

**Министерство науки и высшего образования Российской Федерации**  
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ**  
**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**  
**«Национальный исследовательский университет ИТМО»**  
**(Университет ИТМО)**

**Факультет        БИТ**

**Образовательная программа        Информационная безопасность**

**Направление подготовки (специальность) 10.04.01        Информационная**  
**безопасность / Information security**

**О Т Ч Е Т**

**о научно-исследовательской работе**

**Наименование        темы:        Исследование        актуальности        обеспечения**  
**безопасности        критической        информационной        инфраструктуры**  
**Российской Федерации в современных условиях**

**Обучающийся:        Конаков Александр Михайлович, магистрант группы**  
**N4155c**

**Согласовано:**

**Научный руководитель:        Лившиц Илья Иосифович, д.т.н., профессор**  
**ФБИТ, Университет ИТМО**

**Ответственный за научно-исследовательскую работу:        Заколдаев Данил**  
**Анатольевич, к.т.н., декан ФБИТ, Университет ИТМО**

**Научно-исследовательская работа выполнена с оценкой**

**5 (отлично)**

**Дата        13.04.2023**

**Санкт-Петербург, 2022**

## Оглавление

ВВЕДЕНИЕ .....	3
1. ПРОБЛЕМАТИКА АКТУАЛЬНОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В СОВРЕМЕННЫХ УСЛОВИЯХ .....	4
ВЫВОДЫ ПО ПЕРВОЙ ГЛАВЕ .....	6
2. ОБЗОР ПРЕДМЕТНОЙ ОБЛАСТИ ИССЛЕДОВАНИЯ И СУЩЕСТВУЮЩИХ РАБОТ В ДАННОМ НАПРАВЛЕНИИ .....	7
ВЫВОДЫ ПО ВТОРОЙ ГЛАВЕ .....	11
3. ОПРЕДЕЛЕНИЕ ТЕМЫ ИССЛЕДОВАНИЯ. ФОРМИРОВАНИЕ ЦЕЛЕЙ И ЗАДАЧ .....	12
ВЫВОДЫ ПО ТРЕТЬЕЙ ГЛАВЕ .....	14
ЗАКЛЮЧЕНИЕ .....	15
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ .....	16

## **ВВЕДЕНИЕ**

Основной целью предстоящей научно - исследовательской работы является формирование и определение основного направления магистерского диссертационного исследования.

Для достижения поставленной цели в рамках данного исследования предполагается выполнение следующих задач:

1. Изучить законодательство и нормативно - правовые документы в области критической информационной инфраструктуры Российской Федерации;
2. Обосновать актуальность защиты критической информационной инфраструктуры;
3. Провести обзор предметной области исследования;
4. Провести аналитический обзор существующих научных работ данной сфере;
5. Сформировать основное направление, цели и задачи магистерского диссертационного исследования.

В рамках реализуемой научно - исследовательской работы рассматриваются основные аспекты обеспечения безопасности критической информационной инфраструктуры Российской Федерации в современных условиях.

# **1. ПРОБЛЕМАТИКА АКТУАЛЬНОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В СОВРЕМЕННЫХ УСЛОВИЯХ**

В современных условиях при активной реализации политики развития и внедрения информационных систем и технологий различных специфик и классификаций во все сферы жизни и нашего взаимодействия, ежегодно регистрируется неуклонный рост количества атак на объекты критической информационной инфраструктуры как в Российской Федерации, так и в других странах по всему миру.

Особая «целенаправленность» атак злоумышленников ставит под удар безопасность личности, общества и государства при эксплуатации объектов критической информационной инфраструктуры и её связующих элементов и систем. И с прогнозируемым учётом последующего роста кибератак и их негативными последствиями на объекты КИИ, обеспечение защиты, устойчивого и бесперебойного функционирования этих объектов, становится одним из приоритетных направлений в информационной безопасности нашей страны.

Атаки на объекты критической информационной инфраструктуры происходят все чаще. Особенностью современных кибератак является их целенаправленность и ориентированность на конкретную сферу деятельности или отдельную компанию.

Согласно исследованиям, проведённым научно - техническим центром ФГУП «ГРЧЦ», в 2020 году потери мировой экономики от кибератак составили 2,5 трлн. долларов, а возможный рост в последующие годы составит порядка 8 трлн. долларов. В первом полугодии 2021 года число атак с использованием вредоносного программного обеспечения на критическую инфраструктуру Российской Федерации возросло более чем на 150% по сравнению с предыдущим годом. При этом, по подсчётам экспертов и

аналитиков, порядка 40% атак исходят от независимых киберпреступников и 60% приходится на проправительственные хакерские группировки.

В свою очередь, наибольший интерес со стороны злоумышленников вызывают такие сферы деятельности как:

1. Промышленность;
2. Государственное управление;
3. Энергетика;
4. Медицина;
5. Военно - промышленный комплекс.

И учитывая все факторы, как было уже сказано ранее, в России, критическая информационная инфраструктура становится приоритетным направлением в области защиты информации и развития информационной безопасности.

Основываясь на положения Федерального закона № 187-ФЗ от 26.07.2017 г.[3], под критической информационной инфраструктурой - понимается комплекс объектов информационной инфраструктуры, а также сетей электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры между собой, т.е. критически важных для деятельности в различных областях деятельности.

В свою очередь, безопасность критической информационной инфраструктуры представляет собой комплекс мероприятий по организации устойчивого и бесперебойного функционирования критичных процессов предприятия, при проведении компьютерных атак по отношению к ним.

Поэтому, с целью обеспечить непрерывное функционирование всех процессов критической информационной инфраструктуры возникает острая необходимость новых методов обеспечения её защиты, соответствующих требованиям нормативно - правовых и методических документов регуляторов [4] и иных органов государственной власти и способных противостоять современным угрозам, а также снижать риски реализации возникающих угроз.

## **ВЫВОДЫ ПО ПЕРВОЙ ГЛАВЕ**

Проанализировав данные из открытых источников (законодательство, нормативно - правовые и нормативно - методические документы регуляторов), включая статистику зарегистрированных совершенных атак (реализованных угроз безопасности информации) на объекты критической информационной инфраструктуры Российской Федерации, можно сделать вывод о том, что защита критической информационной инфраструктуры является стратегическим направлением в области информационной безопасности на долгие годы вперёд, независимо от сферы деятельности, указанной в Федеральном законе №187 «О безопасности критической информационной инфраструктуры» от 26.07.2017 и категории значимости объекта критической информационной инфраструктуры согласно Постановлению Правительства РФ от 8.02.2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» [5].

Также, отдельным пунктом хотелось бы выделить тенденцию разработки и внедрения совершенно новых методов и средств защиты от атак на критическую инфраструктуру, соответствующие «современным» требованиям к защите ресурсов и способные отражать большинство реализуемых угроз, снижая уровень негативного воздействия и последствий.

## **2. ОБЗОР ПРЕДМЕТНОЙ ОБЛАСТИ ИССЛЕДОВАНИЯ И СУЩЕСТВУЮЩИХ РАБОТ В ДАННОМ НАПРАВЛЕНИИ**

Предметная область данной научно - исследовательской работы является критическая информационная инфраструктура Российской Федерации.

По вопросам связанным с обеспечением безопасности и функционированием критической информационной инфраструктуры, написано немало хороших научных статей и работ, опубликованные в научных журналах и в сборниках проведённых конференций различного уровня.

Часть рассмотренных работ представляют собой обзорно - аналитическую часть законодательства и нормативно правовых актов (через призму правового института [6]), которые оказывают непосредственное влияние [7] не только на субъекты (так называемых «законных владельцев») критической информационной инфраструктуры, но и объекты (ИС, АСУ ТП, ИТС) данной сферы [8, 9].

Также авторами рассматриваются некоторые аспекты по возможности и «уместности» применения различных технических средств, позволяющих повысить уровень защиты объектов критической информационной инфраструктуры [10]. Другие, в свою очередь, предлагают новые модели [11,12], методы и решения [13,14] с целью совершенствования уже существующих систем безопасности. При этом, некоторых работах учитываются различные факторы, в контексте как основополагающие или же вспомогательные [15,16].

Проанализированные научные статьи (с их общей характеристикой, содержащей название, имена авторов, год издания и тип работы) представлены в Таблице 1. В дальнейшем, представленный список научных работ будет использован в качестве ряда литературных источников

(литературной базы) для проведения магистерского диссертационного исследования. Также подразумевается и то, что этот список будет дополняться.

Таблица 1 Анализ научных работ в исследуемой области

№	Полное название статьи	Авторы	Год издания	Тип работы
1	Модели и методы разработки комплексов информационной безопасности критической информационной инфраструктуры Российской Федерации	Костин В. Н. Боровский А. С.	2019	Статья, опубликованная в сборнике трудов конференции
2	Аспекты применения технологии vpn в критических информационных инфраструктурах	Зубакин В. В. Кий А. В. Морозов И. В.	2017	Статья, опубликованная в сборнике трудов конференции
3	Методика обоснования тестовых информационно-технических воздействий, обеспечивающих рациональную полноту аудита защищенности объекта критической информационной инфраструктуры	Макаренко С. И. Смирнов Г. Е.	2021	Статья, опубликованная в научном журнале
4	Защита критической информационной инфраструктуры как новый	Ельчанинова Н. Б.	2020	Статья, опубликованная в



	институт правового обеспечения информационной безопасности			научном журнале
5	Эталонная модель безопасности критических информационных инфраструктур	Петухов А.Н. Гуснин С.Ю.	2019	Статья, опубликованная в журнале и являющаяся материалом конференции
6	Разработка модели угроз для объектов критической информационной инфраструктуры с учётом методов социальной инженерии	Новикова Е. Ф. Хализев В. Н.	2019	Статья, опубликованная в научном журнале
7	О безопасности критической информационной инфраструктуры российской федерации	Горелик В.Ю. Безус М. Ю.	2020	Статья, опубликованная в научном журнале
8	Критическая информационная инфраструктура как объект обеспечения безопасности	Абдулоризов А. Н.	2020	Статья, опубликованная в научном журнале
9	Основные подходы к анализу и оценке рисков информационной	Максименко В. Н. Ясюк Е. В.	2017	Статья, опубликованная в

	безопасности			научном журнале
10	Влияние Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» на владельцев критических информационных инфраструктур	Ванцева И. О. Зырянова Т. Ю. Медведева О. О.	2018	Статья, опубликованная в научном журнале
11	Модель процесса функционирования системы обеспечения информационной безопасности объекта критической информационной инфраструктуры в задаче оценивания его эффективности	Беляков М. И.	2020	Статья, опубликованная в научном журнале

## **ВЫВОДЫ ПО ВТОРОЙ ГЛАВЕ**

Проанализировав предметную область предполагаемого исследования, а также изучив несколько научных работ в данной сфере (проанализировано и подобрано 11 научных работ), можно подтвердить, что критическая информационная инфраструктура является одним из основных направлений в информационной безопасности и реализации политики государства по защите критически важных ресурсов от различных видов угроз, и снижению уровня негативных последствий в случае реализации атак. Это подтверждается не только регулярным совершенствованием законодательства в данной сфере, но и количеством научных работ, позволяющих оценить степень влияния критической инфраструктуры на нашу жизнь в целом.

Представленные научные работы, в дальнейшем, предполагаются использоваться в качестве ряда литературных источников для магистерского диссертационного исследования

### **3. ОПРЕДЕЛЕНИЕ ТЕМЫ ИССЛЕДОВАНИЯ. ФОРМИРОВАНИЕ ЦЕЛЕЙ И ЗАДАЧ**

В рамках выполняемого исследования, предстояло сформировать цель и задачи будущего магистерского диссертационного исследования. И опираясь на уже ранее собранный и изученный материал, были выдвинуты следующие формулировки:

#### ***Предмет исследования***

Обеспечение безопасности процессов функционирования и взаимодействия объектов критической информационной инфраструктуры, принадлежащих организации - субъекту.

#### ***Объект исследования***

Математическое обоснование метрик готовности работы организации - субъекта в сфере значимых объектов критической информационной инфраструктуры.

#### ***Цель исследования***

Предложить методику оценки готовности организации в сфере значимых объектов критической информационной инфраструктуры с учётом применяемых в эксплуатации средств защиты.

#### ***Задачи исследования***

1. Проанализировать действующее законодательство Российской Федерации в сфере критической информационной инфраструктуры с уклоном на оптимальное функционирование субъектов.
2. Проанализировать математические и экономические аспекты функционирования субъектов критической информационной инфраструктуры;
3. Сформировать и предложить расчётную формулу оценки готовности субъекта критической информационной инфраструктуры с установленными критериями работы (функционирования).

4. Сформировать методику оценки готовности работы и анализа эффективности применяемых мер защиты;
5. Провести экспериментальное исследование методики в условиях реальной работы объекта критической информационной инфраструктуры;
6. Внести коррективы в предлагаемую методику исходя из полученных экспериментальным путём результатов оценки;
7. Сформировать итоговый отчёт по полученным результатам исследования;
8. Сделать выводы о перспективах внедрения и использования данной методики в организациях - субъектах критической информационной инфраструктуры.

Основная задумка предстоящей магистерской исследовательской работы заключается в следующем: опираясь на положения регуляторов в области обеспечения безопасности информации [17], ГОСТ Р ИСО/МЭК 27004 - 2021 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание» [18], а также на основании математических моделей угроз безопасности информации и экономики её защиты предложить методику оценки, которая в свою очередь, позволит численно выявить необходимость существования объектов критической инфраструктуры в организации, их готовности к работе и возможности непрерывного функционирования, а также результативности применяемых средств защиты информации в процентном соотношении.

## **ВЫВОДЫ ПО ТРЕТЬЕЙ ГЛАВЕ**

Проанализировав информацию, полученную из различных открытых источников (электронные библиотеки, научные работы и статьи, нормативно - правовые и нормативно - методические документы), непосредственно касающихся обеспечения безопасности критической информационной инфраструктуры Российской Федерации, были выдвинуты:

1. Основная тема дальнейшего магистерского исследования;
2. Предмет и объект исследования;
3. А также сформулированы цель и предстоящие задачи.

Выбранная тема исследования, цели и задачи, которые необходимо достигнуть, в перспективе, поспособствуют повышению уровня безопасности субъектов и объектов критической информационной инфраструктуры.

## **ЗАКЛЮЧЕНИЕ**

В ходе выполнения исследования в рамках научно исследовательской - работы, были выполнены в полном объёме цель и поставленные задачи. А соответственно, выполнено в полном объёме индивидуальное задание в соответствии с графиком выполнения работ.

Планируемые результаты научно - исследовательской работы получены полностью и собраны в качестве необходимого материала для реализации дальнейшего исследования в рамках магистерской выпускной квалификационной работы.

Также, в качестве отдельного элемента заключения, хочется отметить актуальность обеспечения безопасности критической информационной инфраструктуры Российской Федерации в современных условиях, при постоянных фиксируемых атаках на вышеуказанные ресурсы.

Реализация всего исследования позволит повысить эффективность обеспечения информационной безопасности критических инфраструктур, распределить нагрузку и задействованные ресурсы при обеспечении защиты в целях устойчивого обеспечения защиты и в перспективе, принесёт огромную пользу в различных областях критической информационной инфраструктуры, затрагивая не только научную (проведение научных - исследовательских экспериментов) и практические (реализация на практике перспективных предложений по обеспечению безопасности) стороны, но и социально - значимые (критическая инфраструктура затрагивает многие сферы жизни от медицины и финансов до ракетостроения и атомной промышленности), напрямую связанные с нашей жизнью.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Кибератаки на критическую информационную инфраструктуру // URL: [https://rdc.grfc.ru/2021/07/kiberataki\\_na\\_kii/#post-1443-\\_Toc74839610](https://rdc.grfc.ru/2021/07/kiberataki_na_kii/#post-1443-_Toc74839610) (Дата обращения 15.12.2022);
2. Защита субъектов и объектов КИИ - безопасность КИИ // URL: <https://ec-rs.ru/resheniya/bezopasnost-kriticheskoy-informatsionnoy-infrastruktury-kii/> (Дата обращения 16.12.2022);
3. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ : принят Государственной Думой 12 Июля 2017 Года : Одобрен Советом Федерации 19 июля 2017 года;
4. Приказ ФСТЭК от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры российской федерации» URL: <https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239> (Дата обращения 16.12.2022);
5. Постановление Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» // Собрание законодательства Российской Федерации, 2017, N 31, ст. 4736;
6. Ельчанинова Н. Б. Защита критической информационной инфраструктуры как новый институт правового обеспечения информационной безопасности // Информационное общество. – 2020. – №. 2. – С. 58-65.;
7. Ванцева И. О., Зырянова Т. Ю., Медведева О. О. Влияние Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» на владельцев критических информационных инфраструктур // Вестник УрФО. Безопасность в информационной сфере. – 2018. – №. 1 (27). – С. 71-76;



8. Горелик В.Ю., Безус М. Ю. О безопасности критической информационной инфраструктуры Российской Федерации // STUDNET. - 2020. - №9. - С. 1438-1448. - URL: <https://cyberleninka.ru/article/n/o-bezopasnosti-kriticheskoy-informatsionnoy-infrastruktury-rossiyskoy-federatsii/viewer> (Дата обращения 15.12.2022);
9. Абдулоризов, А. Н. Критическая информационная инфраструктура как объект обеспечения безопасности / А. Н. Абдулоризов. - Текст : непосредственный // Молодой ученый. - 2020. - № 20 (310). - С. 16-19. - URL: <https://moluch.ru/archive/310/69972/> (дата обращения 16.12.2022);
10. Зубакин В. В., Кий А. В., Морозов И. В. Аспекты применения технологии vpn в критических информационных инфраструктурах //Региональная информатика и информационная безопасность. – 2017. – С. 97-98.;
11. Костин В. Н., Боровский А. С. Модели и методы разработки комплексов информационной безопасности критической информационной инфраструктуры Российской Федерации //Информационные технологии интеллектуальной поддержки принятия решений (ITIDS'2019). – 2019. – С. 210-213.;
12. Петухов А.Н., Гуснин С.Ю. Эталонная модель безопасности критических информационных инфраструктур // Международная конференция по мягким вычислениям и измерениям, 2019.;
13. Макаренко С. И., Смирнов Г. Е. Методика обоснования тестовых информационно-технических воздействий, обеспечивающих рациональную полноту аудита защищенности объекта критической информационной инфраструктуры //Вопросы кибербезопасности. – 2021. – №. 6 (46). – С. 12-25.
14. Максименко В. Н., Ясюк Е. В. Основные подходы к анализу и оценке рисков информационной безопасности // Экономика и качество систем связи. 2017. №2. С. 42 - 48.;
15. Новикова Е. Ф., Хализев В. Н. Разработка модели угроз для объектов критической информационной инфраструктуры с учётом методов

социальной инженерии // Прикаспийский журнал: управление и высокие технологии. 2019. №4 (48). С. 127-135.;

16. Беляков М. И. Модель процесса функционирования системы обеспечения информационной безопасности объекта критической информационной инфраструктуры в задаче оценивания его эффективности //Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. – 2020. – №. 11-12. – С. 71-75.;

17. Методический документ "Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.);

18. ГОСТ Р ИСО/МЭК 27004 - 2021 Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание. Information technology. Security techniques. Information security management. Monitoring, measurement, analysis and evaluation. - М., - 2021. - 50 с.

**Министерство науки и высшего образования Российской Федерации**  
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**  
**«Национальный исследовательский университет ИТМО»**  
**(Университет ИТМО)**

**ГРАФИК ВЫПОЛНЕНИЯ НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЫ**

Студент Конаков Александр Михайлович  
(Фамилия И. О. полностью)

Факультет БИТ Группа № N4155c

Направление подготовки 10.04.01 Информационная безопасность / Information security

Научный руководитель Лившиц Илья Иосифович, д.т.н., профессор ФБИТ, Университет ИТМО  
(Фамилия И. О., место работы, должность)

Наименование темы: Исследование актуальности обеспечения безопасности критической информационной инфраструктуры Российской Федерации в современных условиях

Цель и задачи выполнения работы Цель работы: сформировать и определить основное направление магистерского диссертационного исследования. Задачи: проанализировать законодательство в области критической информационной инфраструктуры, выполнить обзор исследуемой области, анализ существующих научных работ и обосновать актуальность.

Ожидаемые результаты Поставлены цель и задачи магистерского диссертационного исследования, проведён обзор актуальности и обоснованности защиты критической информационной инфраструктуры. Подобран ряд литературных источников по теме работы.

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		планируемая	фактическая	
1	Подготовка материалов для проведения исследования	15.09.22	15.09.22	5 (отл)
2	Выбор основного направления темы исследования	17.09.22	17.09.22	5 (отл)
3	Определить тему исследования	17.09.22	17.09.22	5 (отл)
4	Выполнить обзор исследуемой области	30.09.22	30.09.22	5 (отл)
5	Составление плана и графика работ	30.09.22	30.09.22	5 (отл)
6	Выполнение поставленных задач в рамках НИР	09.01.23	09.01.23	5 (отл)
7	Оформление отчёта и сопутствующих документов, написание аннотации НИР	11.01.23	11.01.23	5 (отл)
8	Защита НИР	13.01.23	13.01.23	5 (отл)

Научный руководитель  (подпись) Лившиц И.И. 30.09.22 (дата)

Студент  (подпись) Конаков А.М. 30.09.22 (дата)

**Министерство науки и высшего образования Российской Федерации**  
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**  
**«Национальный исследовательский университет ИТМО»**  
**(Университет ИТМО)**

**Факультет БИТ**

**Направление подготовки (специальность) 10.04.01 Информационная безопасность**  
**/ Information security**

**ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ**  
на научно-исследовательскую работу

**Обучающийся**      Конаков Александр Михайлович      **Группа №**      N4155с  
(Ф. И. О.)

**Научный руководитель**      Лившиц Илья Иосифович, д.т.н., профессор ФБИТ, Университет ИТМО  
(Ф. И. О., место работы, должность)

**Наименование темы:**      Исследование актуальности обеспечения безопасности критической  
информационной инфраструктуры Российской Федерации в современных  
условиях

**Сроки выполнения научно-исследовательской работы:**      01.09.2022 - 28.01.2023

**Место выполнения научно-исследовательской работы:**      Федеральное государственное автономное образовательное  
учреждение высшего образования «Национальный  
исследовательский университет ИТМО» (Университет ИТМО),  
Факультет безопасности информационных технологий

**Должность:**      Обучающийся

**2. ПЛАН-ГРАФИК**

№ этапа	Наименование этапа	Срок завершения этапа	Виды работ	Форма(-ы) отчетности*
1	2	3	4	5
1	Подготовка материалов для проведения исследования	15.09.22	Изучение законодательства, нормативно правовых и нормативно - методических документов в области выбранного исследования	Отчет, график выполнения НИР
2	Выбор основного направления темы исследования	17.09.22	Формулировка основного направления в контексте предстоящего исследования	Отчет, график выполнения НИР
3	Определить тему исследования	17.09.22	Постановка целей и задач исследования	Отчет, график выполнения НИР
4	Выполнить обзор исследуемой области	30.09.22	Определение актуальности и обоснованности проводимого исследования	Отчет, график выполнения НИР
5	Составление плана и графика работ	30.09.22	Формирование графика выполнения работы	Отчет, график выполнения НИР




6	Выполнение поставленных задач в рамках НИР	09.01.23	Поэтапное выполнение поставленных задач в рамках исследования с соответствующими отметками о результатах выполнения	Отчет, график выполнения НИР
7	Оформление отчёта и сопутствующих документов, написание аннотации НИР	11.01.23	Оформление и подготовка всех необходимых документов согласно требованиям	Отчет, график выполнения НИР
8	Защита НИР	13.01.23	Сдача работы руководителю практики для получения оценки	Индивидуальное задание, отчет, график выполнения НИР, отзыв научного руководителя, аннотация НИР

### 3. ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ОТЧЁТНОСТИ

Наименование формы отчётности	Требования к оформлению
Отчёт	ГОСТ 7.32-2017
Индивидуальное задание	Согласно шаблонам отчётных документов Университета ИТМО
Аннотация научно-исследовательской работы	
Отзыв научного руководителя	
График выполнения научно-исследовательской работы	

Задание выдано:

Научный руководитель

  
(подпись)

Лившиц И. И.

(ФИО)

30.09.2022

(дата)

Ответственный за научно-исследовательскую работу

  
(подпись)

Заколдаев Д. А.

(ФИО)

(дата)

Задание принял к исполнению:

  
(подпись)

Конаков А. М.

(ФИО)

30.09.2022

(дата)

**Министерство науки и высшего образования Российской Федерации**  
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**  
**«Национальный исследовательский университет ИТМО»**  
**(Университет ИТМО)**

**О Т З Ы В РУКОВОДИТЕЛЯ**  
**о научно-исследовательской работе студента**

Студент Конаков Александр Михайлович

(Фамилия И. О. полностью)

Факультет БИТ Группа № N4155c

Направление подготовки 10.04.01 Информационная безопасность / Information security

Научный руководитель Лившиц Илья Иосифович, д.т.н., профессор ФБИТ, Университет ИТМО  
(Фамилия И. О., место работы, должность)

Наименование темы: Исследование актуальности обеспечения безопасности критической информационной инфраструктуры Российской Федерации в современных условиях

**ОЦЕНКА НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЫ СТУДЕНТА**

№	Название компетенции	Оценка			
		5	4	3	0*
1	Способность к работе с литературными источниками, справочной и энциклопедической литературой и Интернет-ресурсами	X			
2	Владение иностранными языками, использование иностранных источников		X		
3	Способность к анализу и обобщению информационного материала, степень полноты обзора состояния вопроса	X			
4	Способность порождать новые идеи, предлагать возможные направления и формулировать задачи исследований	X			
5	Владение базовыми знаниями в профессиональной области, способность применять знания на практике	X			
6	Владение исследовательскими навыками, навыками решения технических задач		X		
7	Уровень и корректность использования в работе методов исследований, математического моделирования, инженерных расчётов	X			
8	Владение навыками использования современных пакетов компьютерных программ и технологий		X		
9	Степень комплексности работы, применения в ней знаний естественно-научных, социально-экономических, общепрофессиональных и специальных дисциплин		X		
10	Оригинальность и новизна полученных результатов, научных, конструкторских и технологических решений		X		
11	Наличие публикаций, участие в н.-т. конференциях, награды за участие в конкурсах		X		
12	Качество оформления пояснительной записки (общий уровень грамотности, стиль изложения, качество иллюстраций, соответствие требованиям стандарта к этим документам)	X			
13	Объем и качество выполнения иллюстративного материала (презентации), навыки оформления отчётных материалов с применением современных пакетов программ	X			
14	Степень самостоятельного и творческого участия студента в работе	X			
15	Навыки планирования и управления временем при выполнении работы	X			
ИТОГОВАЯ ОЦЕНКА		5 / отлично			

\* не оценивается (трудно оценить)

Отмеченные достоинства: понимание поставленной задачи,  
(понимание задач, поставленных руководителем, творческая активность при выполнении работы, способность  
подтверждение творческой работы, достаточный  
оценки перспектив развития работы, проявленные способности к организации самостоятельной работы и т.п.)  
обзор литературы.

Отмеченные недостатки: не выявлено

Заключение о возможности продолжения работы (в рамках магистерской подготовки):

подтверждена готовность к продолжению  
работы по согласованному плану.

Студент

Кочаков А.М.  
(подпись)

Научный руководитель

(подпись)

(подпись)



**Министерство науки и высшего образования Российской Федерации**  
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**  
**«Национальный исследовательский университет ИТМО»**  
**(Университет ИТМО)**

**АННОТАЦИЯ НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЫ**

Студент Конаков Александр Михайлович

(Фамилия И. О. полностью)

Факультет БИТ Группа № N4155c

Направление подготовки 10.04.01 Информационная безопасность / Information security

Научный руководитель Лившиц Илья Иосифович, д.т.н., профессор ФБИТ, Университет ИТМО

(Фамилия И. О., место работы, должность)

Наименование темы: Исследование актуальности обеспечения безопасности критической информационной инфраструктуры Российской Федерации в современных условиях

**ХАРАКТЕРИСТИКА НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЫ**

1. Цель и задачи работы ☒ Предложены студентом ☐ Сформулированы при участии студента  
☐ Определены руководителем

**2. Обзорная часть работы**

Число использованных источников 18, из них:

	Последние 5 лет	От 5 до 10 лет	Более 10 лет
Отечественных	13	5	
Зарубежных			

Использованные электронные научные базы Elibrary

Другие использованные Интернет-ресурсы <https://fstec.ru>; <https://rdc.grfc.ru>; <https://ec-rs.ru>;

**3. Содержание работы**

В данной научно - исследовательской работе представлена актуальность и востребованность выбранной темы направления в области магистерского диссертационного исследования

4. Полученные результаты ☐ Обнаружены новые закономерности/разработаны новые методы  
☒ Подготовлена база для дальнейших исследований/разработок  
☐ Другое

**5. Работа выполнена в рамках действующей НИР?**

☒ Да ☐ Нет

Исследование актуальности обеспечения безопасности критической информационной инфраструктуры Российской Федерации в современных условиях

(Наименование НИР)

**6. Публикации и выступления на конференциях по теме НИР**

1)

(библиографические описания)

2)

Студент

Научный руководитель

(подпись)

(подпись)