Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра защиты информации

**“УТВЕРЖДАЮ”**

Первый проректор В.В. Янпольский

ДОКУМЕНТ ПОДПИСАН ПРОСТОЙ НЕКВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСЬЮ
31.08.2020
Владелец: Янпольский Василий Васильевич
Срок действия: не ограничен
Адрес хранения электронного документа:
https://ciu.nstu.ru/documents_res/download?id=B440CC1F36911A5256B3DC30A1D599BA

# ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Направление подготовки: 10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль): Информационная безопасность автоматизированных систем критически важных объектов

Квалификация: Специалист по защите информации

Форма обучения: очная

Год начала подготовки по образовательной программе: 2019

Новосибирск 2020

Программа государственной итоговой аттестации (ГИА) составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 10.05.03 Информационная безопасность автоматизированных систем

ФГОС ВО утвержден приказом Минобрнауки России 01.12.16 №1509 (зарегистрирован Минюстом России 20.12.16, регистрационный №44831)

Программа разработана кафедрой защиты информации

Заведующий кафедрой:

к.т.н., доцент А.В. Иванов

Ответственный за образовательную программу:

к.т.н., доцент А.В. Иванов

Программа утверждена на ученом совете факультета автоматики и вычислительной техники, протокол № 7 от 31.08.2020 г.

декан АВТФ:

к.т.н., доцент И.Л. Рева

Программа государственной итоговой аттестации (ГИА) составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 10.05.03 Информационная безопасность автоматизированных систем

ФГОС ВО утвержден приказом Минобрнауки России 01.12.16 №1509 (зарегистрирован Минюстом России 20.12.16, регистрационный №44831)

Программу разработал:

к.т.н., доцент А.В. Иванов _____

Программа обсуждена на заседании
кафедры защиты информации, протокол заседания кафедры №6/1 от 20.06.2019 г.

Заведующий кафедрой:

к.т.н., доцент А.В. Иванов _____

Ответственный за образовательную программу:

к.т.н., доцент А.В. Иванов _____

Программа утверждена на ученом совете факультета автоматики и вычислительной техники, протокол № 7 от 21.06.2019 г.

декан АВТФ:

к.т.н., доцент И.Л. Рева_____

**1 Обобщенная структура государственной итоговой аттестации**

Государственная итоговая аттестация по направлению 10.05.03 Информационная безопасность автоматизированных систем (специализация: Информационная безопасность автоматизированных систем критически важных объектов) включает выпускную квалификационную работу (ВКР).

Обобщенная структура государственной итоговой аттестации (ГИА) приведена в таблице 1.1.

Таблица 1.1 - Обобщенная структура ГИА

| Коды | Компетенции | ГЭ | ВКР |
|---|---|---|---|
| **ОК.1** | способность использовать основы философских знаний для формирования мировоззренческой позиции | | + |
| **ОК.2** | способность использовать основы экономических знаний в различных сферах деятельности | | + |
| **ОК.3** | способность анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма | | + |
| **ОК.4** | способность использовать основы правовых знаний в различных сферах деятельности | | + |
| **ОК.5** | способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики | | + |
| **ОК.6** | способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия | | + |
| **ОК.7** | способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности | | + |
| **ОК.8** | способность к самоорганизации и самообразованию | | + |
| **ОК.9** | способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности | | + |
| **ОПК.1** | способность анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач | | + |
| **ОПК.2** | способность корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники | | + |
| **ОПК.3** | способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности | | + |

| | | | |
|---|---|---|---|
| **ОПК.4** | способность понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах | | + |
| **ОПК.5** | способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами | | + |
| **ОПК.6** | способность применять нормативные правовые акты в профессиональной деятельности | | + |
| **ОПК.7** | способность применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций | | + |
| **ОПК.8** | способность к освоению новых образцов программных, технических средств и информационных технологий | | + |
| **ПК.1** | способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке | | + |
| **ПК.2** | способность создавать и исследовать модели автоматизированных систем | | + |
| **ПК.3** | способность проводить анализ защищенности автоматизированных систем | | + |
| **ПК.4** | способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы | | + |
| **ПК.5** | способность проводить анализ рисков информационной безопасности автоматизированной системы | | + |
| **ПК.6** | способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности | | + |
| **ПК.7** | способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ | | + |
| **ПК.8** | способность разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем | | + |
| **ПК.9** | способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности | | + |
| **ПК.10** | способность применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности | | + |
| **ПК.11** | способность разрабатывать политику информационной безопасности автоматизированной системы | | + |
| **ПК.12** | способность участвовать в проектировании системы управления | | + |

| | | | |
|---|---|---|---|
| | информационной безопасностью автоматизированной системы | | |
| **ПК.13** | способность участвовать в проектировании средств защиты информации автоматизированной системы | | + |
| **ПК.14** | способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации | | + |
| **ПК.15** | способность участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем | | + |
| **ПК.16** | способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации | | + |
| **ПК.17** | способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации | | + |
| **ПК.18** | способность организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности | | + |
| **ПК.19** | способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы | | + |
| **ПК.20** | способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности | | + |
| **ПК.21** | способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем | | + |
| **ПК.22** | способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации | | + |
| **ПК.23** | способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа | | + |
| **ПК.24** | способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности | | + |
| **ПК.25** | способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций | | + |
| **ПК.26** | способность администрировать подсистему информационной безопасности автоматизированной системы | | + |
| **ПК.27** | способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы | | + |
| **ПК.28** | способность управлять информационной безопасностью | | + |

| | | | |
|---|---|---|---|
| | автоматизированной системы | | |
| **ПК.29.В** | Способность осуществлять проектную деятельность на всех этапах жизненного цикла проекта | | + |
| **ПСК.3.1** | способность проводить оценку эффективности средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов | | + |
| **ПСК.3.2** | способность участвовать в разработке, осуществлять внедрение и эксплуатацию средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов | | + |
| **ПСК.3.3** | способность применять современную нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов | | + |
| **ПСК.3.4** | способность разрабатывать технические регламенты для различных видов деятельности по обеспечению информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов | | + |
| **ПСК.3.5** | способность проектировать, внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов | | + |

## 3 Содержание и порядок организации защиты выпускной квалификационной работы

### 3.1 Содержание выпускной квалификационной работы

3.1.1 Выпускная квалификационная работа (ВКР) представляет собой выполненную обучающимся работу, демонстрирующую уровень подготовленности выпускника к самостоятельной профессиональной деятельности.

3.1.2 ВКР имеет следующую структуру:

- задание на выпускную квалификационную работу,
- аннотация,
- содержание (перечень разделов),
- введение (включающее актуальность выбранной тематики),
- цели и задачи исследования,
- теоретическую и практическую часть,
- место работы в комплексной защите объекта информатизации,
- заключение,
- список использованных источников,
- приложения (при необходимости).

### 3.2 Порядок защиты выпускной квалификационной работы

3.2.1 Порядок защиты ВКР определяется действующим Положением о государственной итоговой аттестации выпускников федерального государственного бюджетного образовательного учреждения высшего образования «Новосибирский государственный технический университет» по образовательным программам, реализуемым в соответствии с федеральными государственными образовательными стандартами высшего образования.

3.2.2 Защита выпускной квалификационной работы проводится на заседании государственной экзаменационной комиссии.

3.2.3 Методика и критерии оценки ВКР приведены в фонде оценочных средств ГИА.

## 4 Список источников для подготовки к государственной итоговой аттестации

### 4.1 Основные источники

Бабаш А.В. Криптографические методы и средства информационной безопасности / А.В. Бабаш, Е.К.Баранова. - М.: РГСУ, 2010.

Гультяева Т. А. Основы теории информации и криптографии / Т.А. Гультяева. - Новосибирск: Изд-во НГТУ, 2010.

Минеев М. П., Чубариков В. Н. Лекции по арифметическим вопросам криптографии . - М.: Изд-во ≪Попечительский совет Механико-математического факультета МГУ им. М. В. Ломоносова≫, 2010.

Токарева Н.Н. Симметричная криптография. Краткий курс. - Новосибирск: Изд-во Новосиб. гос. ун-та, 2012.

Рябко Б. Я., Фионов А.Н. Криптографические методы защиты информации. - М.: Горячая линия-Телеком, 2010.

Концепция организационно-управленческого аудита. С.А. Потемкин, Т.А. Ларина, 2015г.

Противодействия атакам на популярные сетевые сервисы. С.Е. Линник, И.Л. Рева, Новосибирский государственный технический университет, 2015г.

Моделирование и прогнозирование количества инцидентов в системе информационной безопасности при помощи динамической модели. Новосибирский государственный технический университет. А.Ж. Абденов, Р.Н. Заркумова, 2012г.

Законодательное регулирование распространения информации в сети интернет. О.Ф. Бойкова, 2015г.

О формировании системы международной информационной безопасности. Д. Грибков, 2015г.

Информационная безопасность. Ю. Ю. Громов, 2014г.

Информационная безопасность. А.С. Курлаев, Новосибирский государственный технический университет, 2012г.

Муханин Л. Г. Схемотехника измерительных устройств : [учебное пособие для вузов по направлению подготовки 200100 "Приборостроение" и специальности 200101 "Приборостроение"] / Л. Г. Муханин. - СПб. [и др.], 2009. - 281 с. : ил.

Иванов А. В. Техническая защита информации [Электронный ресурс] : электронный учебно-методический комплекс / А. В. Иванов, В. А. Трушин, И. Л. Рева ; Новосиб. гос. техн. ун-т. - Новосибирск, [2014]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000208799. - Загл. с экрана.

### 4.2 Дополнительные источники

Шеннон К. Теория связи в секретных системах // К. Шеннон Работы по теории информации и кибернетике // М.: ИЛ, 1963. С. 333-369.

Борисенко Н. П. Криптографические методы защиты информации / Н.П. Борисенко, А. В. Гусаров, В. И. Милашенко, С. В. Можин. - Орел: Академия ФСО России, 2007.

Жданов О. Н. Криптоанализ классических шифров / О.Н. Жданов, И.А. Куденкова. - Красноярск: Изд-во Сиб. гос. аэрокосм. ун-та им. акад. М.Ф. Решетнева, 2008.

Зубов А. Ю. Криптографические методы защиты информации. Совершенные шифры. - М.: Гелиос АРВ, 2005.

Минин И. В. Криптографические методы защиты информации / И.В. Минин. - Новосибирск: Изд-во НГТУ, 2009.

Мао В. Современная криптография: теория и практика. - М.: Вильямс, 2005.

Осипян В. О. Криптография в задачах и упражнениях. - М.: Гелиос АРВ, 2004.

Основы информационной безопасности: [учебное пособие для вузов по специальностям "Компьютерная безопасность" и др.]. С.П. Расторгуев, 2007г.

Правовое обеспечение информационной безопасности. С.Я. Казанцев, 2005г.

Информационная защита ПК. Михаэль А. Бэнкс, 2001г.

Модели безопасности компьютерных систем. П.Н. Девянин, 2005г.

Информационная безопасность. В.И. Ярочкин, 2004г.

Лицензирование и сертификация в области защиты информации. А.А. Снытников, 2003г.

Комплексная система защиты информации на предприятии. В.Г. Грибунин, В.В. Чудовский, 2009г.

Информационная безопасность и защита информации. В.П. Мельников, С.А. Клейменов, А.М. Петраков, 2009г.

Стандарты информационной безопасности : курс лекций : учебное пособие для студентов вузов, обучающихся по специальностям в области информационных технологий. В. А. Галатенко, 2006г.

О новой редакции Стандарта Банка России "Обеспечение информационной безопасности организаций банковской системы. Общие положения" А. П. Курило, Деньги и кредит, 2009г.

Бизин А. Т. Введение в цифровую обработку сигналов : учебное пособие / А. Т. Бизин ; Сиб. гос. ун-т телекоммуникаций и информатики. - Новосибирск, 1998. - 52 с. : ил., табл.

Быков В. В. Основы цифровой обработки сигналов : учебное пособие / В. В. Быков ; Воронежский политехнический институт. - Воронеж, 1985. - 73 с. : ил.

Баскаков С. И. Радиотехнические цепи и сигналы : Учебник для вузов по спец. "Радиотехника". - М., 2003. - 462 с. : ил.

Солонина А.И., Арбузов С.М. Цифровая обработка сигналов. Моделирование в MATLAB. БХВ-Петербург, 2008.- 814с.

Зайцев А. П. Технические средства и методы защиты информации : лабораторный практикум : учебное пособие / А. П. Зайцев, А. А. Шелупанов. - Томск, 2005. - 119 с. : ил.

Хорев А. А. Техническая защита информации. В 3 т.. Т. 1 : [учебное пособие для вузов по специальностям в области информационной безопасности] / А. А. Хорев ; Моск. гос. ин-т электрон. техники (техн. ун-т). - М., 2008. - 435 с. : ил., табл.

Торокин А. А. Инженерно-техническая защита информации : учебное пособие для вузов по специальностям в области информационной безопасности / А. А. Торокин. - М., 2005. - 958, [1] с. : ил., табл.

Вернигоров Н. С. Особенности устройств съема информации и методы их блокировки : [учебное пособие] / Н. С. Вернигоров. - Томск, 2006. - 119 с. : ил.

Волович Г. И. Схемотехника аналоговых и аналого-цифровых электронных устройств / Г. И. Волович. - М., 2007. - 527, [1] с. : ил.. - На обл. авт. не указан.

Гутников В. С. Интегральная электроника в измерительных приборах / В. С. Гутников. - Л., 1974. - 142 с. : ил., табл.

Таненбаум Э. С. Компьютерные сети : [пер. с англ.] / Э. Таненбаум. - СПб. [и др.], 2007. - 991 с. : ил.

Гук М. Ю. Аппаратные средства локальных сетей : энциклопедия : [фундаментальное руководство] / Михаил Гук. - СПб. [и др.], 2002. - 572 с. : ил.

Руссинович М. Внутреннее устройство Microsoft Windows : Windows Serwer 2003, Windows XP и Windows 2000 : мастер-класс ; пер. с англ. / М. Руссинович, Д. Соломон. - М., 2008. - 968, [1] с. : ил.

Олифер В. Г. Сетевые операционные системы : [учебное пособие по направлению "Информатика и вычислительная техника"] / В. Г. Олифер, Н. А. Олифер. - Санкт-Петербург [и др.], 2005. - 538 с. : ил.

Колисниченко Д. Н. Linux. Полное руководство / Д. Н. Колисниченко, Питер В. Аллен. - СПб., 2007. - 777 с. : ил.

Баглай М. В. Конституционное право Российской Федерации : Учеб. для вузов. - М., 2003. - 784 с.

Тихонов В. А. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты : [учебное пособие для вузов по специальностям в области информационной безопасности] / В. А. Тихонов, В. В. Райх. - М., 2006. - 526, [1] с. : ил.

**4.3 Методическое обеспечение**

Методика оценки риска для информационных систем на основе экспертных оценок : учебное пособие / А. Ж. Абденов, С. А. Белкин, Р. Н. Заркумова-Райхель ; Новосибирский государственный технический университет, 2014г.

Васюков В. Н. Введение в теорию сигналов : учебное пособие / В. Н. Васюков ; Новосиб. гос. техн. ун-т. - Новосибирск, 2003. - 91 [1] с.

Основы цифровой обработки сигналов : [учебное пособие по направлению подготовки специалистов 654400 "Телекоммуникации"] / А. И. Солонина [и др.]. - СПб., 2005. - 753 с. : ил.

Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы : [учебное пособие по направлению 552800 - "Информатика и вычислительная техника" по специальностям 220100 - "Вычислительные машины, комплексы, системы и сети", 220200 - "Автоматизированные системы обработки информации и управления" и 220400 - "Программное обеспечение вычислительной техники и автоматизированных систем"] / В. Г. Олифер, Н. А. Олифер. - СПб. [и др.], 2008. - 957 с. : ил.

Северин В. А. Правовое обеспечение информационной безопасности предприятия : Учеб.-практ. пособие. - М., 2000. - 192 с.

Правовое обеспечение информационной безопасности : учебное пособие для вузов по специальностям: 075200 - Компьютерная безопасность, 075500 - Комплексное обеспечение информационной безопасности автоматизированных систем, 075600 - Информационная безопасность телекоммуникационных систем / [Казанцев С. Я. и др.] ; под ред. С. Я. Казанцева. - М., 2005. - 238, [1] с. : ил.

Трушин В. А. Защита речевой информации от утечки по акустическим и виброакустическим каналам : учебное пособие / В. А. Трушин ; Новосиб. гос. техн. ун-т. - Новосибирск, 2006. - 39, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000059953

Быков С. В. Защита информации от утечки по каналам побочных электромагнитных излучений (ПЭИТ) : учебно-методическое пособие / С. В. Быков, В. А. Трушин ; Новосиб. гос. техн. ун-т. - Новосибирск, 2008. - 41, [2] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000084306

Трушин В. А. Защита конфиденциальной информации от утечки по цепям электропитания : учебно-методическое пособие / В. А. Трушин, С. В. Быков ; Новосиб. гос. техн. ун-т. - Новосибирск, 2007. - 34, [1] с. : схемы, табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000077941. - Инновационная образовательная программа НГТУ "Высокие технологии".

Иванов А. В. Защита речевой информации от утечки по акустоэлектрическим каналам : [учебное пособие] / А. В. Иванов, В. А. Трушин ; Новосиб. гос. техн. ун-т. - Новосибирск, 2012. - 40, [2] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000167975

Иванов А. В. Оценка защищенности информации от утечки по виброакустическим каналам : [учебное пособие] / А. В. Иванов ; Новосиб. гос. техн. ун-т. - Новосибирск, 2018. - 74, [1] с. : ил.

Иванов А. В. Оценка защищенности информации от утечки по каналам побочных электромагнитных излучений и наводок : [учебное пособие] / А. В. Иванов ; Новосиб. гос. техн. ун-т. - Новосибирск, 2018. - 63, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000239355

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра защиты информации

**“УТВЕРЖДАЮ”**

Первый проректор В.В. Янпольский

ДОКУМЕНТ ПОДПИСАН ПРОСТОЙ НЕКВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСЬЮ
31.08.2020
Владелец: Янпольский Василий Васильевич
Срок действия: не ограничен
Адрес хранения электронного документа:
https://ciu.nstu.ru/documents_res/download?id=B440CC1F36911A5256B3DC30A1D599BA

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

# ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Направление подготовки: 10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль): Информационная безопасность автоматизированных систем критически важных объектов

Квалификация: Специалист по защите информации

Форма обучения: очная

Год начала подготовки по образовательной программе: 2019

Новосибирск 2020

| | | |
|---|---|---|
| | | часть;<br>место работы в комплексной защите объекта информатизации |
| **ОК.7 способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности** | | |
| **у4** | уметь логически верно, аргументировано и ясно строить устную и письменную речь в сфере профессиональной деятельности на русском и иностранном языке | теоретическая и практическая часть;<br>место работы в комплексной защите объекта информатизации |
| **ОК.8 способность к самоорганизации и самообразованию** | | |
| **у1** | умеет адекватно оценивать собственный образовательный уровень, свои возможности, способности и уровень собственного профессионализма | теоретическая и практическая часть;<br>место работы в комплексной защите объекта информатизации |
| **ОК.9 способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности** | | |
| **з1** | знать основы здорового образа жизни | теоретическая и практическая часть;<br>место работы в комплексной защите объекта информатизации |
| **ОПК.1 способность анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач** | | |
| **з1** | базовые знания фундаментальных разделов физики в объеме, необходимом для освоения физических основ в области профессиональной деятельности | теоретическая и практическая часть |
| **ОПК.2 способность корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники** | | |
| **з2** | знать базовые положения фундаментальных разделов математики в объеме, необходимом для владения математическим аппаратом для обработки информации и анализа данных в области профессиональной деятельности | теоретическая и практическая часть |
| **ОПК.3 способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности** | | |
| **з1** | знать современные средства разработки и анализа программного обеспечения на языках высокого уровня | теоретическая и практическая часть |
| **ОПК.4 способность понимать значение информации в развитии современного** | | |

| | | |
|---|---|---|
| **общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах** | | |
| **у6** | уметь осуществлять поиск информации в локальных и глобальных сетях | теоретическая и практическая часть |
| **ОПК.5 способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами** | | |
| **у2** | уметь организовать работу по проведению научных исследований в профессиональной деятельности | теоретическая и практическая часть |
| **ОПК.6 способность применять нормативные правовые акты в профессиональной деятельности** | | |
| **у1** | уметь осуществлять реализацию нормативно-правовых актов в сфере профессиональной деятельности | теоретическая и практическая часть |
| **ОПК.7 способность применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций** | | |
| **у1** | владеть законодательными и правовыми основами в области безопасности и охраны окружающей среды, требованиями безопасности технических регламентов в сфере профессиональной деятельности | теоретическая и практическая часть;<br>место работы в комплексной защите объекта информатизации |
| **ОПК.8 способность к освоению новых образцов программных, технических средств и информационных технологий** | | |
| **з2** | знать основные возможности и принципы действия существующих програмных и технических средств защиты информации | теоретическая и практическая часть;<br>место работы в комплексной защите объекта информатизации |
| **ПК.1 способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке** | | |
| **з3** | знать основные источники получения нормативных и методических материалов | теоретическая и практическая часть |
| **ПК.2 способность создавать и исследовать модели автоматизированных систем** | | |
| **у1** | уметь подобрать составляющие элементы автоматизированной системы для реализации поставленных задач | теоретическая и практическая часть |
| **ПК.3 способность проводить анализ защищенности автоматизированных систем** | | |
| **з3** | знать основные программные средства контроля защищенности автоматизированных систем | теоретическая и практическая часть |
| **ПК.4 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы** | | |
| **з2** | знать основные угрозы безопасности информации и модели нарушителя в атоматизированных системах | теоретическая и практическая часть |

| | | |
|---|---|---|
| **ПК.5 способность проводить анализ рисков информационной безопасности автоматизированной системы** | | |
| **у1** | уметь проводить оценку рисков информационной безопасности | теоретическая и практическая часть; место работы в комплексной защите объекта информатизации |
| **ПК.6 способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности** | | |
| **у1** | уметь сформировать и сопоставить критерии эффективного применения автоматизированной системы | теоретическая и практическая часть; место работы в комплексной защите объекта информатизации |
| **ПК.7 способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ** | | |
| **у2** | уметь формулировать основные положения по результатам работы | Аннотация Введение заключение |
| **ПК.8 способность разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем** | | |
| **з2** | знать нормативные и методические материалы, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем | теоретическая и практическая часть; место работы в комплексной защите объекта информатизации |
| **ПК.9 способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности** | | |
| **з1** | знать требования к автоматизированным системам в защищенном исполнении | теоретическая и практическая часть; место работы в комплексной защите объекта информатизации |
| **ПК.10 способность применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности** | | |
| **у3** | уметь разрабатывать прикладные программы, осуществляющие взаимодействие с базами данных | теоретическая и практическая часть; место работы в комплексной защите объекта информатизации |
| **ПК.11 способность разрабатывать политику информационной безопасности автоматизированной системы** | | |
| **з1** | знать принципы формирования политики | теоретическая и |

| | | |
|---|---|---|
| | информационной безопасности в автоматизированных системах | практическая часть;<br>место работы в комплексной защите объекта информатизации |
| **ПК.12 способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы** | | |
| **з2** | знать методы управления информационной автоматизированной системой | теоретическая и практическая часть;<br>место работы в комплексной защите объекта информатизации |
| **ПК.13 способность участвовать в проектировании средств защиты информации автоматизированной системы** | | |
| **з2** | знать основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации | теоретическая и практическая часть;<br>место работы в комплексной защите объекта информатизации |
| **ПК.14 способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации** | | |
| **з1** | знать методики проверки работоспособности применяемых средств защиты | теоретическая и практическая часть;<br>место работы в комплексной защите объекта информатизации |
| **ПК.15 способность участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем** | | |
| **з1** | организацию работы, нормативные правовые акты и стандарты по сертификации средств защиты информации | теоретическая и практическая часть;<br>место работы в комплексной защите объекта информатизации |
| **ПК.16 способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации** | | |
| **з2** | знать порядок проведения аттестации объектов информатизации по требованиям безопасности информации | теоретическая и практическая часть;<br>место работы в комплексной защите объекта информатизации |
| **ПК.17 способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации** | | |
| **з2** | знать автоматизированную систему как объект | теоретическая и |

| | | |
|---|---|---|
| | информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности | практическая часть; место работы в комплексной защите объекта информатизации |
| **ПК.18 способность организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности** | | |
| **з1** | знать основные организационные и технические мероприятия по ТЗКИ на предприятии | теоретическая и практическая часть; место работы в комплексной защите объекта информатизации |
| **ПК.19 способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы** | | |
| **у1** | уметь администрировать подсистемы безопасности автоматизированных систем | теоретическая и практическая часть; место работы в комплексной защите объекта информатизации |
| **ПК.20 способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности** | | |
| **з1** | знать содержание и порядок деятельности персонала по эксплуатациизащищённых автоматизированных систем и подсистем безопасности автоматизированных систем | теоретическая и практическая часть; место работы в комплексной защите объекта информатизации |
| **ПК.21 способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем** | | |
| **з2** | знать правила аттестации автоматизированных систем с учетом нормативных требований по защите информации | теоретическая и практическая часть; место работы в комплексной защите объекта информатизации |
| **ПК.22 способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации** | | |
| **з1** | знать правила формирования политики информационной безопасности организации | теоретическая и практическая часть; место работы в комплексной защите объекта информатизации |
| **ПК.23 способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа** | | |
| **у1** | уметь контролировать эффективность принятых | теоретическая и |

| | | |
|---|---|---|
| | мер для защиты информации ограниченного доступа | практическая часть;<br>место работы в комплексной защите объекта информатизации |
| **ПК.24 способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности** | | |
| **з1** | знать основы построения информационных систем и формирования информационных ресурсов | теоретическая и практическая часть;<br>место работы в комплексной защите объекта информатизации |
| **ПК.25 способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций** | | |
| **з1** | знать методы и средства контроля эффективности технической защиты информации | теоретическая и практическая часть;<br>место работы в комплексной защите объекта информатизации |
| **ПК.26 способность администрировать подсистему информационной безопасности автоматизированной системы** | | |
| **з3** | знать принципы организации информационных систем в соответствии с требованиями по защите информаци | теоретическая и практическая часть;<br>место работы в комплексной защите объекта информатизации |
| **ПК.27 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы** | | |
| **з1** | знать методы и средства проведения аудита и мониторинга безопасности информационных систем | теоретическая и практическая часть;<br>место работы в комплексной защите объекта информатизации |
| **ПК.28 способность управлять информационной безопасностью автоматизированной системы** | | |
| **з2** | знать основные методы управления информационной безопасностью | теоретическая и практическая часть;<br>место работы в комплексной защите объекта информатизации |
| **ПК.29.В Способность осуществлять проектную деятельность на всех этапах жизненного цикла проекта** | | |

| | | |
|---|---|---|
| **у1** | уметь определять необходимые ресурсы для реализации проектных задач | практическая часть |
| **у2** | уметь организовывать и координировать работу участников проекта | практическая часть |
| **у3** | уметь определять проблему и способы ее решения в проекте | практическая часть |
| **ПСК.3.1 способность проводить оценку эффективности средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов** | | |
| **з1** | знать характеристики основных каналов утечки информации на критически важных объектах | теоретическая и практическая часть; место работы в комплексной защите объекта информатизации |
| **ПСК.3.2 способность участвовать в разработке, осуществлять внедрение и эксплуатацию средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов** | | |
| **з1** | знать средства защиты информации, используемые на критически важных объектах | теоретическая и практическая часть; место работы в комплексной защите объекта информатизации |
| **ПСК.3.3 способность применять современную нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов** | | |
| **з1** | знать современную нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение информационной безопасности критически важных объектов | теоретическая и практическая часть; место работы в комплексной защите объекта информатизации |
| **ПСК.3.4 способность разрабатывать технические регламенты для различных видов деятельности по обеспечению информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов** | | |
| **з1** | знать способы и средства охраны объектов | теоретическая и практическая часть; место работы в комплексной защите объекта информатизации |
| **ПСК.3.5 способность проектировать, внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов** | | |
| **з1** | знать терминологию и системный подход к построению защищенных автоматизированных систем критически важных объектов | теоретическая и практическая часть; место работы в |

| | | |
|---|---|---|
| | | комплексной защите объекта информатизации |

**2.2 Структура выпускной квалификационной работы**

Выпускная квалификационная работа содержит следующие разделы:

- задание на выпускную квалификационную работу,
- аннотация,
- содержание (перечень разделов),
- введение (включающее актуальность выбранной тематики),
- цели и задачи исследования,
- теоретическую и практическую часть,
- место работы в комплексной защите объекта информатизации,
- заключение,
- список использованных источников,
- приложения (при необходимости).

**2.3 Методика оценки выпускной квалификационной работы**

2.3.1 Выпускная квалификационная работа оценивается на заседании ГЭК. Члены ГЭК оценивают содержание работы и ее защиту, включающую доклад и ответы на вопросы, по критериям, приведенным в разделе 2.4.

2.3.2 Согласованная итоговая оценка выставляется на основании оценок членов ГЭК с учетом оценки руководителя работы. Итоговая оценка по результатам защиты выпускной квалификационной работы выставляется по 100-балльной шкале, по буквенной шкале ECTS и в традиционной форме (в соответствии с действующим Положением о балльно-рейтинговой системе оценки достижений студентов НГТУ).

**2.4 Критерии оценки ВКР**

Критерии оценки выпускной квалификационной работы приведены в таблице 2.4.1. На основании приведенных критериев при оценке ВКР делается вывод о сформированности соответствующих компетенций на разных уровнях.

Таблица 2.4.1

| **Критерии оценки ВКР** | **Уровень сформированности компетенций** | **Диапазон баллов** |
|---|---|---|
| • структура и оформление ВКР полностью соответствует всем предъявляемыми требованиями<br>• исследование проведено глубоко и полно, тема раскрыта<br>• в работе отражены и обоснованы положения, выводы, подтверждены актуальность и значимость работы, аргументация полученных выводов достаточная<br>• отзыв руководителя не содержит замечаний<br>• представление работы в устном докладе полностью отражает полученные результаты, иллюстративный материал отличается наглядностью<br>• ответы на вопросы комиссии сформулированы четко, с достаточной аргументацией и свидетельствуют о полном владении материалом исследования | Продвинутый | 87-100 |
| • структура и оформление ВКР отвечает | Базовый | 73-86 |

| | | |
|---|---|---|
| большинству предъявляемых требований<br>• исследование проведено в полном объеме, тема раскрыта<br>• в работе отражены и обоснованы положения, выводы, подтверждены актуальность и значимость работы, но аргументация полученных выводов не достаточно полная<br>• отзыв руководителя не содержит принципиальных замечаний<br>• представление работы в устном докладе отражает основные полученные результаты, иллюстративный материал отличается наглядностью<br>• ответы на вопросы комиссии сформулированы четко, но с недостаточной аргументацией | | |
| • структура и оформление ВКР отвечает большинству предъявляемых требований<br>• тема исследования раскрыта не достаточно полно<br>• выводы и положения в работе недостаточно обоснованы, не подтверждены актуальность и значимость работы<br>• отзыв руководителя содержит не более двух принципиальных замечаний<br>• в устном докладе представлены основные полученные результаты, но есть недочеты в иллюстративном материале<br>• ответы на вопросы комиссии свидетельствуют о недостаточно полном владении материалом исследования | Пороговый | 50-72 |
| • структура и оформление ВКР не отвечает большинству предъявляемых требований<br>• тема исследования не раскрыта<br>• выводы и положения в работе недостаточно обоснованы, не подтверждены актуальность и значимость работы<br>• отзыв руководителя содержит более двух принципиальных замечаний<br>• представление работы в устном докладе не отражает основные полученные результаты, есть существенные недочеты в иллюстративном материале<br>• ответы на вопросы комиссии свидетельствуют о недостаточном владении материалом исследования | Ниже порогового | 0-50 |

Составитель _____ А.В. Иванов
(подпись)

«____»_____2019 г.