А.И.* Субъективные аспекты новой Концепции внешней политики России // Обозреватель. 2023. № 4 (399). С. 5–25.

References

Mityushin, D.A. (2022), "The use of unmanned aerial vehicles in the OSM "Surveillance". Model of threats for the information security", *RSUH/RGGU Bulletin. "Informatics. Information security. Mathematics" Series*, no. 3, pp. 43–65.

Podberezkin, A.I. (2023), "Subjective aspects of the new Concept of Russian foreign policy", *Observer*, no. 4 (399), pp. 5–25.

Zhiltsov, S.S. (2023), "The Arctic in the Concept of Russian Foreign Policy 2023. Key trends and challenges", *Bulletin of the Diplomatic Academy of the Russian Foreign Ministry. Russia and the world*, no. 3 (37), pp. 6–19.

Информация об авторах

Дмитрий Н. Баранников, кандидат военных наук, доцент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; d.2006@mail.ru.

Анастасия И. Мартынова, студент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; anastasia.martynova2004@mail.ru.

Information about the authors

Dmitrii N. Barannikov, Cand. Of Sci. (Military Science), associate professor, Russian State University for the Humanities, Moscow, Russia; 6, Miusskaya Sq., Moscow, 125047, Russia; d.2006@mail.ru.

Anastasiya I. Martynova, student, Russian State University for the Humanities, Moscow, Russia; 6, Miusskaya Sq., Moscow, 125047, Russia; anastasia.martynova2004@mail.ru.

УДК 004.056:347.157(470)
DOI: 10.28995/2686-679X-2024-1-65-79

Современные подходы к обеспечению информационной безопасности детей

Дмитрий Н. Баранников
Российский государственный гуманитарный университет, Москва, Россия, d.2006@mail.ru

Ирина А. Русецкая
Российский государственный гуманитарный университет, Москва, Россия, irkom@mail.ru

Аннотация. В статье проводится анализ современных подходов к обеспечению информационной безопасности детей в Российской Федерации. Работа включает краткий обзор нормативно-правовых источников, определяющих приоритеты и направления государственной политики в рассматриваемой области, в частности, таких как Федеральный закон «Об информации, информационных технологиях и о защите информации» и Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию». Особое внимание уделяется изучению положений Концепции информационной безопасности детей в Российской Федерации, утвержденной Распоряжением Правительства Российской Федерации от 28 апреля 2023 г. № 1105-р. В статье проводится изучение причин повышенной уязвимости несовершеннолетних к деструктивным информационным воздействиям. Внимание уделяется также анализу информационных угроз для детей в Интернете. Обозначаются подходы к регулированию рынка информационной продукции, предназначенной для детей. Определяются субъекты, влияющие на информационную безопасность несовершеннолетних, а также риски, управление которыми влияет на состояние информационной безопасности детей. Рассматриваются отдельные общественные мероприятия и проекты, способствующие формированию культуры информационной безопасности детей, находящиеся в стадии реализации. Особое внимание уделяется анализу мер, способствующих совершенствованию системы обеспечения информационной безопасности детей на уровне государства, общества и представителей отдельных социальных групп.

Ключевые слова: информационная безопасность, защита детей, Концепция информационной безопасности детей, кибербезопасность, негативное информационное воздействие

Для цитирования: Баранников Д.Н., Русецкая И.А. Современные подходы к обеспечению информационной безопасности детей // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 1. С. 65–79. DOI: 10.28995/2686-679X-2024-1-65-79

Modern approaches to ensuring children's information security

Dmitrii N. Barannikov
Russian State University for the Humanities, Moscow, Russia, d.2006@mail.ru

Irina A. Rusetskaya
Russian State University for the Humanities, Moscow, Russia, irkom@mail.ru

Abstract. The article analyzes modern approaches to ensuring the information security of children in the Russian Federation. The work includes a brief overview of regulatory sources that determine the priorities and directions of state policy in the area under consideration, in particular, such as the Federal Law "On Information, Information Technologies and Information Protection" and the Federal Law "On the Protection of Children from Information Harmful to Their Health and Development". Particular attention is paid to studying the provisions of the Concept of Information Security of Children in the Russian Federation, approved by Order of the Government of the Russian Federation of April 28, 2023 No. 1105-r. The article studies the reasons for the increased vulnerability of minors to destructive information influences. Attention is also paid to the analysis of information threats to children on the Internet. Approaches to regulating the market of information products intended for children are outlined. It identifies subjects influencing the information security of minors as well as the risks, the management of which affects the state of information security of children. Individual public events and projects that are currently under implementation to promote the formation of a culture of information security for children are considered. Particular attention is paid to the analysis of measures that contribute to improving the system of ensuring information security for children at the level of the state, society and representatives of individual social groups.

Keywords: information security, child protection, Children's information security concept, cybersecurity, negative information impact

For citation: Barannikov, D.N. and Rusetskaya, I.A. (2024), "Modern approaches to ensuring children's information security", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 1. pp. 65–79, DOI: 10.28995/2686-679X-2024-1-65-79

Введение

Понятие информационной безопасности включает в себя совокупность трех составляющих:

- предоставление субъектам информационных отношений информации, соответствующей требованиям к информационным ресурсам, необходимым для принятия управленческих решений;
- защиту информации;
- защиту от деструктивного воздействия информации, не являющейся нейтральной, то есть, имеющей целью получения какого-либо нежелательного для субъекта, к которому она обращена, результата.

Традиционно специалисты по информационной безопасности занимаются решением задач, связанных с первыми двумя направлениями. Однако третья из названных составляющих информационной безопасности является не менее важной и актуальной, чем первые две. Особенное значение она имеет применительно к защите детей от деструктивного информационного воздействия. Это связано как с тем, что важность физического, эмоционального и духовного развития детей сложно переоценить, так и с тем, что дети являются одной из наиболее уязвимых социальных категорий с точки зрения влияния на них информации.

Целью данной статьи является анализ современных подходов к обеспечению информационной безопасности несовершеннолетних в Российской Федерации, а также акцентирование внимания на эффективном решении вопросов при совершенствовании информационной безопасности детей.

Реализация этой цели предполагает решение авторами следующих задач:

- анализ принципов и подходов государственной политики в области обеспечения информационной безопасности детей;
- изучение нормативно-правовых документов, отражающих требования к обеспечению информационной безопасности детей;
- анализ положений Концепции информационной безопасности детей 2023 г.;
- изучение отдельных организационных мероприятий и проектов, которые ведут к созданию культуры информационной безопасности общества;
- определение организационных мер, которые ведут к совершенствованию системы обеспечения информационной безопасности детей на уровне трех субъектов информационного пространства: государства, общества и его отдельных представителей.

Анализ современных подходов к обеспечению информационной безопасности детей в Российской Федерации

Как международные, так и российские нормы права предоставляют ребенку возможность получения информации, способствующей его физическому, ментальному, психическому, социальному, духовному развитию, что зафиксировано, например, в статьях 13–17 Конвенции ООН о правах ребенка. В этом документе также отмечено, что право на получение информации является частью права свободного выражения своего мнения, предполагающего поиск и получение информации в любых источниках для его формирования.

При этом несомненно, что необходимо обеспечение информационной безопасности несовершеннолетних. Указом Президента Российской Федерации от 29 мая 2017 г. № 2402 2018–2027 гг. в Российской Федерации объявлены Десятилетием детства. Тем самым государство признает важность правильного воспитания подрастающего поколения и необходимость участия в этом всех субъектов информационных отношений: государства, общества и отдельных граждан.

Проблема сочетания здорового физического и интеллектуального развития детей и парадигмы свободного доступа информации лежит в основе подходов к государственному управлению информационной безопасностью детей [Полянина 2021]. В основу государственной политики в этой сфере должны быть положены два принципа: предоставления детям информации, способствующей здоровому развитию, и ограничение доступа к информации, имеющей деструктивное содержание [Гришина, Мецатунян, Русецкая 2012].

Для защиты информационной безопасности детей предполагаются ограничения на распространение информации, которая может оказывать на них негативное и дестабилизирующее воздействие. Органами государственной власти Российской Федерации реализуется планомерная деятельность по обеспечению информационной безопасности детей, которая имеет нормативно-правовую основу.

Так, Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ определил основные законодательные положения, определяющих подходы к защите детей от негативного информационного воздей-

ствия[1]. Данный закон определяет нормы государственного регулирования в области использования информационных технологий с учетом обеспечения информационной безопасности детской аудитории.

В законе указываются обязанности производителей, распространителей и владельцев аудиовизуальных сервисов по классификации аудиовизуальных произведений, предназначенных для различных возрастных категорий до начала их распространения, а также требования по обозначению категории этих информационных продуктов соответствующим знаком и (или) текстовым предупреждением. Эти меры направлены на ограничение распространения среди детей информации, которая может оказывать дестабилизирующее влияние на них [Наумова, Баранников, Митюшин 2020].

В законе также рассматриваются особенности распространения информации в сети Интернет, в том числе на сайтах, в социальных сетях и в различных информационных системах, на владельцев которых возлагаются требования по обеспечению защиты детской аудитории от негативного информационного воздействия.

В качестве одной из мер обеспечения информационной безопасности, рассматриваемый закон предполагает создание единой автоматизированной информационной системы, получившей название «Единый реестр доменных имен, указателей страниц сайтов в сети “Интернет” и сетевых адресов, позволяющих идентифицировать сайты в сети “Интернет”, содержащие информацию, распространение которой в Российской Федерации запрещено», и в том числе фиксация сведений о распространении информации, наносящей урон здоровью и развитию детей.

Важнейшим законодательным актом, обеспечивающим нормативное регулирование рассматриваемой сферы и целиком посвященным ей, является Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 г. № 436-ФЗ[2].

В законе рассматриваются категории информации, которая может причинять вред детям, классификация информационных

---

[1] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=453479&dst=100001#TH3TBsTnX1JfuGO2

[2] Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 г. № 436-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=446169&dst=100001#VkHWBsT04igwvyYI (дата обращения 17.05.2023).

продуктов, предназначенных для детей различных возрастных категорий и требования к ней, а также особенности распространения этих продуктов в Интернете. Закон также определяет основные элементы и этапы проведения экспертизы информационных продуктов, предназначенных для детей, и регламентирует вопросы составления экспертных заключений. Данный закон устанавливает принципы государственного и общественного контроля за соблюдением действующих правовых норм в рассматриваемой сфере, а также ответственность за их нарушение.

В 2015 г. распоряжением Правительства РФ была утверждена первая в России Концепция информационной безопасности детей, определяющая основные концептуальные подходы к обеспечению защиты детей от негативных информационных воздействий. Целью ее принятия стала реализация единой политики государства по созданию информационного пространства, безопасного для детей и учитывающего риски распространения информационных технологий в современном мире[3]. Инициатором создания этого документа стал Роскомнадзор, по приглашению которого ученые и преподаватели нескольких десятков российских вузов создали масштабный проект по научному изучению принятых в международной практике подходов к обеспечению информационной безопасности детей. Результатом этой работы стал краткая Концепция информационной безопасности детей[4].

В апреле 2023 года опубликована новая Концепция информационной безопасности детей (утверждена распоряжением Правительства РФ от 28.04.2023 № 1105-р), в которой значительно расширены и уточнены приоритеты, цели и задачи политики государственного регулирования в рассматриваемой сфере. Проанализируем основные элементы новой Концепции[5].

---

[3] Концепция информационной безопасности детей, утвержденная распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р. URL: http://static.government.ru/media/files/mPbAMyJ29uSPhL3p20168GA6hv3CtBxD.pdf (дата обращения 17.05.2023).

[4] *Фирсов С.* IT-эксперт о концепции информационной безопасности детей: «Нужно передавать опыт подрастающему поколению» 5 мая 2023 // ФедералПресс. URL: https://fedpress.ru/expert-opinion/3240060 (дата обращения 17.05.2023).

[5] Концепция информационной безопасности детей в Российской Федерации, утвержденная распоряжением Правительства Российской Федерации от 28 апреля 2023 г. № 1105-р. URL: http://static.government.ru/media/files/0vjjsdBmSsIdUZ4c8Z2eOAiGkCbCf7OJ.pdf (дата обращения 17.05.2023).

На момент составления Концепции дети составляли более 20% населения Российской Федерации, а почти 90% из этого числа являлись активными пользователями Интернета и современных информационно-коммуникационных технологий. Эта категория населения является и наиболее уязвимой с точки зрения информационной безопасности, что может приводить к потенциальным или реальным угрозам мошенничества, манипулирования, вымогательства, шантажа, вовлечения в противоправную деятельность, нарушения здоровья и психики несовершеннолетних и т. п. В качестве причин повышенной уязвимости этой категории населения к деструктивным информационным воздействиям можно назвать: недостаточную в силу возраста развитость критического мышления эмоциональную нестабильность, незнание принципов и правил обеспечения личной информационной безопасности, желание соответствовать моде на социальную самопрезентацию без учета требований безопасности.

При этом данные программы криминологического наблюдения, в рамках которой в онлайн-формате проанкетировано около 45 тыс. детей в возрасте от 12 до 18 лет в трех субъектах РФ, показывают, что у подростков с возрастом в два раза увеличивается число тех, кто проводит в Интернете более пяти часов в день. То есть, если в 12–13 лет их было 16% от общего числа прошедших анкетирование, то к 16–18 годам их количество выросло до 32%. Примерно две трети анкетируемых указали, что они проводят 1–4 часа в день в Telegram (78,5%), WhatsApp (62,4%), Viber (43%), Вконтакте (87%), YouTube (80%), Одноклассники (11%), TikTok (63%), Instagram (27%).

Это же исследование показывает, что 76% опрошенных, по их словам, не пользуются информационными ресурсами, которые считают вредными для их жизни и здоровья. Только 18% из их числа постоянно используют фильтрующие контент настройки. При этом 1,6% анкетированных отметили, что постоянно посещают запрещенные сайты и им это нравится, а 2,7% делают это редко, когда считают нужным найти необходимую им информацию [Нынюк 2023].

Новая Концепция информационной безопасности детей выделяет меры, которые призваны способствовать повышению эффективности подходов к обеспечению информационной безопасности несовершеннолетних и которые должны быть объединены в единый комплекс мероприятий, в совокупности обеспечивающий поставленные цели:

– меры правового государственного регулирования рассматриваемой сферы;
– обеспечение взаимодействия государственных и общественных усилий с родительским сообществом с учетом того, что

родители и семья имеют определяющие приоритетные права и обязанности в вопросах информационной безопасности несовершеннолетних;
– привлечение различных организаций-участников медиарынка для мониторинга Интернета в целях выявления деструктивной информации, распространение которой может нанести вред несовершеннолетним;
– информирование широких слоев населения о существующих угрозах информационной безопасности детей и мерах их пресечения;
– проведение федеральных и региональных мероприятий, целью которых ставится защита несовершеннолетних от информационных угроз;
– производство информационных продуктов, рассчитанных на детей, и контроль за информационной продукцией;
– обучение детей правилам безопасности в информационном пространстве;
– обучение детей навыкам критического и самостоятельного мышления и развитие их творческого, образовательного, исследовательского и духовного потенциала для самореализации в цифровой среде;
– внедрение в образовательных организациях основного и дополнительного образования и других детских учреждениях, в том числе библиотеках, современных технических и программно-аппаратных мер обеспечения информационной безопасности детей.

Предваряющий создание Концепции анализ моделей построения комплексной системы обеспечения информационной безопасности несовершеннолетних в различных государствах показал, что можно выделить три возможных варианта регулирования рынка информационной продукции:
– государственное регулирование;
– саморегулирование силами участников медиасообщества;
– регулирование путем объединения усилий государства и медиа.

Именно последний, третий подход положен в основу Концепции и отвечает принципам государственной политики в сфере защиты детей от негативного воздействия информации.

В качестве обучающих информационной безопасности мер Концепция рекомендует проведение анализа образовательных программ и программ дополнительного образования и интеграцию в них курсов, посвященных кибербезопасности, а также регулярное проведение мероприятий различной направленности по обучению алгоритмам безопасного поведения в цифровой среде.

Концепция также вводит перечень из количественных и качественных критериев, позволяющих проводить оценку состояния информационной безопасности несовершеннолетних. К первой категории критериев можно отнести оценку количества:

- субъектов РФ, на территории которых проводятся просветительские и иные мероприятия, обеспечивающие формирование безопасной для детства информационной среды;
- детей, педагогических работников и родителей, принявших участие в таких мероприятиях или обучении по вопросам защиты информации;
- созданных для детей безопасных интернет-ресурсов;
- специализированных детских СМИ и созданных ими печатных и электронных ресурсов для несовершеннолетних;
- обнаруженных и пресеченных фактах вовлечения детей через социальные сети в противоправные или наносящие им вред действия.

К качественным критериям оценки относится достаточность федеральных и региональных мероприятий по обеспечению защиты детей от деструктивного воздействия информации, а также по производству информационных продуктов для детей и юношества.

Таким образом, новая Концепция закладывает фундамент государственной политики в области обеспечения информационной безопасности подрастающего поколения, предполагающий внедрение разноплановых норм и организационных мероприятий.

Как было указано выше, помимо определения нормативно-правовых требований к обеспечению информационной безопасности детей органы государственной власти организуют различные инициативы, рассчитанные на широкую общественность, которые способствуют формированию культуры информационной безопасности населения.

Так, Минцифры при поддержке организаций-партнеров претворяет в жизнь всероссийскую программу «Кибергигиена», задачами которой являются повышение информированности общества в сфере информационной безопасности частной жизни и формирование у широких слоев российского населения культуры грамотного и безопасного поведения в киберпространстве[6]. Дети могут считаться одной из ключевых категорий населения, на которую ориентирован этот проект, поскольку они являются наиболее активными и заинтересованными потребителями интернет-контента

[6] Сайт проекта «Кибергигиена». URL: https://kiber-bez.ru/about/# (дата обращения 17.05.2023).

и пользователями социальных сетей и при этом уязвимыми с точки зрения информационной безопасности. Реализация мероприятий данного проекта рассчитана на три года и проводится в рамках Федерального проекта «Информационная безопасность» Национальной программы «Цифровая экономика».

Программа «Кибергигиена» включает в себя ряд независимых проектов, направленных на просветительскую деятельность в сфере обучения граждан правилам обеспечения информационной безопасности личности. К ним относятся проекты:

- «КиберЗОЖ», предполагающий обучение основным правилам поведения в информационном пространстве;
- «Сложные несложные пароли», который призван обучать навыкам идентификации и аутентификации пользователей в Сети;
- «Выучи свою роль», обучающий правильному реагированию на звонки мошенников;
- «Кибербуллинг», позволяющий детям и подросткам противостоять оскорблениям, угрозам и травле в киберпространстве;
- «Прокачай скилл защиты», разработанный для геймеров и направленный на противостояние хакерским атакам на игровые аккаунты;
- «Подготовка к известности», нацеленный на помощь детям, ведущим свои блоги, и в доходчивой форме объясняющий правила защиты и поведения в соцсетях.

Проект «Кибергигиена» включает в себя различные формы проведения мониторинга уровня грамотности российского населения в сфере кибербезопасности, одной из целей которого является ранжирование угроз информационной безопасности для различных групп граждан. По результатам такого мониторинга предполагается разработка образовательных проектов, в рамках которых, в том числе с использованием средств геймификации, в обществе будет формироваться культура информационной безопасности, а также распространяться информация о методах противостояния актуальным угрозам в информационном пространстве[7].

Основные угрозы, с которыми дети могут сталкиваться в Интернете, могут быть разделены на угрозы физическому, мате-

[7] *Бенгин В.Н.* Минцифры повышает киберграмотность россиян 1 августа 2022. URL: https://digital.gov.ru/ru/events/41771/?utm_referrer=https%3a%2f%2fd-russia.ru%2f&utm_referrer=https%3a%2f%2fdigital.gov.ru%2fru%2fevents%2f41771%2f%3futm_referrer%3dhttps%253a%252f%252fd-russia.ru%252f (дата обращения 17.05.2023).

риальному и духовному состоянию и развитию ребенка. Первые включают в себя угрозы здоровью и жизни, вторые связаны с возможным хищением денег, материальных ресурсов вследствие мошеннических схем или заражения компьютеров и смартфонов вредоносным программным обеспечением, а последняя категория угроз связана с опасностями деструктивного влияния на духовное и нравственное развитие детей, включая киберзависимость, игроманию, вовлечение в опасные и противоправные действия и пр. [Кундышева, Русецкая 2018].

Для реализации требований обеспечения информационной безопасности, как было указано выше, необходима реализация комплекса мер по взаимодействию государства, педагогов и родителей несовершеннолетних.

Так, родителям в этой связи рекомендуется:

– объяснять ребенку правила безопасности в цифровой среде;
– ограничить или исключить неконтролируемый поиск информации и доступ к информационным ресурсам, которые могут содержать нежелательную информацию;
– устанавливать прокси-серверы, DNS и программы для блокировки нежелательного контента, в том числе рекламного характера.

Педагогическим работникам, в свою очередь, следует:

– обращать внимание детей и родителей на вопросы информационной безопасности;
– отражать информацию о необходимости обеспечения мер безопасности на сайте образовательной организации и в соцсетях;
– использовать технические и программные средства для защиты от негативного воздействия информации и фильтрации содержания сайтов на компьютерах образовательного учреждения [Контылева 2023].

При этом в федеральных государственных образовательных стандартах заложены положения, касающиеся развития у детей навыков работы с информацией и ее оценивания. Так, согласно ФГОС НОО 2021 г., уже выпускники начальных классов должны овладеть первичными навыками работы с информацией, уметь ее искать, преобразовывать и применять, а также оценивать ее достоверность. Это касается работы с информацией как на уроках в школе, так и в свободные часы [Маркушевская 2022].

В целом следует выделить четыре группы субъектов, влияющих на информационную безопасность несовершеннолетних, исходя из состава которых можно оценивать риски информационной безопасности, существующие в этой сфере:

– субъекты, создающие информационные продукты, содержащие деструктивную информацию и распространяющие ее;
– субъекты, получающие коммерческую выгоду от распространения таких информационных продуктов;
– субъекты, обеспечивающие защиту от негативного воздействия информации;
– субъекты-представители государственной власти, участвующие в системе управления информационной безопасностью несовершеннолетних [Полянина 2022].

Существующие риски в рассматриваемой сфере можно отнести к трем категориям:

– риски, связанные с содержанием информационных продуктов;
– риски коммерческого характера, связанные с получением потребительской выгоды от использования или продажи запрещенного контента;
– собственно риски информационной безопасности [Сустина 2022].

Заключение

Итак, в данном исследовании были изучены нормативно-правовые и организационные подходы к реализации принципов государственной политики в сфере защиты детей от негативного воздействия информации, которая может нанести вред их развитию, физическому и духовному здоровью.

Наряду с рядом законодательных актов, проанализированных в статье, авторы уделили внимание Концепции информационной безопасности детей в Российской Федерации, утвержденной Распоряжением Правительства Российской Федерации от 28 апреля 2023 г. № 1105-р, которая определяет современные ракурсы решения проблем информационной безопасности детей в нашей стране.

В качестве ключевых положений Концепции были рассмотрены меры, которые призваны способствовать совершенствованию системы обеспечения информационной безопасности детей и которые должны быть объединены в единый комплекс мероприятий.

В статье также был проведен анализ количественных и качественных критериев, позволяющих проводить оценку состояния информационной безопасности несовершеннолетних, которыми в дальнейшем предполагается руководствоваться представителям государственных, общественных и коммерческих организаций для решения рассматриваемых проблем.

Для планомерного и эффективного решения вопросов обеспечения информационной безопасности детей помимо определения нормативно-правовых требований к информационной безопасности органы государственной власти и коммерческие компании организуют различные инициативы, рассчитанные на широкую общественность, которые способствуют формированию культуры информационной безопасности населения.

Таким образом, только комплексный подход к реализации требований законодательства и организации мероприятий, в которых участвуют представители разных структур, может способствовать решению задач обеспечения информационной безопасности подрастающего поколения.

Литература

Гришина, Мецатунян, Русецкая 2012 – *Гришина Н.В., Мецатунян М.В., Русецкая И.А.* Влияние социально-психологических аспектов на обеспечение информационной безопасности субъектов информационных отношений // Безопасность информационных технологий. 2012. № 1. С. 43–45.

Контылева 2023 – *Контылева Е.А.* Информационная безопасность детей и подростков в сети Интернет // Энергетические установки и технологии. 2023. Т. 9. № 1. С. 165–172.

Кундышева, Русецкая 2018 – *Кундышева И.Р., Русецкая И.А.* Инструменты и методы негативного информационного воздействия в социальных сетях // Информационная безопасность: вчера, сегодня, завтра: Международная научно-практическая конференция (г. Москва, 12 апреля 2018 г.): Сб. статей. М.: РГГУ, 2018. С. 104–109.

Маркушевская 2022 – *Маркушевская Е.А.* Формирование представлений об информационной безопасности у детей младшего школьного возраста / Е.А. Маркушевская, В.Г. Яриков, Д.В. Мазниченко // Вестник ВИЭПП. 2022. № 1. С. 25–30.

Наумова, Баранников, Митюшин 2020 – *Наумова Л.А., Баранников Д.Н., Митюшин Д.А.* Обеспечение информационной безопасности детей в Российской Федерации // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2020. № 4. С. 19–30.

Нынюк 2023 – *Нынюк Р.Н.* Информационная безопасность детей в Российской Федерации: проблемы реализации // Криминалистика: вчера, сегодня, завтра. 2023. № 2 (26). С. 110–119.

Полянина 2021 – *Полянина А.К.* Синергия государственного регулирования и гражданской активности при обеспечении информационной безопасности детей // Теория и практика общественного развития. 2021. № 11 (165). С. 63–66.

Полянина 2022 – *Полянина А.К.* Мотивы субъектов риска в системе управления информационной безопасностью детей // Теория и практика общественного развития. 2022. № 12 (178). С. 82–87.

Сустина 2022 – *Сустина Т.И.* Европейский опыт правового обеспечения информационной безопасности детей – в поисках основополагающих принципов // Право и государство: теория и практика. 2022. № 1 (205). С. 156–159.

References

Grishina, N.V., Metsatunyan, M.V. and Rusetskaya, I.A. (2012), "The influence of socio-psychological aspects on ensuring information security of subjects of information relations subjects", *Security of information technologies*, no. 1, pp. 43–45.

Kontyleva, E.A. (2023), "Information security of children and adolescents on the Internet", *Energy installations and technologies*, vol. 9, no. 1, pp. 165–172.

Kundysheva, I.R. and Rusetskaya, I.A. (2018), "Tools and methods of negative information influence in social networks", *Information security: yesterday, today, tomorrow. International scientific and practical conference* (Moscow, April 12, 2018). *Coll. of articles*, RGGU, Moscow, Russia, 2018, pp. 104–109.

Markushevskaya, E.A., Yarikov, V.G. and Maznichenko, D.V. (2022), "Formation of ideas about information security in children of primary school age", *Vestnik VIEPP*, no. 1, pp. 25–30.

Naumova, L.A., Barannikov, D.N. and Mityushin, D.A. (2020), "Ensuring information security of children in the Russian Federation", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 4, pp. 19–30.

Nynyuk, R.N. (2023), "Information security of children in the Russian Federation. Issues of implementation", *Forensic science: yesterday, today, tomorrow*, no. 2 (26), pp. 110–119.

Polyanina, A.K. (2021), "Synergy of state regulation and civic activity in ensuring children's information security", *Theory and practice of social development*, no. 11 (165), pp. 63–66.

Polyanina, A.K. (2022), "Motives of the risk subjects in the information security management system for children", *Theory and practice of social development*, no. 12 (178), pp. 82–87.

Sustina, T.I. (2022), "European experience of legal support for information security of children – in search of fundamental principles", *Law and state. Theory and practice*, no. 1 (205), pp. 156–159.

Информация об авторах

Дмитрий Н. Баранников, кандидат военных наук, доцент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; d.2006@mail.ru

Ирина А. Русецкая, кандидат исторических наук, доцент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; irkom@mail.ru

Information about the authors

Dmitrii N. Barannikov, Cand. of Sci. (Military Science), associate professor, Russian State University for the Humanities, Moscow, Russia; 6, Miusskaya Sq., Moscow, 125047, Russia; d.2006@mail.ru

Irina A. Rusetskaya, Cand. of Sci. (History), associate professor, Russian State University for the Humanities, Moscow, Russia; 6, Miusskaya Sq., Moscow, 125047, Russia; irkom@mail.ru

УДК 004.056
DOI: 10.28995/2686-679X-2024-1-80-90

Модель импульсного управления устойчивостью системы информационной безопасности

Андрей Е. Краснов
Российский государственный социальный университет, Москва, Россия, krasnovmgutu@yandex.ru

Андрей С. Кузнецов
Российский государственный социальный университет, Москва, Россия, askgoogle@internet.ru

Виталий М. Смирнов
Московский университет МВД России им. В.Я. Кикотя, Москва, Россия, smirnov.v.m.002@gmail.com

Аннотация. В статье подробно рассмотрены вопросы, связанные с организацией управления устойчивостью систем информационной безопасности. Проведен сравнительный анализ литературных источников на предмет описания актуальных методов, инструментов и алгоритмов управления устойчивостью функционирования и безопасности информационных систем на основе различных моделей управления. Рассмотрены основные подходы к формализации управления структурной динамикой систем информационной безопасности на основе математической теории множеств достижимости, а также вопросы обеспечения комплексной информационной безопасности. Предложены подходы к построению моделей стратегического и тактического управления потерей устойчивости системы информационной безопасности (СИБ) в условиях ее естественного износа, а также при наличии внешних возмущающих воздействий случайного импульсного характера. Приведены динамические модели, реализующие принципы высокоэффективного управления устойчивостью системы информационной безопасности при ее расстройке, а также и при наличии внешних возмущающих воздействий случайного импульсного характера. Сформированы основные принципы стратегического управления устойчивостью системы информационной безопасности на основе критериального подхода; выполнено формирование тактического управления ее устойчивостью на основе регулирования по отклонению.

Предложена концепция импульсного управления с помощью регулятора для поддержания динамической устойчивости информационных систем безопасности.

Ключевые слова: система информационной безопасности, устойчивость, управление по отклонению, тактическое управление, структурная динамика

Для цитирования: Краснов А.Е., Кузнецов А.С., Смирнов В.М. Модель импульсного управления устойчивостью системы информационной безопасности // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 1. С. 80–90. DOI: 10.28995/2686-679X-2024-1-80-90

The model of pulse control of the information security system stability

Andrei E. Krasnov
Russian State Social University, Moscow, Russia, krasnovmgutu@yandex.ru

Andrei S. Kuznetsov
Russian State Social University, Moscow, Russia, askgoogle@internet.ru

Vitalii M. Smirnov
Kikot Moscow University of the Ministry of Internal Affairs of Russia, Moscow, Russia, smirnov.v.m.002@gmail.com

Abstract. The article considers in detail issues related to organizing management of the stability in information security systems. A comparative analysis of literature sources was carried out to describe current methods, tools and algorithms for managing the stability of operation and security of information systems based on various management models. It also considers the main approaches to formalizing the control of the structural dynamics of information security systems based on the mathematical theory of reachability sets, as well as issues of ensuring comprehensive information security. The authors propose approaches to the construction of models for strategic and tactical management of the loss of stability of an information security system (ISS) under conditions of its natural wear and tear, as well as in the presence of external disturbing influences of a random impulse. There are given dynamic models that implement the principles of highly effective control of the stability in an information security system when it is upset, as well as in the presence of

external disturbing influences of a random impulse nature. The basic principles of strategic management of the stability in the information security system are formed based on the criteria-based approach. Formation of tactical control of its stability was carried out based on regulation by deviation.

The concept of pulse control using a regulator is proposed to maintain the dynamic stability of security information systems.

Keywords: information security system, stability, deviation control, tactical control, structural dynamics

For citation: Krasnov, A.E., Kuznetsov, A.S. and Smirnov, V.M. (2024), "The model of pulse control of the information security system stability", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 1, pp. 80–90, DOI: 10.28995/2686-679X-2024-1-80-90

Введение

Вопросы, связанные с управлением устойчивостью информационных систем (ИС), являются чрезвычайно важными для решения задач обеспечения их информационной безопасности как в условиях естественного износа ИС, так и при наличии внешних воздействий.

Ввиду важности отмеченных вопросов и малого количества посвященных им работ следует считать научное направление, связанное с управлением устойчивостью ИС, актуальным.

По рассматриваемому направлению стоит отметить следующие работы. В работе [Соколов, Охтилев 2007] проводится анализ показателей целевых и информационно-технологических возможностей ИС, устойчивости их функционирования. Предложено использовать множества достижимости (МД), которые ставятся в соответствие тем динамическим моделям, с помощью которых описывается структурная динамика ИС. Разработаны оригинальные методы и алгоритмы построения и аппроксимации МД, позволяющие повысить оперативность расчета и анализа различных показателей ИС.

В работе [Тутубалин, Кирпичников 2017] рассмотрена модель анализа устойчивости, распределенной ИС в смысле устойчивого обеспечения ее информационной безопасности некоторыми средствами защиты. На основе предложенной модели строится область функциональной безопасности распределенной информационной системы, находящейся под воздействием информационных атак. При этом данная задача решается из условия заданных допустимых интервалов: вероятности обеспечения информационной безопас-

ности рассматриваемой системы, а также критерия ухудшения значения основного показателя ее эффективности от вмешательства в процесс ее функционирования.

В статье [Гавдан 2022] исследована устойчивость объектов КИИ, проводится анализ нормативных правовых актов (НПА) и научных публикаций по теме исследования. Анализ НПА КИИ показал, что в данной области существуют проблемы, поэтому подход к обеспечению безопасности и устойчивости функционирования как КИИ, так и отдельных ее объектов должен строиться на определенных принципах.

В работе [Краснов и др. 2021] оценивание устойчивости ИС в целом основано на вычислении устойчивости ее парных активов и информационной технологии рекуррентного пересчета при подключении новых компонентов. Метод имитационного моделирования применен для моделирования влияния рисков информационной безопасности на КИИ в условиях неполных и неоднозначных данных об их составляющих, логико-вероятностные методы – для оценки влияния рисков как на составляющие (активы) ИС, так и систему в целом с учетом иерархической связи этих активов. Для оценивания влияния базовой угрозы «технического воздействия» (информационной безопасности и системы физической защиты) на риски системы безопасности производственных объектов использовался метод Монте-Карло. Проведение мероприятий по оценке устойчивости ИС и стабильности систем безопасности ориентировано на критически важные объекты в медицине, образовании, промышленности, структурах государственного управления.

В статье [Мосолов и др. 2022] применение метода смещенного идеала, а также метода сокращенного анализа иерархий позволило найти наиболее уязвимые элементы технологических систем и выявить зависимость работоспособности этих элементов от защищенности информационных потоков в автоматизированных системах управления технологическими процессами. Показана необходимость формирования обоснованных требований к политике информационной безопасности предприятия и акцентирования внимания на обеспечение достаточного уровня защиты от угроз элементам информационной системы предприятия. Исполнение таких угроз может привести к последствиям, наносящим наибольший ущерб по критериям: зона чрезвычайной ситуации, экономический ущерб, количество пострадавших, вероятность отказа системы. Проведен анализ значимости угроз для информационных систем и анализ устойчивости как отдельных компонентов, так и их агрегатов. Показан характер взаимосвязанности (отношений) компонентов информационных систем предприятия. В рамках рассмотрения

угроз для компонентов информационных систем выявлена иерархическая зависимость защищенности сложных активов информационной системы от защищенности базовых компонентов низшего уровня. Разработана модель угроз на основании утвержденного Федеральной службой по техническому и экспортному контролю перечня угроз в базе данных угроз информационной безопасности для информационных систем. Применение данного подхода позволяет сформировать положения для политики информационной безопасности предприятия и предложить специалистам по обеспечению информационной безопасности разработать меры программно-аппаратной защиты для информационной системы предприятия.

С 27 февраля по 1 марта 2023 г. в ДЦ «Юбилейный» (г. Магнитогорск) проходил форум «Цифровая устойчивость и информационная безопасность России». Главные темы форума – основные направления развития нормативной правовой базы, выполнение мероприятий, предусмотренных Указом Президента Российской Федерации от 01.05.2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности РФ», идентификация недопустимых событий для организации, импортозамещение в сфере ИБ, практика противодействия кибератакам, практики повышения защищенности организаций.

Целью настоящей работы является описание модели как стратегического, так и тактического управления устойчивостью системы информационной безопасности (СИБ) в условиях ее естественного износа, а также при наличии внешних воздействий случайного импульсного характера.

Задачами работы являются: построение модели потери устойчивости СИБ; формирование критериального стратегического управления ее устойчивостью; формирование тактического управления ее устойчивостью на основе регулирования по отклонению.

Модели потери устойчивости

Были рассмотрены три модели потери первоначальной устойчивости X_0 СИБ в моменты n дискретного времени $t_n = n\Delta t$.

Экспоненциальная:

$$X_n = \frac{1}{1+\frac{\Delta t}{T}} X_{n-1}; X_{n=0} = X_0; n = 1, 2, ..., 13, \quad (1)$$

где t – интервал времени, а T – период потери устойчивости.

Почти экспоненциальная:

$$X_n = X_{n-1} - X_{n-1}^2 \frac{(1-a)}{X_0} \frac{\Delta t}{T} e^{\frac{(n-1)\Delta t}{T}};$$

$$X_{n=0} = X_0, \qquad (2)$$

где $a < 1$.

Модель старения:

$$X_n = \frac{X_0}{a+(1-a)e^{\frac{(n-1)\Delta t}{T}}}, \qquad (3)$$

где $a < 1$.

Расчет устойчивости информационных систем с учетом взаимосвязи их компонентов подробно рассмотрен в [4, 5]. Здесь же мы используем некий единый интегральный критерий устойчивости, считая, что $X_0 = 1$.

Динамика потери устойчивости СИБ, соответствующая рассмотренным моделям, показана на рис. 1.

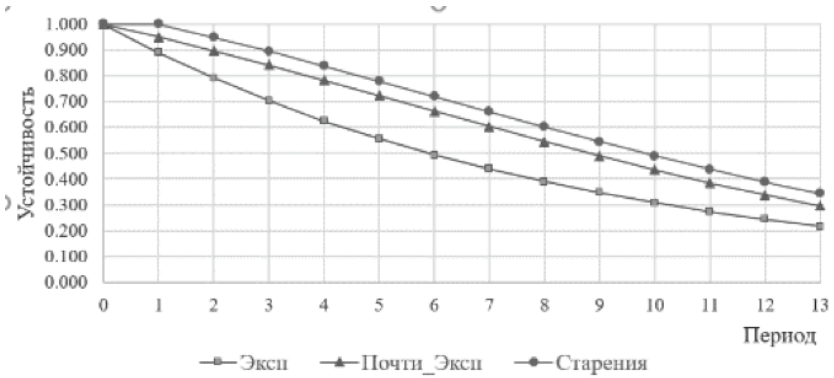


Рис. 1. Динамика потери устойчивости СИБ.

Диаграммы рис. 1 рассчитаны для параметров $\Delta t = 1$, $T = 6$ и $a = 0{,}7$.

Импульсное управление устойчивостью

Если задать критическое значение устойчивости $X_{кр}$, то, например, при $X_{кр} = 0{,}5$ устойчивость СИБ будет потеряна ($X < X_{кр}$) для первой модели уже к 6-му периоду, а двух остальных – к 10-му периоду.

Сформируем импульсные управляющие воздействия на СИБ, например, в виде денежных средств U_0, вкладываемых в отдельные периоды на поддержание (настройку) СИБ. Сформируем стратегическое управление, добавив управляющие воздействия в правую часть уравнений (1–3). Так, например, для первой модели:

$$X_n = \frac{1}{1+\frac{\Delta t}{T}} X_{n-1} \frac{1}{1+\frac{\Delta t}{T}} \frac{\Delta t}{T} \delta U_n, \qquad (4)$$

где $\delta U_n \in (0, 1)$.

При этом общие затраты на управление оценим как $U_{стр.} = N_{\delta U} U_0$, где $N_{\delta U}$ – количество управляющих импульсов. Найдем с помощью оптимизации минимальное количество $N_{\delta U}$ управляющих импульсов при условии, что все значения устойчивости $X_n > X_{кр}, \forall n$. В результате получим динамику устойчивости для разных моделей, показанную на рис. 2.

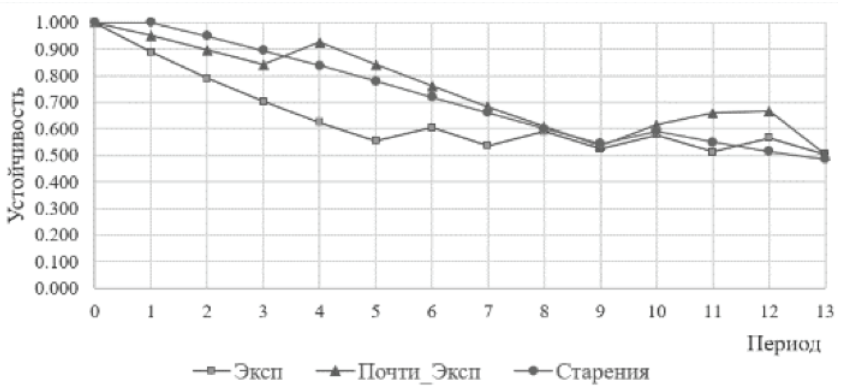


Рис. 2. Динамика потери устойчивости СИБ при стратегическом управлении

Из рисунка 2 видно, что для разных моделей оптимальные управляющие воздействия формируются в различные моменты времени. При этом для первых двух моделей было $N_{\delta U} = 4$ воздействия, что привело к общим затратам $U_{стр} = 4\ U_0$. Для третьей мо-

дели было также затрачено $U_{стр} = 4\ U_0$, однако в 13-м периоде, т. е. в начале следующего года устойчивость не восстановлена ($X_{13} = 0{,}486 < X_{кр}$).

Запишем динамику потери устойчивости при оптимальном стратегическом управлении для всех трех моделей в табл. 1.

Таблица 1

Динамика потери устойчивости
при оптимальном стратегическом управлении ($X_{n\ опт}$)

Эксп.	Почти эксп.	Старения
1.000	1.000	1.000
0.889	0.950	1.000
0.790	0.897	0.948
0.702	0.841	0.894
0.624	0.925	0.837
0.555	0.842	0.779
0.604	0.760	0.719
0.537	0.682	0.660
0.589	0.607	0.601
0.523	0.537	0.544
0.576	0.615	0.632
0.512	0.658	0.580
0.566	0.665	0.531
0.503	0.502	0.486

Сгенерируем в случайные моменты времени импульсные воздействия δS_n на СИБ. Например, для первой модели:

$$X_n = \frac{1}{1+\frac{\Delta t}{T}} X_{n-1} + \frac{1}{1+\frac{\Delta t}{T}} \frac{\Delta t}{T} \delta U_n - \frac{1}{1+\frac{\Delta t}{T}} \frac{\Delta t}{T} \delta S_n \qquad (5)$$

где $\delta S_n \in (0, 1)$.

Динамика потери устойчивости СИБ показана на рис. 3.

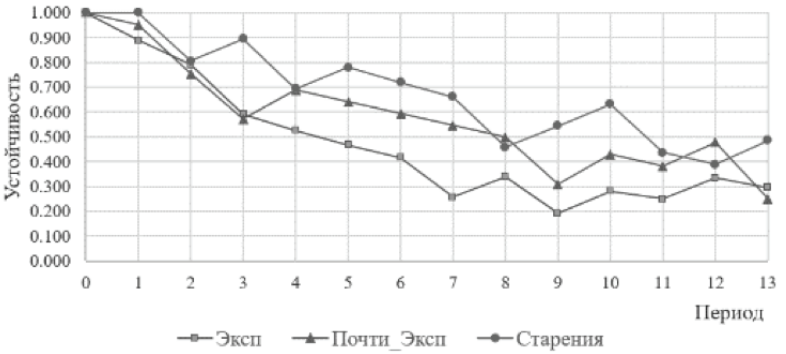


Рис. 3. Динамика потери устойчивости СИБ при стратегическом управлении и стохастическом импульсном воздействии

Для восстановления устойчивости подключим регулятор, вырабатывающий импульсные воздействия R_n в те моменты времени, когда значения устойчивости будут меньше значений $X_{n\,\text{опт}}$ из табл. 1. Например, для первой модели динамика потери и восстановления устойчивости подчиняется уравнению:

$$X_n = \frac{1}{1+\frac{\Delta t}{T}} X_{n-1} + \frac{1}{1+\frac{\Delta t}{T}} \frac{\Delta t}{T} \delta U_n + \frac{1}{1+\frac{\Delta t}{T}} \frac{\Delta t}{T} \delta R_n - \frac{1}{1+\frac{\Delta t}{T}} \frac{\Delta t}{T} \delta S_n, \quad (6)$$

$$\delta R_n = \begin{cases} 1, \text{если } X_n < X_{n\,\text{опт}}, \\ 0, \text{если } X_n \geq X_{n\,\text{опт}}. \end{cases}$$

Данная динамика отражена на рис. 4.

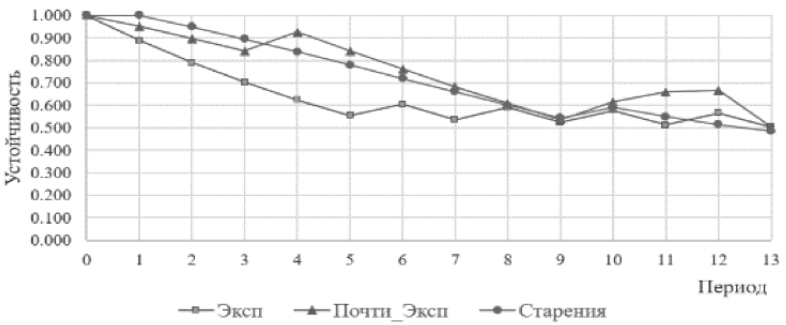


Рис. 4. Динамика потери и восстановления устойчивости СИБ при стратегическом и тактическом управлении

Заключение

Применение импульсного управления для поддержания устойчивости СИБ на заданном уровне позволяет парировать как естественный процесс расстройки системы, так и стохастические внешние импульсные воздействия, приводящие к кратковременной потере устойчивости.

Литература

Гавдан 2022 – *Гавдан Г.П.* Устойчивость функционирования объектов критической информационной инфраструктуры // Безопасность информационных технологий, [S. l]. 2022. Т. 29. № 4. С. 53–66.

Краснов и др. 2021 – *Краснов А.Е., Мосолов А.С., Феоктистова Н.А.* Оценивание устойчивости критических информационных инфраструктур к угрозам информационной безопасности // Безопасность информационных технологий [S. l]. 2021. Т. 28. № 1. С. 106–120.

Мосолов и др. 2022 – *Мосолов А.С., Краснов А.Е., Урбан Н.А.* О применении метода анализа уязвимостей технологического процесса производственного объекта для обеспечения информационной безопасности АСУ ТП с учетом взаимосвязи компонентов // Безопасность информационных технологий [S. l]. 2022. Т. 29. № 3. С. 38–52.

Соколов, Охтилев 2007 – *Соколов Б.В., Охтилев М.Ю.* Методы и алгоритмы оперативного решения задач оценивания показателей возможностей и устойчивости функционирования информационной системы // Труды СПИИРАН. 2007. № 4. С. 255–269.

Тутубалин, Кирпичников 2017 – *Тутубалин П.И., Кирпичников А.П.* Модель анализа устойчивого управления информационной безопасностью распределенной информационной системой // Вестник технического университета. 2017. Т. 20. № 19. С. 96–101.

References

Gavdan, G.P. (2022), “Stability of the functioning of critical information infrastructure objects”, *Security of information technologies, [S. l.]*, vol. 29, no. 4, pp. 53–66.

Krasnov, A.E., Mosolov, A.S. and Feoktistova, N.A. (2021), “Assessing the resilience of critical information infrastructures to information security threats”, *Information Technology Security, [S. l.]*, vol. 28, no. 1, pp. 106–120.

Mosolov, A.S., Krasnov, A.E. and Urban, N.A. (2022), “On the application of the method of analyzing the vulnerabilities of the technological process in a production facility to ensure the information security of automated process control systems, taking

into account the relationship of components", *Information Technology Security, [S. l.]*, vol. 29, no. 3, pp. 38–52.

Sokolov, B.V. and Okhtilev, M.Yu. (2007), "Methods and algorithms for quickly solving problems of assessing indicators of capabilities and stability in the functioning of an information system", *Proceedings of SPIIRAS,* no. 4, pp. 255–269.

Tutubalin, P.I. and Kirpichnikov, A.P. (2017), "Model for analyzing sustainable information security management of a distributed information system", *Bulletin of Technical University*, vol. 20, no. 19, pp. 96–101.

Информация об авторах

Андрей Е. Краснов, доктор физико-математических наук, профессор, Российский государственный социальный университет, Москва, Россия; 129226, Россия, Москва, ул. Вильгельма Пика, д. 4, стр. 8; krasnovmgutu@yandex.ru

Андрей С. Кузнецов, кандидат технических наук, Российский государственный социальный университет, Москва, Россия; 129226, Россия, Москва, ул. Вильгельма Пика, д. 4, стр. 8; askgoogle@internet.ru

Виталий М. Смирнов, кандидат технических наук, Московский университет МВД России им. В.Я. Кикотя, Москва, Россия; 119991, Россия, Москва, ул. Житная, д. 16; smirnov.v.m.002@gmail.com

Information about the authors

Andrei E. Krasnov, Dr. of Sci. (Physics and Mathematics), professor, Russian State Social University, Moscow, Russia; 4-8, V. Pika Str., Moscow, 129226, Russia; krasnovmgutu@yandex.ru

Andrei S. Kuznetsov, Cand. of Sci. (Mechanical Engineering), associate professor, Russian State Social University, Moscow, Russia; 4-8, V. Pika Str., Moscow, 129226, Russia; askgoogle@internet.ru

Vitalii M. Smirnov, Cand. of Sci. (Mechanical Engineering), Kikot Moscow University of the Ministry of Internal Affairs of Russia, Moscow, Russia; 16, Zhitnaya Str., Moscow, 119991, Russia; smirnov.v.m.002@gmail.com

УДК 004.056
DOI: 10.28995/2686-679X-2024-1-91-105

Способ защиты корпоративной сети на основе динамического распределения информационных ресурсов

Евгений Н. Надеждин
Российский государственный гуманитарный университет, Москва, Россия, en-hope@yandex.ru

Аннотация. Общей тенденцией в обеспечении сетевой безопасности является переход к использованию комплексных систем защиты информации. Как показала статистика кибератак, объектами деструктивных воздействий, как правило, являются программное обеспечение и информационные ресурсы корпоративных сетей. В рамках известной концепции комплексной защиты сетевых ресурсов обоснован принцип ситуационного переноса информационных ресурсов на защищенные узлы. В настоящей статье сформулирована задача динамического распределения локальных баз данных по узлам корпоративной информационной сети. Реализация такого механизма осуществляется в случае возникновения угрозы целостности информационным ресурсам путем априорной формализации и инициации алгоритма решения задачи о назначениях специального типа в булевых переменных. Особенностями математической модели экстремальной задачи являются минимизация затрат вычислительных ресурсов при решении комплекса прикладных задач и учет требования размещения локальных баз данных на нескольких узлах сети с возможностью резервного копирования. Иными словами, формируемый ситуационно план хранения информационных ресурсов предполагает размещение одной локальной базы данных, как минимум, на основном и резервном сервере. В статье рассмотрены общая методика определения плана размещения баз данных на узлах корпоративной сети и пример ее численной реализации с применением метода целочисленного программирования. По результатам исследований сформулированы рекомендации, заключающиеся в выборе оптимального варианта размещения компонентов распределенной базы данных на узлах корпоративной сети, при котором обеспечивается ее полная функциональность и минимизируются риски нарушения целостности информационных ресурсов.

Ключевые слова: корпоративная информационная сеть, комплексная защита информации, информационные ресурсы, план размещения локальных баз данных, задача о назначениях

Для цитирования: Надеждин Е.Н. Способ защиты корпоративной сети на основе динамического распределения информационных ресурсов // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 1. С. 91–105. DOI: 10.28995/2686-679X-2024-1-91-105

A method for protecting a corporate network based on dynamic distribution of information resources

Evgenii N. Nadezhdin
Russian State University for the Humanities, Moscow, Russia, en-hope@yandex.ru

Abstract. The general trend in ensuring network security is the transition to the use of comprehensive information security systems. As the statistics of cyber attacks have shown, the objects of destructive influences, as a rule, are software and information resources of corporate networks. Within the framework of the well-known concept of comprehensive protection of network resources, the principle of situational transfer of information resources to protected nodes is substantiated. The article formulates the problem of dynamic distribution of local databases across nodes of a corporate information network. The implementation of such a mechanism is carried out in the event of a threat to the integrity of information resources by a priori formalization and initiation of an algorithm for solving the problem of assignments of a special type in Boolean variables. The features of the mathematical model of an extremal problem are the minimization of the cost of computing resources when solving a set of applied problems and taking into account the requirement for placing local databases on several network nodes with backup capabilities. In other words, a situationally formed plan for storing information resources involves placing one local database on at least the main and backup servers. The article considers the general methodology for determining the plan for placing databases on corporate network nodes and an example of its numerical implementation using the integer programming method. Based on the research results, recommendations are formulated consisting of choosing the optimal option for placing distributed database components on corporate network nodes, which ensures its full functionality and minimizes the risks of violating the integrity of information resources.

Keywords: corporate information network, comprehensive information protection, information resources, local database placement plan, assignment problem

For citation: Nadezhdin, E.N. (2024), "A method for protecting a corporate network based on the dynamic distribution of information resources", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series,* no. 1, pp. 91–105, DOI: 10.28995/2686-679X-2024-1-91-105

Введение

На современном этапе социально-экономического развития России одной из наиболее острых технических проблем является обеспечение устойчивости функционирования и защищенности информационно-вычислительных сетей (ИВС) в условиях деструктивных воздействий различной физической природы. Современные исследования в области сетевой безопасности подтвердили перспективность применения интеллектуальных механизмов защиты информации, построенных на базе комплексирования нескольких методов и средств защиты информационных, программных и вычислительных ресурсов. Как показала практика, существенные затраты на разработку, внедрение и эксплуатацию комплексных систем защиты информационной инфраструктуры предприятий многократно перекрываются достигаемым положительным эффектом при отражении и/или нейтрализации широкого спектра массированных информационных атак и деструктивных воздействий.

Обзор публикаций предметной области

В интересах конкретизации направления исследования в настоящей статье ограничимся рассмотрением интеллектуальных механизмов защиты (МЗ) от деструктивных воздействий, в которых наряду с традиционными методами и приемами защиты используется идея переноса и динамического распределения информационных ресурсов корпоративной информационной сети (КИС). Конечная цель реконфигурации плана (схемы) размещения информационных ресурсов обусловлена стремлением скрыть или вывести базовые компоненты распределенной базы данных КИС за пределы досягаемости злоумышленника.

В работе [Уланов, Котенко 2007] представлен развернутый анализ существующих механизмов защиты от DDoS-атак и дана их классификация с учетом накопленного опыта. Авторы последовательно развивают концепцию создания комплекса механизмов защиты, способных согласованно действовать на протяжении всех стадий отражения сетевой атаки. Отмечается, что перспективная система защиты от сетевых атак типа DDoS должна функционировать за счет кооперации разнообразных системных, сетевых и глобальных механизмов защиты, осуществляемых как в рамках конкретной КИС, так и в масштабах соответствующего сегмента сети Интернет. По мнению ряда ведущих экспертов, основой пер-

спективных многоагентных систем защиты от DDoS-атак должна стать распределенная сеть гетерогенных компонентов, объединенных общей целью реализации эффективной защиты и обладающих децентрализованной системой управления рисками информационной безопасности. Особую группу интеллектуальных МЗ от сетевых атак образуют методы и средства, осуществляющие защиту на основе процедур переноса, изменения количества и оптимального разграничения ресурсов [Уланов, Котенко 2007].

Механизмы защиты, основанные на изменении и переносе ресурсов, обычно представляются на платформе распределенных ИВС, так как для реализации их функционала необходимы узлы с дополнительными ресурсами и по меньшей мере один узел, управляющий процессом переноса ресурсов. Примером такого механизма может служить известная система *Server Roaming* [Sangpachatanaruk 2004].

Идея оптимального распределения сетевых ресурсов теоретически обоснована и получила развитие в 80-х годах XX века и в последующем нашла применение в различных сферах. Наиболее продуктивными оказались области, связанные с разработкой специализированных вычислительных комплексов и сетей ЭВМ, к производительности которых предъявлялись повышенные требования.

В статье [Ворожцов, Тутова, Тутов 2016] рассматривается проблема динамичного распределения виртуальных машин в облачных центрах обработки данных (ЦОД). В основе предложенной авторами методики лежит алгоритм многокритериальной оценки характеристик существующей схемы распределения ресурсов с учетом энергопотребления, тепловыделения и коэффициента неиспользованных ресурсов сервера. Конечная цель динамического распределения вычислительных ресурсов заключается в обеспечении высокой информационной производительности ЦОД за счет выбора наилучшей схемы размещения виртуальных машин на физических серверах. Основанием для смены плана виртуальных машин служат данные учета в реальном масштабе времени потребностей приложений и системных показателей вычислительной среды.

Задачи динамического распределения ресурсов в ИВС характеризуются высоким уровнем сложности и требуют применения специальных математических методов и моделей. Известен способ управления распределением информационных ресурсов в облачных вычислительных средах [Хантимиров 2017], заключающийся в том, что посредством компьютера формируют модель использования и перераспределения ресурсов в облачных вычислительных

средах на основе концепции интеллектуальных алгоритмов, последовательно выполняя совокупность операций; на первом этапе в вычислительном облаке (ВО) выделяют ресурсы запускаемому экземпляру, на втором этапе проводят прогноз динамических параметров функционирования хостов (серверов), а на третьем этапе осуществляют динамическое перераспределение ресурсов между экземплярами ВО облака путем минимизации неравномерности использования нагрузки на основе поиска оптимальных решений. В известном способе управления распределение информационных ресурсов строится на базе модели IaaS (*Infrastructure as a Service*). При этом модель формируют для максимизации комплексного показателя эффективности, что в итоге позволяет обеспечить равномерное и оптимальное распределение нагрузки с минимальной потерей производительности ВО при одновременном сокращении операционных затрат при предоставлении вычислительных мощностей.

К настоящему времени накоплен значительный опыт в области проектирования распределенных баз данных (РБД) [Мамиконов 1990]. Большинство разработанных моделей и алгоритмов синтеза логических структур РБД базируется на исследовании задач размещения баз данных (или информационных массивов) и программных средств по узлам вычислительной сети заданной конфигурации. Эти задачи решаются, как правило, с использованием численных методов целочисленного программирования [Сергиенко 1985].

Представляется перспективным развитие и обобщение известной концепции ситуационного управления рисками информационной безопасности на основе алгоритмов адаптивного выбора вариантов и формирования оптимального плана размещения сетевых ресурсов [Надеждин, Репин 2017]. В работе [Надеждин 2019] для повышения устойчивости системы защиты информации получил развитие подход с использованием алгоритмов динамического распределения программных ресурсов между узлами сети. Задача определения оптимального плана размещения программных средств в узлах выделенного сегмента КИС интерпретирована как задача о назначениях специального типа. Отличительными чертами предложенной автором модели распределения ресурсов (относительно канонической задачи о назначениях) являются: несоответствие числа размещаемых программных средств и количества узлов, выделяемых для их размещения; учет логических условий, определяющих допустимые правила распределения ресурсов и введение дополнительных функциональных ограничений, регламентирующих затраты на обслуживание программных средств

и величину риска сокращения номенклатуры информационных услуг. В результате численного решения сформулированной задачи целочисленного программирования получен оптимальный по критерию минимума затрат план распределения программных средств на конечном множестве узлов сегмента ИВС. Полученное оптимальное решение гарантирует допустимый риск в вопросах снижения функциональности сети из-за реконфигурации программного обеспечения.

Постановка задачи выбора оптимального плана распределения ресурсов

Рассмотрим укрупненную модель задачи формирования плана размещения сетевых ресурсов в узлах корпоративной информационной сети [Надеждин 2019].

Примем следующие обозначения:

$D = (d_1, \ldots, d_i, \ldots, d_k)$, $i = \overline{1, k}$ – множество сервисов и услуг, предоставляемых пользователю;

$B = (b_1, \ldots, b_r, \ldots, b_n)$, $r = \overline{1, h}$ – множество альтернативных вариантов ресурсов, допустимых для установки;

$g_{r,j}$ – материальные затраты на установку ресурса b_r в узле u_j;

$q_{r,i}$ – материальные затраты на предоставление установленным ресурсом b_r услуги d_i для реализации соответствующего сервиса.

Дополнительно введем следующие переменные:

$x_{rj} = \{0; 1\}$ – булева переменная, указывающая, входит или нет ресурс b_r в состав обеспечения узла u_j;

$y_{rj} = \{0; 1\}$ – булева переменная, указывающая, используется или нет ресурс b_r для предоставления услуги d_i.

С учетом принятых обозначений для конкретного узла u_j КИС определим суммарные затраты на установку и использование ресурсов заданного вида:

$$F_j = \sum_{r=1}^{h} g_{r,j} \cdot x_{r,j} + \sum_{r=1}^{h} \sum_{i=1}^{k} q_{r,i} \cdot y_{r,}. \qquad (1)$$

Здесь

$$x_{r,j} = \begin{cases} 1, & \textit{если оборудование } b_r \textit{ входит в состав узла } u_j; \\ 0, & \textit{в противном случае.} \end{cases}$$

$$y_{r,i} = \begin{cases} 1, & \textit{если оборудование } b_r \textit{ используется для реализации услуги } d_i; \\ 0, & \textit{в противном случае.} \end{cases}$$

Функциональность программного средства рассчитана на оказание определенного набора услуг, поэтому предусмотрим минимальное c_r^0 и максимальное c_r^1 количество услуг, предоставляемых ресурсом b_r конечному пользователю. Для этого в модель задачи добавим областное ограничение в виде неравенства:

$$c_r^1 \le \sum_{r=1}^{h} y_{r,i} \ge c_r^0 \ . \tag{2}$$

Далее введем дисциплинирующее условие

$$x_{r,j} \ge y_{r,i}, \tag{3}$$

которое означает, что услуга d_i может быть предоставлена ресурсом b_r, если этот ресурс введен в состав ресурсного обеспечения узла u_j.

Учитывая конечное значение вычислительной мощности каждого узла u_j, предусмотрим ограничение на размещение дополнительного ресурса:

$$\sum_{r=1}^{h} x_{r,j} \le \omega_j \quad \forall\ j = \overline{1,h}\ , \tag{4}$$

где ω_j – допустимое число единиц ресурса, которое может быть установлено в узле u_j.

С учетом введенных обозначений совокупные затраты на перемещение и использование ресурсов в узлах сети зададим с помощью обобщенного показателя

$$F = F_1 + F_2 = \sum_{j=1}^{n}\sum_{r=1}^{h} g_{r,j} \cdot x_{r,j} + \sum_{j=1}^{n}\sum_{r=1}^{h}\sum_{i=1}^{k} q_{r,i} \cdot x_{r,j} \cdot y_{r,i}\ . \tag{5}$$

В соответствии с изложенными положениями оптимальным будет такой план $\pi^* = (x^*, y^*)$ размещения ресурсов на узлах сети, при котором значение показателя совокупных затрат (5) будет минимальным. Иными словами, поиск оптимального плана размещения ресурсов в КИС заключается в решении задачи дискретного программирования вида (1)–(5) в булевых переменных.

Далее под сетевыми ресурсами будем понимать набор локальных баз данных (ЛБД), которые используются для реализации прикладных информационно-вычислительных процессов и сервисов, определяемых запросами конечных пользователей.

Отметим, что реконфигурация информационного обеспечения КИС направлена на повышение устойчивости ее функционирования в условиях дестабилизирующих воздействий путем ситуационного изменения плана размещения ЛБД в узлах сети. Представленную выше модель задачи (1)–(5) выбора нового пла-

на размещения информационных ресурсов требуется дополнить функциональным ограничением, учитывающим прогностическую оценку риска информационной безопасности.

Представим модель риска нарушения доступности информационных ресурсов в виде функционала

$$R(x, y) = \Phi(V, \Omega, \pi, Z),$$

где V – вектор параметров модели сетевой атаки; Ω – вектор параметров модели сети; π – вектор параметров плана размещения ресурсов; Z – вектор параметров механизма защиты ресурсов.

На практике получить аналитическую модель совокупного риска достаточно сложно. Необходимость учета большого числа неопределенных факторов и условий функционирования КИС затрудняет запись функционала $\Phi(V, \Omega, \pi, Z)$ в явном виде. Предположим, что прогностическая оценка риска производится через реализацию семантической модели на основе нечетких когнитивных карт [4, 10]. В этом случае каждому варианту сочетания факторов (V, Ω, π, Z) можно поставить в соответствие прогностическую оценку совокупного риска. Тогда модель задачи выбора плана размещения информационных ресурсов (1)–(5) будет дополнена функциональным ограничением:

$$R(x, y) = \Phi(V, \Omega, \pi, Z) \le R_{Д}, \qquad (6)$$

где $R_{Д}$ – допустимый уровень риска.

Таким образом, для определения плана $\pi^* = (x^*, y^*)$ размещения информационных ресурсов в узлах КИС требуется найти численное решение комбинаторной задачи дискретного программирования (1)–(6). Оптимальным будет такой план размещения ЛБД в узлах сети, при котором совокупные затраты, определяемые показателем (5), будут минимальны, а величина риска, обусловленного реализацией сетевой атаки (или другими деструктивными воздействиями), не превысит допустимого уровня $R_{Д}$. Представленная выше модель может быть интерпретирована как специальная задача о назначениях, которая относится к классу нелинейных задач целочисленного программирования в булевых переменных. Для ее решения могут быть использованы вычислительные методы, устойчивые к высокой размерности вектора изменяемых параметров и к нелинейности целевого функционала и функциональных ограничений [Сергиенко 1985].

Решение задачи

Для экспериментальной проверки и апробации предложенного подхода к повышению устойчивости информационно-вычислительного процесса выполнена модификация изложенной выше укрупненной модели задачи выбора оптимального плана размещения сетевых ресурсов на узлах КИС с априорно заданной архитектурой.

Содержательная постановка задачи состоит в следующем. Задана конфигурация КИС с конечным числом (m = 5) узлов. В интересах обеспечения устойчивости функционирования сети необходимо найти схему безопасного размещения n = 8 критических ЛБД, которые могут предоставить $k = 10$ услуг по информационной поддержке решения комплекса прикладных информационно-аналитических задач. При этом каждая ЛБД должна быть размещена на основном и резервном носителях.

Для удобства формализации поиска оптимального решения и его последующей интерпретации представим целевую функцию как функцию полезности, зависящую от характеристик решаемых прикладных задач и схемы размещения ЛБД на узлах КИС:

$$F(x) = \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{r=1}^{k} x_{i,j} \cdot g_{i,j} \cdot h_{j,r}. \qquad (7)$$

Здесь

$$x_{i,j} = \{0; 1\} \quad \forall i = \overline{1, m}, \;\; j = \overline{1, n}.$$

Риск совокупный риск нарушения функциональности КИС представим в виде соотношения

$$R(x) = \sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{r=1}^{k} (x_{i,j} \cdot u_{i,j} \cdot h_{j,r}). \qquad (8)$$

Затраты на использование вычислительных ресурсов для конкретной схемы размещения ЛБД на узлах сети отразим с помощью показателя

$$C(x) = \sum_{i=1}^{m}\sum_{j=1}^{n} (x_{i,j} \cdot c_{i,j}). \qquad (9)$$

Дополнительно потребуем, чтобы в плане размещения информационных ресурсов была предусмотрена возможность резервного хранения образа каждой ЛБД. Указанное условие отразим с помощью системы ограничений следующего вида:

$$\sum_{i=1}^{m} x_{i,j} = 2 \quad \forall\ j = \overline{1,n}. \tag{10}$$

Требуется определить оптимальный план $\pi^* = x^* = (x^*_{i,j}, i = \overline{1, m}; j = \overline{1, n})$ размещения ЛБД на узлах КИС, для которого функция полезности (7) принимает максимальное значение $F(x) \to \max$; при этом затраты вычислительных ресурсов (9) на информационное обеспечение функциональности КИС должны соответствовать выделяемым ресурсам $C_Д$: $C(x) \le C_Д$, а величина совокупного риска (8) не должна превышать допустимого уровня $R_Д$: $R(x) \le R_Д$.

Исходные данные для контрольной задачи распределения ЛБД представлены в табл. 1–4.

Таблица 1

Матрица коэффициентов полезности от использования ЛБД в составе информационного обеспечения узло в $G = (g_{ij})$, $i = i,...,m$; $j = 1,...,n$

i/j	1	2	3	4	5	6	7	8
1	0,33	0,12	0,43	0,32	0,24	0,15	0,28	0,12
2	0,31	0,21	0,12	0,32	0,25	0,21	0,54	0,23
3	0,57	0,33	0,43	0,20	0,21	0,10	0,15	0,21
4	0,45	0,10	0,20	0,18	0,15	0,19	0,21	0,32
5	0,41	0,30	0,25	0,23	0,22	0,21	0,20	0,14

Таблица 2

Матрица затрат вычислительных ресурсов при решении прикладных задач в случае размещения j-й ЛБД в составе информационного обеспечения i-го узла КИС $C = (c_{ij})$, $i = i,...,m$; $j = 1,...,n$

i/j	1	2	3	4	5	6	7	8
1	16	12	43	19	24	15	28	10
2	30	28	12	26	35	31	30	24
3	31	33	19	20	21	16	14	23
4	45	40	43	38	35	35	51	42
5	40	60	45	33	52	61	20	23

Таблица 3

Матрица использования ЛБД
при решении комплекса прикладных задач
$H = (h_{ij})$, $i = i,...,n$; $j = 1,...,k$

i/j	1	2	3	4	5	6	7	8	9	10
1	1	1	1	0	0	1	0	1	0	0
2	1	1	0	1	1	0	0	1	0	0
3	0	1	0	0	1	1	1	1	0	0
4	1	0	1	1	1	1	0	0	0	0
5	0	0	1	0	0	0	0	1	1	1
6	0	0	1	1	1	1	1	0	1	1
7	0	0	0	1	0	1	1	0	1	1
8	0	0	0	0	1	0	1	0	1	1

Таблица 4

Матрица нормативных рисков для ЛБД
при возникновении угрозы
вследствие деструктивного воздействия
$U = (u_{ij})$, $i = i,...,m$; $j = 1,...,n$

i/j	1	2	3	4	5	6	7	8
1	0,10	0,15	0,10	0,25	0,10	0,25	0,20	0,25
2	0,25	0,25	0,15	0,20	0,15	0,20	0,25	0,25
3	0,30	0,30	0,35	0,30	0,15	0,20	0,25	0,10
4	0,10	0,15	0,15	0,10	0,25	0,10	0,15	0,10
5	0,25	0,15	0,25	0,15	0,35	0,25	0,15	0,30

Таблица 5

Опорный план размещения ЛБД
$x_0 = \{x_{ij}\}$, $F(x_0) = 19{,}94$ (у. е.)

i/j	1	2	3	4	5	6	7	8
1	0	0	0	1	0	1	0	0
2	1	1	0	1	0	0	0	1
3	0	1	0	0	1	0	1	0
4	0	0	1	0	0	0	0	1
5	1	0	1	0	1	1	1	0

Таблица 6

Оптимальный план размещения ЛБД
$x^* = \{x_{i,j}\}$, $F(x^*) = 26{,}95$ (у. е.)

i/j	1	2	3	4	5	6	7	8
1	0	0	1	1	1	0	1	0
2	0	0	0	1	1	1	1	1
3	1	1	1	0	0	0	0	0
4	1	0	0	0	0	0	0	1
5	0	1	0	0	0	1	0	0

Для определения оптимального плана размещения ЛБД на узлах сети применен известный метод дискретной оптимизации на основе вектора спада [Сергиенко 1985]. В результате реализации задачи целочисленного программирования найдено оптимальное решение в виде плана (матрицы) закрепления ЛБД за узлами сети $x^* = \{x_{i,j}\}$ (табл. 5). Полученному результату соответствует значение критерия полезности $F(x^*) = 26{,}95$ (у. е.).

Таким образом, в результате решения задачи целочисленного программирования в булевых переменных получен оптимальный план размещения ЛБД на узлах сети (табл. 6), реализация которого позволит повысить эффективность решения комплекса прикладных задач (по сравнению с опорным планом) на 35,4%. По материалам расчетов совокупный риск информационной безопасности снизится на 10%. При этом затраты на использование вычислительных ресурсов для нового варианта конфигурации информационных ресурсов вырастут незначительно с 513 у. е. (при опорном плане) до 550 у. е. (при рекомендуемом плане размещения ЛБД).

Выводы

В ходе настоящего исследования выявлена зависимость устойчивости информационно-вычислительного процесса и рисков информационной безопасности (ИБ) от информированности злоумышленника о конфигурации распределенного информационного обеспечения КИС. В интересах осуществления концепции ситуационного управления ИБ предложен способ динамического перераспределения информационных ресурсов на узлах КИС по

результатам решения экстремальной задачи о назначениях. В терминах дискретного программирования построена математическая модель выбора оптимального плана размещения ЛБД на конечном множестве узлов. В процессе численного решения комбинаторной задачи по критерию максимума функции полезности при учете ограничений на затраты вычислительных ресурсов и величину совокупного риска определена структура информационного обеспечения КИС. Реализация оптимального плана размещения ЛБД на узлах сети с учетом их однократного резервирования позволит снизить уровень совокупного риска при решении комплекса прикладных задач не менее чем на 10%.

Таким образом, обоснована и экспериментально подтверждена возможность обеспечения заданной функциональности КИС в условиях деструктивных воздействий на основе динамического распределения ее информационных ресурсов в соответствии с оптимальным планом, полученным в результате формализации и численного решения специальной задачи целочисленного программирования.

Литература

Ворожцов, Тутова, Тутов 2016 – *Ворожцов А.С., Тутова Н.В., Тутов А.В.* Динамическое распределение вычислительных ресурсов центров обработки данных // T-Comm: Телекоммуникации и транспорт. 2016. Т. 10. № 7. С. 47–51.

Мамиконов 1990 – *Мамиконов А.Г.* Оптимизация структур распределенных баз данных в АСУ / А.Г. Мамиконов, В.В. Кульба, С.А. Косяченко, И.А. Ужастов. М.: Наука, 1990. 240 с.

Надеждин 2019 – *Надеждин Е.Н.* Задача распределения программных ресурсов информационно-вычислительной сети // Современные наукоемкие технологии. 2019. № 12-1. С. 89–94. URL: https://top-technologies.ru/ru/article/view?id=37839 (дата обращения 02.11.2023).

Надеждин, Репин 2017 – *Надеждин Е.Н., Репин Д.С.* Ситуационный подход к задаче динамического распределения сетевых ресурсов при отражении DDOS-атак // Современные инновации в науке и технике: Сборник научных трудов 7-й Всероссийской научно-технической конференции с международным участием (13–14 апреля 2017 г.). Курск: Университетская книга, 2017. С. 139–142.

Сергиенко 1985 – *Сергиенко И.В.* Математические модели и методы решения задач дискретной оптимизации. Киев: Наукова думка, 1985. 384 с.

Уланов, Котенко 2007 – *Уланов А.В., Котенко И.В.* Защита от DDos-атак: механизмы предупреждения, обнаружения, отслеживания источника и противодействия // Защита информации. Инсайт. 2007. № 1 (13). С. 60–67.

Хантимиров 2017 – Патент (RU) № 2609076. МПК G06F 9/00 (2006.01). Способ и система интеллектуального управления распределением ресурсов в облачных вычислительных средах. Патентообладатель: Хантимиров Р.И. (RU). Опубл. 2017.01.30.

Sangpachatanaruk 2004 – *Sangpachatanaruk C., Khattab S.M, Znati T., Melhem R., Mosse' D.* Design and Analysis of a Replicated Elusive Server Scheme for Mitigating Denial of Service Attacks // Journal of Systems and Software. 2004. Vol. 73 (1). P. 15–29.

References

Khantimirov, R.I. (2017), Patent (RU) No. 2609076. IPC G06F 9/00 (2006.01), Method and system for intelligent management of resource distribution in cloud computing environments, Patent holder: Khantimirov R.I. (RU), Publ. 2017.01.30.

Mamikonov, A.G., Kulba, V.V., Kosyachenko, S.A., and Horror, I.A. (1990), *Optimizatsiya struktur raspredelennykh baz dannykh v ASU* [Optimization of distributed database structures in automated control systems], Nauka, Moscow, Russia, 240 p.

Nadezhdin, E.N. (2019), "The problem of distributing software resources of an information-computing network", *Modern science-intensive technologies*, no. 12-1, pp. 89–94.

Nadezhdin, E.N. and Repin, D.S. (2017), "Situational approach to the problem of dynamic distribution of network resources when repelling DDOS attacks", *Modern innovations in science and technology: Collection of scientific papers of the 7th All-Russian scientific and technical conference with international participation (April 13–14, 2017)*, Universitetskaya kniga, Kursk, Russia, pp. 139–142.

Sangpachatanaruk, C., Khattab, S.M, Znati, T., Melhem, R. and Mosse', D. (2004), "Design and Analysis of a Replicated Elusive Server Scheme for Mitigating Denial of Service Attacks", *Journal of Systems and Software*, vol. 73 (1), pp. 15–29.

Sergienko, I.V. (1985), "Mathematical models and methods for solving discrete optimization problems", Naukova Dumka, Kiev, Ukraine, 384 p.

Ulanov, A.V. and Kotenko, I.V. (2007), "Protection against DDos attacks: mechanisms for prevention, detection, source tracking and counteraction", *Information protection. Insight*, no. 1 (13), pp. 60–67.

Vorozhtsov, A.S., Tutova, N.V. and Tutov, A.V. (2016), "Dynamic distribution of computing resources of data centers", *T-Comm, Telecommunications and Transport*, vol. 10, no. 7, pp. 47–51.

Информация об авторе

Евгений Н. Надеждин, доктор технических наук, профессор, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; en-hope@yandex.ru

Information about the author

Evgenii N. Nadezhdin, Dr. of Sci. (Computer Science), professor, Russian State University for the Humanities, Moscow, Russia; 6, Miusskaya Sq., Moscow, 125047, Russia; en-hope@yandex.ru

УДК 004.056
DOI: 10.28995/2686-679X-2024-1-106-122

Сравнительный анализ решений класса DDP для защиты инфраструктуры предприятий

Вячеслав Е. Самойлов
Московский государственный лингвистический университет, Москва, Россия;
Российская академия народного хозяйства и государственной службы, Москва, Россия, samoilov.1992@list.ru

Сергей П. Шумилов
Московский государственный лингвистический университет
Москва, Россия, shumilovru2@gmail.com

Аннотация. В статье рассматриваются вопросы использования и внедрения современных решений в области технологий обмана в информационную инфраструктуру критических промышленных объектов. Анализируются их преимущества и ключевые особенности использования, рассматривается принцип действия распределенной инфраструктуры ложных целей. Проводится сравнительный анализ шести различных решений класса DDP иностранных и отечественных производителей по четырем критериям: наличие возможности безагентного размещения приманок; типы ловушек и приманок для промышленных систем; системы информационной безопасности, с которыми взаимодействует решение; наличие возможности размещения FullOS-ловушек. Обосновывается подход к реализации решений класса DDP для обеспечения информационной безопасности критических промышленных объектов. В рамках рассматриваемого подхода предлагается реализация в виде пяти крупных этапов настройки и внедрения распределенной структуры ложных целей. Проводится оценка перспективности применения решений DDP для повышения безопасности промышленных предприятий. Приводится пример эффективного использования применения решения класса DDP для промышленного объекта. Перспективность применения распределенной структуры ложных целей для критических промышленных объектов предлагается оценивать способом моделирования угроз, оценки рисков реализации угроз и определения среднего количества инцидентов информационной безопасности.

Ключевые слова: Distributed Deception Platform, кибербезопасность, информационная безопасность, технологии обмана, сетевая безопасность

Для цитирования: Самойлов В.Е., Шумилов С.П. Сравнительный анализ решений класса DDP для защиты инфраструктуры предприятий // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 1. С. 106–122. DOI: 10.28995/2686-679X-2024-1-106-122

Comparative analysis of DDP class solutions for enterprise infrastructure protection

Vyacheslav E. Samoilov
Moscow State Linguistic University, Moscow, Russia;
Russian Academy of National Economy and Public Administration, Moscow, Russia, samoilov.1992@list.ru

Sergei P. Shumilov
Moscow State Linguistic University, Moscow, Russia,
shumilovru2@gmail.com

Abstract. The article considers the use and implementation of modern solutions in the field of deception technologies in the information infrastructure of critical industrial facilities. Their advantages and key features of use are analyzed, the principle of operation of the distributed infrastructure of false goals is considered. A comparative analysis of six different DDP class solutions of foreign and domestic manufacturers is carried out according to four criteria: the possibility of agentless placement of baits; types of traps and baits for industrial systems; information security systems with which the solution interacts; FullOS trapping possibilities. The approach to the implementation of DDP class solutions to ensure the information security of critical industrial facilities is substantiated. Within the framework of the considered approach, the implementation is proposed in the form of five major stages of setting up and implementing a distributed structure of false goals. The prospects of using DDP solutions to improve the safety of industrial enterprises are evaluated and an example of the effective use of the DDP class solution for an industrial facility is given. The prospects of using a distributed structure of false targets for critical industrial facilities are proposed to be assessed by the threat modeling, threat risk assessment and determination of the average number of information security incidents.

Keywords: Distributed Deception Platform, cybersecurity, information security, deception technologies, network security

For citation: Samoilov, V.E. and Shumilov, S.P. (2024), "Comparative analysis of DDP class solutions for enterprise infrastructure protection", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 1, pp. 106–122, DOI: 10.28995/2686-679X-2024-1-106-122

Введение

Решения класса DDP (Distributed Deception Platform), платформы распределенного обмана, начали приобретать популярность относительно недавно и являются новыми направлениями для повышения кибербезопасности сетевой инфраструктуры организации. На это, например, указывает отчет Gartner “Hype Cycle for Threat-Facing Technologies” 2018 г., где Gartner утверждает, что рынок данных решений находится на этапе раннего развития[1,2].

На момент 2023 г. основными лидерами в области разработки платформ распределенного обмана являются компании из США, такие как Symantec, Rapid, Fortinet и другие. Однако существуют популярные решения и из ряда других стран, например Великобритании, Австрии и Израиля. В России также присутствуют компании, разрабатывающие решения в области технологий обмана. Это R-Vision, Xello, AVSoft и другие. Активному развитию отечественных решений также способствовал уход зарубежных компаний-разработчиков Deception-платформ из России.

Зачастую считается, что зарубежные решения класса DDP превосходят продукты российских компаний. Одной из причин является позднее появление российских решений в этой области и позднее начало их развития [Гуломов, Салимова, Бобомуродов 2022]. Однако активное развитие подобных систем в России может привести к изменению данного мнения. Тем не менее зарубежные решения необходимо рассматривать в качестве удачного опыта, анализ положительных сторон иностранных продуктов позволит повысить качество разрабатываемого отечественного программного обеспечения.

---

[1] Обзор рынка платформ для создания распределенной инфраструктуры ложных целей (Distributed Deception Platform). URL: https://www.anti-malware.ru/analytics/Market_Analysis/Distributed-Deception-Platform#part3 (дата обращения 12.10.2023).

[2] Новые доклады на The Standoff: искусство взлома, борьба с вирусами-шифровальщиками и автоматизация honeypot. URL: https://www. ptsecurity.com/ru-ru/about/news/novye-doklady-na-the-standoff-iskusstvo-vzloma-borba-s-virusami-shifrovalshchikami-i-avtomatizaciya-honeypot/?sphrase_id=291991 (дата обращения 12.10.2023).

Постановка задачи

Целью исследования является сравнительный анализ существующих иностранных и отечественных решений класса DDP для применения в области обеспечения информационной безопасности критических промышленных объектов. Для достижения этой цели необходимо решить следующие задачи:

- обосновать критерии для сравнительного анализа;
- проанализировать существующие решения класса DDP;
- обосновать подход к реализации решений класса DDP в области обеспечения безопасности сетевой инфраструктуры критических промышленных объектов;
- оценить перспективность применения решений DDP для повышения безопасности промышленных предприятий.

Основные принципы работы DDP

Базовым принципом, положенным в основу работы платформ для создания распределенной инфраструктуры ложных целей (англ. Distributed Deception Platform –DDP), является создание для хакеров ловушек, приманок, ложных приложений, ложных данных и баз данных, ложной Active Directory. Современные платформы распределенной инфраструктуры ложных целей могут обеспечить широкие возможности для обнаружения угроз, анализа атак и автоматизации ответных действий [Diamantoulakis, Dalamagkas, Radoglou-Grammatikis, Sarigiannidis, Karagi-annidis 2020; Mohammed, Rehman 2015; Meggelen, Madsen, Bryant 2013].

Развертывание инфраструктуры DDP преобразовывает ИТ-инфраструктуру организации таким образом, что она выстраивается в два слоя [Mohammed, Rehman 2015]: первый слой – это реальная инфраструктура предприятия, второй слой – это «эмулированная» среда, которая состоит из ловушек и приманок, расположенных на реальных физических устройствах сети (рис. 1). Например, злоумышленник может обнаружить ложные базы данных с «конфиденциальными документами», подложные учетные записи с «привилегированными правами» и т. д. Все это ложные цели, которые уводят внимание от реальных целей, и при несанкционированном доступе к ним происходит информирование SIEM системы, т. е. объявляется инцидент информационной безопасности.

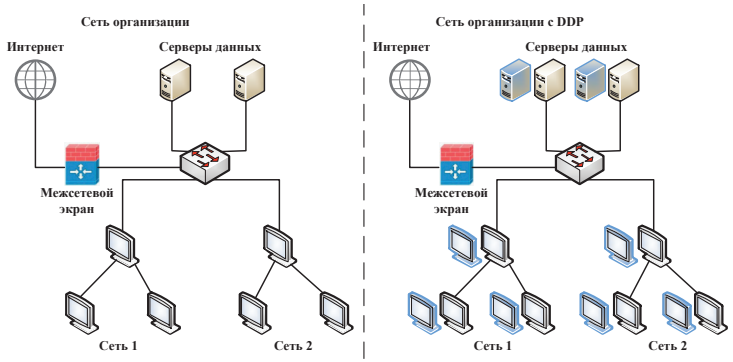


Рис. 1. Развернутая инфраструктура DDP в ИТ-системе организации

DDP – новинка рынка продуктов информационной безопасности, этим решениям всего несколько лет. Однако уже сегодня на рынке существуют серьезные решения, которые легки в развертывании и масштабировании, а также располагают серьезным арсеналом «ловушек» и «приманок». Одна из возможностей существующих DDP – эмулирование таких объектов, как базы данных, рабочие станции, маршрутизаторы, коммутаторы, банкоматы, серверы и SCADA и IoT [Сильнов, Титов 2016].

Обоснование критериев сравнительного анализа

Для проведения сравнительного анализа решений класса DDP с целью повышения уровня защищенности сетевой инфраструктуры промышленного объекта были выбраны следующие критерии:

– наличие возможности безагентного размещения приманок;
– типы ловушек и приманок для промышленных систем;
– системы информационной безопасности, с которыми взаимодействует решение;
– наличие возможности размещения FullOS-ловушек.

Возможность безагентного размещения приманок означает отсутствие необходимости устанавливать агенты на устройствах для размещения приманок. Агент – это отдельное программное обеспечение, которое устанавливается на устройстве, на котором будут размещаться приманки. Агент взаимодействует с сервером управления и позволяет разворачивать и управлять приманками на устройстве

[Красов, Петрив, Сахаров, Сторожук, Ушаков 2019]. Злоумышленники могут обнаружить агент и определить, что на устройстве присутствуют элементы ложной инфраструктуры. Чтобы этого избежать, может быть использован безагентный способ размещения приманок. В таком случае размещение и управление приманками происходит с помощью удаленного выполнения команд. Это снижает риски обнаружения злоумышленником ложной инфраструктуры.

Наличие специальных ловушек и приманок для промышленных систем позволяет использовать решения для повышения защищенности ИТ-инфраструктуры промышленного объекта [Логинов 2023]. К таким ловушкам относятся ловушки АСУ ТП, интернета вещей, SCADA. Эти ловушки могут быть размещены в специальных сегментах промышленной сети и обнаруживать атаки на промышленные системы.

Наличие возможности интеграции с наиболее популярными классами систем информационной безопасности позволяет выстроить эффективные процессы обеспечения информационной безопасности [Очередько, Бачманов, Путято, Макарян 2021]. К таким системам относятся, например, SIEM-системы, SOAR-системы, сетевые экраны, песочницы. Решения класса DDP, при наличии возможности взаимодействия с такими системами, помогут специалистам информационной безопасности автоматизировать процессы работы с инцидентами информационной безопасности.

Возможность размещения FullOS ловушек означает, что решение может создавать высоко интерактивные ловушки, имитирующие полноценные операционные системы[3]. Наличие таких ловушек позволяет собирать больше информации о действиях злоумышленников и предоставляет большую правдоподобность ложной инфраструктуре.

Анализ возможностей иностранных и отечественных решений класса DDP

Illusive Shadow направлено на обнаружение злоумышленника и применения техники горизонтального перемещения. Для размещения приманок используется безагентный способ. У данной платформы есть встроенные возможности интеграции с такими системами информационной безопасности, как IDS, ASM, EDR, PAM, SIEM.

[3] Как настроить собственный honeypot. URL: https://www.anti-malware.ru/practice/solutions/How-To-Setup-Your-Own-Honeypot (дата обращения 12.10.2023).

Из информации, размещенной в открытом доступе, не удалось выяснить, обладает ли система возможностями создания FullOS-ловушек, а также интегрирования с промышленными системами.

Fidelis Deception Platform позволяет обнаружить применение техники горизонтального перемещения, компрометацию службы каталогов Active Directory, обнаружить атаку «человек посередине», определить зараженные IoT-устройства, обнаружить использование украденных учетных данных и активность программ-вымогателей, а также собирать информацию о тактиках и техниках злоумышленника. Особенностью данного решения является высокий уровень имитации взаимодействия ложных пользователей и ложных активов. Платформа Fidelis Deception позволяет интегрироваться с различными системами информационной безопасности. Например, NTA, IPS/IDS, DLP, EDR, SIEM, SOAR. Также у данной системы есть функционал интеграции с системами интернета вещей, что может быть полезно для предприятий промышленного сектора. Однако у данного решения нет информации о возможности безагентного размещения элементов ложной инфраструктуры и возможности создания FullOS-ловушек.

TrapX DeceptionGrid обладает возможностью безагентного развертывания элементов ложной инфраструктуры. С помощью данной платформы можно развернуть несколько тысяч ложных элементов в сети организации. Данная платформа может имитировать как банкоматы, так и различные устройства интернета вещей. TrapX DeceptionGrid обладает возможностями интеграции с промышленными системами, к которым относятся IoT, OT, SCADA, SWIFT, ICS. Помимо этого, данная платформа может интегрироваться с такими системами информационной безопасности, как XDR, SIEM, EDR, IDS, IPS и другими, умеет обнаруживать ботнеты и создавать FullOS-ловушки.

Теперь перейдем к рассмотрению решений класса DDP, представленных российскими компаниями-разработчиками.

R-Vision TDP, как и зарубежные аналоги, обладает возможностями безагентного развертывания элементов ложной инфраструктуры. Касаемо интеграции с другими системами, данное решение может интегрироваться с системами информационной безопасности, такими как SOAR, SIEM, TI и другими. Данное решение также может быть использовано в сетях промышленных предприятий. Также данная платформа обладает возможностями создания FullOS-ловушек. Важным преимуществом при использовании данного решения является наличие решений класса SOAR, TI, SGRC у компании-разработчика, что позволяет выстроить наиболее эффективные процессы взаимодействия данных систем.

Xello Deception умеет создавать приманки без использования агентов, интегрироваться с устройствами интернета вещей и системами информационной безопасности, например, SOAR, NAC, NGFW. Данная платформа умеет разворачивать FullOS-ловушки, а также в системе представлен функционал базовой работы с инцидентами.

AVSoft LOKI обладает возможностью размещать приманки без агентов и создавать FullOS-ловушки. Данная платформа в основном интегрируется с песочницами и SIEM-системами. Однако есть интеграция с другим решением от AVSOFT – системой ATHENA, которая является мультисканером и песочницей. Для промышленных предприятий платформа предлагает ловушки в виде устройств интернета вещей и промышленного интернета вещей, ICS / SCADA. Особенностью данного решения также является возможность размещения исследовательских ловушек в Интернете для сбора материала и статистики для исследований и общего анализа киберугроз.

Сравнительный анализ решений класса DDP для применения в промышленности

Ранее мы рассмотрели шесть различных популярных решений класса DDP. Ниже приведена табл. 1, в которой показано сравнение рассмотренных решений по критериям, разработанным ранее.

Как видно из табл. 1, большинство решений класса DDP обладает возможностью безагентного размещения приманок. Эта возможность часто является ключевой, поскольку использование агентов для размещения приманок может стать индикатором ловушки для злоумышленника в случае обнаружения агента. Что примечательно, все российские решения обладают такой возможностью.

Часто компании, которые используют платформы распределенного обмана для повышения защищенности, хотят обладать возможностью имитировать не только типичные сетевые устройства, такие как маршрутизаторы, коммутаторы, различные сервера, АРМ, но и специфичные для какой-либо сферы устройства, например банкоматы, АСУ ТП, медицинское оборудование, устройства интернета вещей и так далее [Пономарев 2023]. Наиболее в этом плане выделяется решение TrapX DeceptionGrid, которое предлагает широкий выбор имитируемых специфичных систем, включая имитацию SWIFT и OT. Среди российских решений наиболее широкий выбор предлагает AVSoft LOKI.

Таблица 1

Сравнительный анализ решений класса DDP

Критерий	Название Deception-платформы					
	Illusive Shadow	Fidelis Deception Platform	TrapX DeceptionGrid	R-Vision TDP	Xello Deception	AVSoft LOKI
Безагентное решение	да	–	да	да	да	да
Использование с промышленными и специфичными системами	нет	IoT	IoT, SCADA, ICS, SWIFT, OT	АСУ ТП	IoT	IoT, SCADA
Интеграции с другими системами ИБ	IDS, ASM, EDR, PAM, SIEM	NTA, IPS/IDS, DLP, EDR, SIEM, SOAR	XDR, SIEM, NAC, EDR, IDS/IPS	SOAR, SIEM, TI, EDR, UEBA	SOAR, NAC, NGFW, Sandbox	SIEM, SOAR, Sandbox
FullOS-ловушки	–	–	да	да	да	да

Что касается наличия API, то оно присутствует у всех рассматриваемых систем. Наличие API также важно, поскольку позволяет внешним системам взаимодействовать с решением класса DDP. Однако наличие API не всегда позволяет в полной мере выстроить взаимодействие между системами, все зависит от возможностей API, заложенных разработчиками [Salimova 2022].

Поскольку платформы распределенного обмана используются в ИТ-инфраструктуре организации с другими системами информационной безопасности, то большим преимуществом является способность интеграции данных платформ с наиболее популярными системами информационной безопасности. Часто такими системами являются SIEM, SOAR [Salimova 2022]. Как мы можем увидеть из проведенного анализа, большинство решений класса DDP умеет интегрироваться с SIEM-системами. Также часто разработчики заявляют о возможности интеграции и с SOAR-системами. Помимо этих систем, также существуют возможности интеграции и с другими решениями, например, сетевыми экранами, песочницами. Иногда это обусловлено партнерством компании-разработчика решения класса DDP с компанией-разработчиком решения другого класса. Кроме того, некоторые компании-разработчики предоставляют возможности интеграции с другими своими продуктами и использовании решения класса DDP в связке с ними. Например, такими российскими компаниями являются R-Vision и AVSoft.

Еще одной важной функцией является возможность размещения FullOS-ловушек [Пономарев 2023; Salimova 2022]. Не все из рассматриваемых нами компаний заявляют о наличии такой возможности несмотря на то, что она часто может быть востребована. Благодаря данному функционалу возможно создавать высокоинтерактивные ловушки, имитирующие полноценные операционные системы. У всех российских решений присутствует данный функционал, что отличает их от некоторых зарубежных решений.

Обоснование подхода к реализации решений класса DDP для повышения уровня информационной безопасности критических промышленных объектов

Внедрение и подготовка к эксплуатации решения класса DDP на промышленном предприятии состоит из нескольких этапов, как организационных, так и технических. Большинство из них является типовыми для любой организации [Hong, Cao, Du 2013].

Первым шагом является разработка и согласование плана внедрения. При составлении такого плана необходимо определить:

– какие устройства присутствуют в сетевой инфраструктуре предприятия, при использовании решения класса DDP в промышленном предприятии необходимо определить, какие устройства входят в АСУ ТП, например, промышленные контролеры и рабочие станции операторов;
– какие существуют сегменты сети;
– как будут размещены сервер управления ложной инфраструктурой и сервера управления ловушками;
– какие сетевые доступы потребуются для работы элементов решения класса DDP.

В зависимости от особенностей организационной структуры предприятия план необходимо согласовать с руководителями ИТ-отдела, отдела информационной безопасности и руководством предприятия.

Вторым шагом является внедрение и развертывание элементов решения класса DDP: главного сервера управления и серверов управления ловушками. Сервера управления ловушками размещают в разных сегментах сети, включая сегмент с АСУ ТП, и обеспечивают возможность размещения элементов ложной инфраструктуры в сегменте. Серверы управления ловушками взаимодействуют с главным сервером управления, от которого они получают команды от оператора системы. Для обеспечения взаимодействия серверов управления ловушками и главного сервера управления необходимо настроить сетевой доступ между ними.

Далее производится настройка самих серверов. Этот процесс может отличаться в зависимости от выбранного решения. Сюда может относиться создание пользователей и назначение им определенных прав доступа, настройка сетевых интерфейсов, настройка ловушек и приманок, их наполнения и так далее.

После настройки серверов через главный сервер управления размещаются элементы ложной инфраструктуры. Этот процесс также отличается для разных решений класса DDP. В общем случае можно выбрать определенные типы ловушек и приманок для размещения, выбрать сегменты сети и иные параметры для размещения. Сам процесс развертывания происходит автоматически с помощью серверов управления ловушками.

Следующим шагом является настройка взаимодействия со смежными системами информационной безопасности, такими как SIEM, SOAR и другими.

После того как были развернуты и настроены сервера решения класса DDP, настроены интеграции со смежными системами информационной безопасности, элементы ложной инфраструктуры будут фиксировать события. Эти события с большой долей веро-

ятности будут указывать на действия злоумышленников [Hong, Cao, Du 2013]. События будут передаваться в смежные системы информационной безопасности, например, SIEM или SOAR, для их дальнейшей обработки специалистами по информационной безопасности.

В результате можно формализовать подход к реализации в виде следующих шагов:

1) разработка и согласование плана внедрения, включающая определение мест расстановки ловушек в IT-ландшафте организации;
2) развертывание основного сервера управления элементами решения класса DDP;
3) развертывание сервера управления ловушками, которые размещаются в разных сегментах сети;
4) размещение элементов ложной инфраструктуры на главном сервере управления;
5) настройка взаимодействия со смежными системами информационной безопасности.

Решение класса DDP позволяет увеличить эффективность обнаружения злоумышленников в системе, определить атаки, направленные на устройства АСУ ТП и иные устройства, изучить поведение злоумышленников и алгоритм их действий, в том числе применяемые ими тактики и техники атаки [Hong, Cao, Du 2013]. Все это позволяет вовремя обнаружить атаку и избежать серьезных последствий для промышленного предприятия.

Оценка перспективности применения решений класса DDP для повышения уровня информационной безопасности критических промышленных объектов

Информационную систему промышленного предприятия чаще всего отличает наличие особых технических и программных средств, предназначенных для управления технологическим процессом. Вместе они представляют АСУ ТП. АСУ ТП обладает множеством уникальных характеристик, которые делают более сложным обеспечение информационной безопасности. Например, недостатки физической защиты устройств АСУ ТП могут обеспечить злоумышленнику доступ к системе в обход систем обнаружения и предотвращения вторжений и межсетевых экранов.

Стандартные системы обнаружения атак основываются на определении подозрительной активности по известным паттернам и сигнатурам [Лебедкина, Соколовский 2021]. Такой подход неэф-

фективен при атаках с эксплуатацией уязвимостей нулевого дня или с использованием инструментов, которые позволяют изменять сигнатуры атак, что усложняет их обнаружение.

Для промышленного предприятия важно вовремя обнаружить атаку, определить объекты, подвергшиеся атаке, и скомпрометированные системы, и обеспечить быстрое реагирование на нее.

Решения класса DDP обладают возможностью размещать элементы ложной инфраструктуры в сети АСУ ТП, имитируя различные устройства и протоколы. Обнаружение подозрительной активности не основывается на сигнатурах, паттернах и анализе трафика, а на имитации реальных активов и использовании приманок [Кобец 2022]. При взаимодействии с элементами ложной инфраструктуры определяется IP-адрес атакующего, ведется журнал действий и происходит обмен с другими системами информационной безопасности. Также анализ атак с помощью решений класса DDP позволяет определить, на какие объекты нацелена атака, с помощью приманок, размещенных на реальных устройствах, можно определить, какие устройства стали объектом воздействия злоумышленников, а благодаря обмену со смежными системами информационной безопасности обеспечить быстрое реагирование на атаку и предотвратить дальнейшее ее развитие.

Примером эффективного использования является применение решения класса DDP для промышленного объекта, расположенного на большой территории. Несмотря на то что сеть АСУ ТП данного предприятия защищена межсетевым экраном, существуют угрозы информационной безопасности, связанные с физическим доступом к элементам АСУ ТП, поскольку у предприятия нет возможности обеспечить физическую безопасность на всей территории из-за ее размера. Кроме того, при обновлении программного обеспечения существуют риски заражения программой-трояном через инфицированные пакеты обновления. Примером такой программы является Havex. После заражения системы он собирает информацию об OPC-серверах, при этом оставаясь необнаруженным такими системами, как IDS, IPS и межсетевыми экранами.

Для снижения рисков, описанных выше, предприятие использует решение класса DDP. Данное решение воспроизводит работу OPC-серверов, АРМ операторов АСУ ТП, промышленных контроллеров. При атаке злоумышленникам трудно отличить настоящие активы от ложных. Часто они взаимодействуют с элементами ложной инфраструктуры, чем выдают себя. Благодаря решению класса DDP специалисты по информационной безопасности могут вовремя обнаружить атаку, изучить связанную с ней информацию, например IP-адрес атакующего и действия

злоумышленников. Поскольку было выстроено взаимодействие со смежными системами информационной безопасности, специалисты по информационной безопасности могут определить инфицированный узел, отключить его от сети и отправить на карантин, предотвращая развитие атаки.

Перспективность применения распределенной структуры ложных целей для критических промышленных объектов становится очевидной при ее оценке способом моделирования угроз, оценки рисков реализации угроз и определения среднего количества инцидентов информационной безопасности. По данным Positive Technologies, в 65% атак злоумышленники применяют в качестве инструментов вредоносные программы. Опираясь на те же данные, можно предполагать, что хакеры проводят тщательную предварительную разведку и адаптируют свой инструментарий под специфику ИТ-инфраструктуры организации, поскольку 8 из 10 атак являются целевыми [Кобец 2023]. Для быстрого выявления и реагирования на подобные угрозы и следует разворачивать приманки, точно имитирующие реальные рабочие станции сотрудников и провоцирующие атакующих выдать себя.

Заключение

В исследовании был проведен сравнительный анализ зарубежных и отечественных решений класса DDP для применения в области обеспечения информационной безопасности промышленных объектов с развитой информационной инфраструктурой. Роль распределенной инфраструктуры ложных целей растет в связи с тем, что она позволяет эффективно противостоять целевым атакам хакеров. В результате исследования известных решений класса DDP можно сделать вывод, что не все решения могут использоваться с АСУ ТП, большинство существующих на рынке систем могут использоваться со специфичными системами типа IoT. Кроме того, не у всех решений есть возможность использования FullOS-ловушек, что значительно сужает функционал DDP.

Отечественные решения предоставляют актуальные типы ловушек с учетом особенностей инфраструктуры конкретного промышленного предприятия. Наибольшим выбором промышленных типов ловушек обладает продукт AVSoft LOKI, но наибольшими возможностями обладают решения компании R-Vision, поскольку могут быть интегрированы с большим числом других систем обеспечения информационной безопасности. Актуальными проблемами в области развития систем в области DDP являются:

1) развитие систем распределенной инфраструктуры ложных целей для АСУ ТП;
2) развитие DDP для защиты хостов, обнаружения и реагирования на инциденты, происходящие в этой точке;
3) автоматизация рутинных задач.

Уход зарубежных компаний с отечественного рынка информационных технологий вследствие политики санкций позволяет национальным проектам класса DDP привлекать больше инвестиций, что положительно влияет на темпы их разработки и внедрения.

Литература

Гуломов, Салимова, Бобомуродов 2022 – *Гуломов Ш.Р., Салимова Х.Р., Бобомуродов Ш.А.* Обзор многоуровневой безопасности с использованием honeypot // Academic research in educational sciences. 2022. Т. 3. № 5. С. 800–806.

Кобец 2022 – *Кобец П.Н.* Отечественные и зарубежные подходы по разработке понятийного аппарата в сфере борьбы с кибертерроризмом и предложения по совершенствованию данного нормотворческого процесса // Правопорядок: история, теория, практика. 2022. № 1 (32). С. 94–101.

Кобец 2023 – *Кобец П.Н.* Предупреждение террористических атак на предприятиях и организациях, производящих либо хранящих опасные химические вещества // Юристъ– Правоведъ. 2023. № 2 (105). С. 136–142.

Красов, Петрив, Сахаров, Сторожук, Ушаков 2019 – *Красов А.В., Петрив Р.Б., Сахаров Д.В., Сторожук Н.Л., Ушаков И.А.* Масштабируемое honeypot-решение для обеспечения безопасности в корпоративных сетях // Труды учебных заведений связи. 2019. Т. 5. № 3. С. 86–96.

Лебедкина, Соколовский 2021 – *Лебедкина Т.В., Соколовский С.П.* Модель функционирования защищенной технологии файлового обмена // Вопросы кибербезопасности. 2021. № 5 (45). С. 52–61.

Логинов 2023 – *Логинов О.А.* Применение honeypot-ловушек для сбора данных о кибератаках на промышленные сети // E-Scio. 2023. № 3 (78).

Очередько, Бачманов, Путято, Макарян 2021 – *Очередько А.Р., Бачманов Д.А., Путято М.М., Макарян А.С.* Исследование IRP-систем на основе анализа механизмов реагирования на инциденты информационной безопасности // Прикаспийский журнал: управление и высокие технологии. 2021. № 1 (53). С. 74–82.

Пономарев 2023 – Пономарев М.В. Обнаружение вторжений в сеть организации с использованием honeynet // Международный журнал гуманитарных и естественных наук. 2023. № 4–3 (79). С. 106–108.

Сильнов, Титов 2016 – *Сильнов Д.С., Титов К.Е.* Разработка и реализация honeypot-ловушки сетевых служб, использующих протокол SIP // Современные информационные технологии и ИТ-образование. 2016. № 3-2. Т. 12. С. 143–149.

Diamantoulakis, Dalamagkas, Radoglou-Grammatikis, Sarigiannidis, Karagiannidis 2020 – *Diamantoulakis P., Dalamagkas C., Radoglou-Grammatikis P., Sarigiannidis P., Karagiannidis G.* Game theoretic honeypot deployment in smart grid // Sensors. 2020. Vol. 20 (15). P. 1–24. DOI: 10.3390/s20154199.

Hong, Cao, Du et al. 2013 – *Hong C., Cao X.B., Du W.B., et al.* The effect of attack cost on network robustness // Phys. Scr. 2013. Vol. 87 (5). P. 055801. DOI: 10.1088/0031-8949/87/05/055801.

Meggelen, Madsen, Bryant 2013 – *Meggelen J.V., Madsen L., Bryant R.* Asterisk: The Definitive Guide. Sebastopol, CA: O' Reilly Meadia, 2013. 293 p.

Mohammed, Rehman 2015 – *Mohammed M., Rehman H.* Honeypots and Routers Collecting Internet Attacks. New York: Routledge, 2015, 198 p.

Salimova 2022 – *Salimova* H.R. A virtual honeypot framework // CARJIS. 2022. Vol. 2 (5). P. 479–486.

References

Diamantoulakis, P., Dalamagkas, C., Radoglou-Grammatikis, P., Sarigiannidis, P. and Karagiannidis, G. (2020), "Game theoretic honeypot deployment in smart grid", *Sensors*, vol. 20 (15), pp. 1–24, DOI: 10.3390/s20154199.

Gulomov, Sh.R., Salimova, H.R. and Bobomurodov, Sh.A. (2022), "Review of multilevel security using honeypot", *Academic research in educational sciences*, vol. 3, no. 5, pp. 800–806.

Hong, C., Cao, X.B., Du, W.B., et al. (2013), "The effect of attack cost on network robustness", *Phys. Scr.*, vol. 87 (5), pp. 055801, DOI: 10.1088/0031-8949/87/05/055801.

Kobets, P.N. (2022), "Russian and foreign approaches to the development of the conceptual apparatus in the field of combating cyberterrorism and proposals for improving such rule-making process", *Law and order. History, theory, practice*, vol. 1 (32), pp. 94–101.

Kobets, P.N. (2023), "Prevention of terrorist attacks at enterprises and organizations producing or storing dangerous chemicals", *Yurist– Pravoved*, vol. 2 (105), pp. 136–142.

Krasov, A.V., Petriv, R.B., Sakharov, D.V., Storozhuk, N.L. and Ushakov, I.A. (2019), "Scalable honeypot-solution for security in corporate networks", *Proceedings of Communications educational institutions*, vol. 5, no. 3, pp. 86–96.

Lebedkina, T.V. and Sokolovskii, S.P. (2021), "The model of functioning of the protected technology of file exchange", *Issues of cybersecurity*, no. 5 (45), pp. 52–61.

Loginov, O.A. (2023), "Application of honeypot-traps for collecting data on cyberattacks against industrial networks", *E-Scio*, vol. 3 (78).

Meggelen, J.V., Madsen, L. and Bryant, R. (2013), *Asterisk: The Definitive Guide*, O'Reilly Meadia, Sebastopol, CA, USA, 293 p.

Mohammed, M. and Rehman, H. (2015), *Honeypots and Routers Collecting Internet Attacks*, Routledge, New York, USA, 198 p.

Ponomarev, M.V. (2023), "Detection of intrusions into the organization's network using honeynet", *International Journal of Humanities and Natural Sciences*, vol. 4-3 (79), pp. 106–108.

Ochered'ko, A.R., Bachmanov, D.A., Putyato, M.M. and Makaryan, A.S. (2021), "The study of IRP systems based on the analysis of mechanisms for responding to information security incidents", *Caspian Journal: Management and High Technologies*, vol. 1 (53), pp. 74–82.

Salimova, H.R. (2022), "A virtual honeypot framework", *CARJIS*, vol. 2 (5), pp. 479–486.

Silnov, D.S. and Titov, K.E. (2016), "Development and implementation of honeypot traps for network services using the SIP protocol", *Modern Information Technologies and IT Education*, no. 3-2, vol. 12, pp. 143–149.

Информация об авторах

Вячеслав Е. Самойлов, кандидат технических наук, Московский государственный лингвистический университет, Москва, Россия; 119034, Россия, Москва, ул. Остоженка, д. 38, стр. 1;

Российская академия народного хозяйства и государственной службы, Москва, Россия; 119571, Россия, Москва, просп. Вернадского, д. 84, стр. 1; samoilov.1992@list.ru

Сергей П. Шумилов, студент, Московский государственный лингвистический университет, Москва, Россия; 119034, Россия, Москва, ул. Остоженка, д. 38, стр. 1; shumilovru2@gmail.com

Information about the authors

Vyacheslav E. Samoilov, Cand. of Sci. (Computer Science), Moscow State Linguistic University, Moscow, Russia; 38-1, Ostozhenka Str., Moscow, 119034, Russia;

Russian Academy of National Economy and Public Administration, Moscow, Russia; 84-1, Vernadskii Lane, Moscow, 119571, Russia; samoilov.1992@list.ru

Sergei P. Shumilov, student, Moscow State Linguistic University, Moscow, Russia; 38-1, Ostozhenka Str., Moscow, 119034, Russia; shumilovru2@gmail.com

Научный журнал
Вестник РГГУ
Серия «Информатика.
Информационная безопасность. Математика»
№ 1
2024

Дизайн обложки
Е.В. Амосова

Корректор
Ж.П. Григорьева

Компьютерная верстка
Н.В. Москвина

Учредитель и издатель
Российский государственный гуманитарный университет
125047, Москва, Миусская пл., 6

Свидетельство о регистрации СМИ
ПИ № ФС77-72977 от 25.05.2018 г.
Периодичность 4 раза в год

Подписано в печать 15.03.2024
Выход в свет 22.03.2024
Формат 60×90 1/16
Уч.-изд. л. 7,7. Усл. печ. л. 7,8
Тираж 1050 экз. Свободная цена
Заказ № 1930

Отпечатано в типографии Издательского центра
Российского государственного гуманитарного университета
125047, Москва, Миусская пл., 6
www.rsuh.ru