

МИНОБРНАУКИ РОССИИ



Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНЫЙ УНИВЕРСИТЕТ»  
(ФГБОУ ВО «РГГУ»)

Институт информационных наук и технологий безопасности  
Факультет информационных систем и безопасности

## **ПРОГРАММА ВСТУПИТЕЛЬНОГО ЭКЗАМЕНА**

по информационной безопасности (организационно-правовые, организационно-технические  
и программно-аппаратные средства и меры по защите информации)  
на магистерскую программу 10.04.01 Информационная безопасность  
«Организация и технологии защиты государственной тайны»

Москва 2024

## ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Настоящая программа вступительного экзамена на магистерскую программу «Организация и технологии защиты государственной тайны» отражает современное состояние данного научного направления и включает важнейшие разделы, знание которых необходимо для поступления на эту программу.

Исторический опыт показывает, что система защиты секретов – это наиболее сильное звено государственного опосредования общественных отношений в информационной сфере. Сведения, составляющие государственную тайну, имеют особую важность для общества и государства. Вследствие величины возможного ущерба от ее разглашения государственная тайна занимает приоритетное место в системе социального института тайн.

Экспоненциально растущий объём обрабатываемых данных показывает рост требований к защите информации, в первую очередь, информации ограниченного распространения. Особые требования предъявляются к защите информации, составляющей государственную тайну с учетом современных тенденций и технологий. Это выдвигает новые задачи как перед руководителями организаций (учреждений), перед специалистами в этой области, так и перед сотрудниками отделов по защите государственной тайны.

Для эффективного управления процессами защиты информации необходимо:

- изучить особенности правовой и организационной защиты государственной тайны;
- овладеть методами защиты информации и управления информационной безопасностью;
- овладеть технологиями инженерно-технической, программно-аппаратной и криптографической защитой информации с учетом нормативных документов в области защиты государственной тайны.

Поступающий на данную магистерскую программу должен не только владеть необходимым объёмом знаний в рамках вузовской подготовки специалистов и бакалавров в области информационной безопасности, но и уметь разбираться в теоретических подходах к решению задач по защите информации, в том числе составляющей государственную тайну.

В основу программы положены следующие вузовские дисциплины:

«Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Аппаратные средства вычислительной техники», «Сети и системы передачи информации», «Базы данных, системы управления базами данных», «Основы управления информационной безопасностью», «Гуманитарные аспекты информационной безопасности».

## СОДЕРЖАНИЕ ПРОГРАММЫ

### *1. Основы информационной безопасности*

Понятие и сущность информационной безопасности современного общества. Доктрина информационной безопасности Российской Федерации. Понятия «информация», «сообщение», «сведения», «документированная информация», «информационные технологии», «информационные системы». Способы и средства документирования информации, возникающие угрозы. Информация как предмет защиты. Понятие и сущность информационной безопасности объекта. Понятие уязвимости информации. Формы и виды проявления уязвимости информации.

### *2. Правовая защита информации*

Особенности правовой защиты государственной тайны. Определение понятия государственной тайны. Правовые основы защиты государственной тайны. Понятие о перечнях сведений, составляющих государственную тайну. Принципы и порядок отнесения сведений к государственной тайне. Степени секретности сведений. Порядок распоряжения сведениями, составляющими государственную тайну. Особенности передачи сведений, составляющих государственную тайну, другим государствам. Ограничение прав обладателя информации, в связи с ее засекречиванием. Органы по защите государственной тайны и их полномочия. Контроль и надзор за обеспечением защиты государственной тайны. Уголовно-правовая защита информации, составляющей государственную тайну.

Особенности правовой защиты служебной тайны. Определение понятия служебной тайны. Правовые основы защиты служебной тайны. Виды информации, относящейся к служебной тайне. Меры по охране конфиденциальности информации ограниченного доступа, переданной в государственные органы юридическими и физическими лицами. Полномочия руководителя федерального органа в отношении использования собственной служебной тайны.

### *3. Организационная защита информации.*

Организация работы по определению состава, засекречиванию и рассекречиванию конфиденциальной информации. Установление и изменение степени ограничения доступа сведений, содержащихся в работах, документах и изделиях. Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности. Присвоение и изменение грифа секретности работам, документам и изделиям. Понятие «рассекречивание сведений». Основания для рассекречивания сведений, документов и изделий.

Лицензирование деятельности предприятия по проведению работ, связанных с использованием сведений, составляющих государственную тайну. Основные цели, задачи, функции уполномоченных органов по ведению лицензионной деятельности. Порядок лицензирования деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны. Организация и проведение специальных экспертиз предприятий. Порядок рассмотрения заявлений предприятий о выдаче лицензии. Основания для выдачи (отказе) в выдаче лицензии, приостановлении действия или о ее аннулировании. Порядок проведения государственной аттестации руководителей предприятий.

Порядок сертификации средств защиты информации. Участники сертификации и их функции. Виды средств защиты информации, подлежащих сертификации. Порядок проведения сертификации средств защиты информации. Понятие о сертификате соответствия и знаках соответствия СЗИ-ГТ. Инспекционный контроль.

Порядок допуска и доступа персонала и иных лиц к конфиденциальной информации. Допуск должностных лиц и граждан к государственной тайне. Основания для отказа или

прекращения допуска. Ограничение прав. Переоформление допуска. Назначение и формы допусков к государственной тайне, порядок оформления и учета. Особенности доступа к конфиденциальной информации. Назначение, принципы и задачи разрешительной системы доступа к информации ограниченного доступа. Порядок оформления разрешения на доступ. Особенности доступа к информации лиц, командированных из других предприятий.

#### *4. Инженерно-техническая защита информации*

Классификация демаскирующих признаков по характеристикам объектов и информативности. Мера информативности признака. Понятие об эталонной и текущей признаковых структурах. Принципы инженерно-технической защиты информации и построения ее системы. Назначение и типы контролируемых зон. Классификация и сущность методов инженерно-технической защиты информации. Основные показатели эффективности инженерно-технической защиты информации. Назначение и виды физической защиты источников информации. Принципы работы системы контроля управления доступом. Способы и средства нейтрализации угроз. Принципы нейтрализации угроз в автономных и централизованных системах охраны. Основные этапы и показатели проектирования системы инженерно-технической защиты информации. Принципы оценки показателей. Мероприятия по выявлению каналов утечки информации. Специальные проверки. Цель и способы проведения.

#### *5. Средства и системы обработки, хранения и передачи информации*

Системы счисления – позиционная и непозиционная, двоичная, десятичная, шестнадцатеричная. Структура современного компьютера. Виды машинных носителей информации.

Понятия информационной и автоматизированной системы. Различие между информационной и автоматизированной системами. Основные компоненты автоматизированной системы. Виды обеспечения автоматизированных систем.

Понятие сетей связи, их структура. Семиуровневая модель взаимодействия открытых систем ISO/OSI. Понятие протокола и стека протоколов. Назначение уровней модели ISO/OSI. Адресация в IP-сетях. MAC-адреса, IP-адреса, номера портов. Символьные имена в IP-сетях.

#### *6. Базы данных, системы управления базами данных*

Понятия «база данных», «система управления базами данных», «схема базы данных». Виды связей. Типы бинарных связей. Реляционные базы данных, объекты реляционной БД. ; Нормализация. Классы отношений. Нормальные формы от первой до третьей. Нормальная форма Бойса-Кодда. Четвёртая нормальная форма. Доменно-ключевая нормальная форма. Приложения БД. Функции приложения базы данных. Многопользовательские базы данных. Администрирование баз данных. Управление параллельной обработкой

#### *7. Комплексная система защиты информации (КСЗИ) на предприятии*

Сущность, задачи и принципы функционирования комплексной системы защиты информации. Сущность и основные этапы организационного проектирования комплексной системы защиты информации. Понятие и сущность управления комплексной системой защиты информации. Сущность и содержание контроля эффективности комплексной системы защиты информации. Методы принятия управленческих решений в комплексной системе защиты информации. Кадровое и ресурсное обеспечение защиты информации.

## КРИТЕРИИ ОЦЕНИВАНИЯ ОТВЕТОВ

(отлично)	Абитуриент показывает прочные знания по вопросам программы, ответ отличается глубиной и полнотой; уверенное владение понятийным аппаратом; умение объяснять сущность информационных процессов, делать выводы и обобщения, давать аргументированные ответы на дополнительные вопросы, приводит примеры; свободное владение речью, логичность и последовательность ответа.
(хорошо)	Абитуриент демонстрирует достаточные знания по вопросам программы, ответ полный; владение понятийным аппаратом; умение объяснять сущность информационных процессов, делать выводы и обобщения, давать аргументированные ответы на дополнительные, приводит примеры; свободное владение речью, логичность и последовательность ответа. Допускается одна - две неточности в ответе.
(удовлетворительно)	Абитуриент даёт ответ, свидетельствующий в основном о знании вопросов программы, отличающийся недостаточной глубиной и полнотой; знает основные вопросы теории; навыки анализа информационных процессов сформированы слабо, показывает недостаточное умение давать аргументированные ответы и приводить примеры; демонстрирует недостаточно свободное владение речью, недостаточную логичность и последовательность ответа. Допускается несколько ошибок в содержании ответа.
(неудовлетворительно)	Ответ обнаруживает незнание вопросов программы, отличается неглубоким и неполным раскрытием темы, незнанием основных вопросов теории, несформированными навыками анализа информационных процессов; абитуриент не умеет давать аргументированные ответы на дополнительные вопросы, слабо владеет речью, демонстрирует отсутствие логичности и последовательности. Имеются серьезные ошибки в содержании ответа.

## СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

Закон Российской Федерации от 21.07.93 № 5485-1 “О государственной тайне”, Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_2481/](http://www.consultant.ru/document/cons_doc_LAW_2481/)

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_61798/](http://www.consultant.ru/document/cons_doc_LAW_61798/)

Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_48699/](http://www.consultant.ru/document/cons_doc_LAW_48699/)

Федеральный закон от 28.12.2010 №390-ФЗ «О безопасности», Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_108546/](http://www.consultant.ru/document/cons_doc_LAW_108546/)

Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности», Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_113658/](http://www.consultant.ru/document/cons_doc_LAW_113658/)

Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных», Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_61801/](http://www.consultant.ru/document/cons_doc_LAW_61801/)

Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании», Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_40241/](http://www.consultant.ru/document/cons_doc_LAW_40241/)

Указ Президента Российской Федерации от 06.03.97 № 188 “Об утверждении перечня сведений конфиденциального характера”, Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_13532/](http://www.consultant.ru/document/cons_doc_LAW_13532/)

Постановление Правительства Российской Федерации от 15.04.1995 № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны», Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_6387/](http://www.consultant.ru/document/cons_doc_LAW_6387/)

Постановление Правительства РФ от 07.02.2024 N 132 "Об утверждении Правил допуска должностных лиц и граждан Российской Федерации к государственной тайне", Режим доступа: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=469293&cacheid=90BDBC698EAD34A8849E89AE3AE2A61C&mode=splus&rnd=0.8756444116227469#z2fvd4US9Fqz4KZq>

Постановление Правительства Российской Федерации от 03.11.94 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти», Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_54870/](http://www.consultant.ru/document/cons_doc_LAW_54870/)

**Машинно-ориентированное программирование:** Учебное пособие / Абрамов Е.С., Сидоров И.Д. – Таганрог: Южный федеральный университет, 2016. – 87 с.: ISBN 978-5-9275-2065-7 - Режим доступа: <http://znanium.com/catalog/product/991870>

**Программные и аппаратные средства информатики** / Царев Р.Ю., Прокопенко А.В., Князьков А.Н. – Краснояр.: СФУ, 2015. – 160 с.: ISBN 978-5-7638-3187-0 - Режим доступа: <http://znanium.com/catalog/product/550017>

**Таненбаум Э., Бос Х.** Современные операционные системы. 4-е изд. – СПб.: Питер, 2015. – 1120 с.: ил. – (Серия «Классика computer science»)

**Олифер В., Олифер Н.** Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. – СПб.: Питер, 2016. – 992 с.: ил. – (Серия «Учебник для вузов»).

**Теория и практика построения баз данных. 8-е изд.** / Д. Крёмке. – СПб.: Питер, 2003. — 800 с: ил. – (Серия «Классика computer science»).

**Базы данных: Учебник** / Шустова Л.И., Тараканов О.В. – М.:НИЦ ИНФРА-М, 2016. – 304 с.: – Режим доступа: <http://znanium.com/catalog/product/491069>.

**Базы данных и системы управления базами данных: Учебное пособие** / Лазицкас Е.А., Загумённикова И.Н., Гилевский П.Г. – Мн.:РИПО, 2016. – 268 с.: ISBN 978-985-503-558-0 - Режим доступа: <http://znanium.com/catalog/product/946561>

**Защита информации ограниченного доступа от утечки по техническим каналам:** Справочное пособие / Бузов Г.А. – Москва :Гор. линия-Телеком, 2015. – 586 с.: 60x90 1/16 (Обложка) ISBN 978-5-9912-0424-8 - Текст : электронный. - URL: <https://new.znanium.com/catalog/product/895240>

**Ельчанинова, Н.Б. Правовые основы защиты информации с ограниченным доступом:** учебное пособие / Н.Б. Ельчанинова ; Южный федеральный университет. - Ростов-на-Дону - Таганрог : Издательство Южного федерального университета, 2017. - 76 с. - ISBN 978-5-9275-2501-0. - Текст : электронный. - URL: <https://new.znanium.com/catalog/product/1021578>

**Баринов А.В. Организационное проектирование:** Учебник. - Москва : ООО "Научно-издательский центр ИНФРА-М", 2015. - 384 с. - ISBN 978-5-16-010992-3. -Режим доступа: <http://znanium.com/go.php?id=492911>. –С. 126-178.

**Капгер И.В. Программно-аппаратные средства защиты информации** – Пермь: Изд-во Перм.нац. исслед. политехн. ун-та, 2022 – 223с.

**Жарова, А.К. Правовое регулирование создания и использования информационной инфраструктуры в Российской Федерации:** монография / А. К. Жарова. — Москва : Издательство Юрайт, 2022. — 301 с. // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/496939>

**Организационное и правовое обеспечение информационной безопасности:** учебник и практикум для вузов/ под редакцией Т. А. Поляковой, А.А. Стрельцова.— Москва : Издательство Юрайт, 2022.— 325 с. // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/498844>