МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Самарский государственный технический университет»
(ФГБОУ ВО «СамГТУ»)

УТВЕРЖДАЮ
Ректор ФГБОУ ВО «СамГТУ»,
д.т.н., профессор

_____ Д. Е. Быков
«27» ____12_____ 2024 г.

ПРОГРАММА ВСТУПИТЕЛЬНОГО ЭКЗАМЕНА
в аспирантуру СамГТУ

по научной специальности

2.3.6. Методы и системы защиты информации, информационная безопасность

Самара 2024

1. ОБЩИЕ ПОЛОЖЕНИЯ

К вступительным испытаниям по программам подготовки научных и научно-педагогических кадров в аспирантуре СамГТУ допускаются лица, имеющие образование не ниже высшего (специалитет или магистратура).

Прием осуществляется на конкурсной основе по результатам вступительных испытаний.

2. ЦЕЛЬ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

Вступительные испытания призваны определить степень готовности поступающего к освоению основной образовательной программы аспирантуры по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

3. ФОРМА ПРОВЕДЕНИЯ И КРИТЕРИИ ОЦЕНКИ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

Вступительное испытание проводится в письменной форме в соответствии с установленным приемной комиссией СамГТУ расписанием.

Поступающему предлагается ответить письменно на вопросы и (или) решить задачи в соответствии с экзаменационными заданиями, которые охватывают содержание разделов и тем программы вступительных испытаний. Для подготовки ответа поступающие используют экзаменационные листы, которые впоследствии хранятся в их личном деле.

При приеме на обучение по программам подготовки научных и научно-педагогических кадров в аспирантуре результаты каждого вступительного испытания оцениваются **по пятибалльной шкале.**

Минимальное количество баллов для каждой научной специальности, подтверждающее успешное прохождение вступительного испытания, составляет **3 балла**.

Шкала оценивания:

«Отлично» – выставляется, если поступающий представил развернутые, четкие ответы на основные вопросы экзаменационного билета.

«Хорошо» – выставляется, если поступающий представил относительно развернутые, четкие ответы на основные вопросы экзаменационного билета;

«Удовлетворительно» – выставляется, если поступающий представил относительно развернутые, четкие ответы на основные вопросы экзаменационного билета, при этом некоторые ответы раскрыты не полностью;

«Неудовлетворительно» – выставляется, если при ответе поступающего основные вопросы билета не раскрыты.

4. ПЕРЕЧЕНЬ РАЗДЕЛОВ, ТЕМ И СПИСОК ЛИТЕРАТУРЫ

РАЗДЕЛ 1. МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1.1 Сущность и общие задачи защиты информации

Понятие и сущность защиты информации (ЗИ). Назначение ЗИ, цели ЗИ. Задачи ЗИ. Основные факторы, влияющие на организацию ЗИ: организационно-правовая форма и характер основной деятельности предприятия(организации), состав, объем и степень конфиденциальности защищаемой информации; структура и территориальное расположение предприятия4 режим функционирования предприятия; технологии обработки, хранения и передачи информации, степень их автоматизации. Характер и степень влияния различных факторов на организацию ЗИ. Общие требования, предъявляемые к ЗИ. Унифицированная концепция построения систем ЗИ.

1.2 Определение состава защищаемой информации и объектов защиты

Методика определения состава защищаемой информации. Этапы работ по выявлению состава защищаемой информации. Функции руководства предприятия и подразделений предприятия, экспертной комиссии, службы защиты информации. Нормативное закрепление состава защищаемой информации; структура перечня сведений, относимых к различным видам тайны.

Носители информации как объекты защиты. Факторы, определяющие состав носителей информации. Методика выявления состава носителей защищаемой информации. Хранилища носителей информации как объект защиты. Особенности помещений для работы с защищаемой информацией как объектов защиты. Состав технических средств обработки, хранения, передачи и защиты информации, являющихся объектами защиты.

Локальная вычислительная сеть как объект защиты. Корпоративная информационная система (КИС) предприятия как объект защиты. КИС как открытая система. Технология Интернет и Интернет как факторы, влияющие на защиту информации в КИС. Корпоративные порталы. Персонал предприятия как объект защиты.

1.3 Анализ и оценка угроз безопасности защищаемой информации

Классификация различных видов и источников угроз. Угрозы экономической безопасности. Угрозы физической безопасности. Угрозы информационной безопасности. Угрозы материальной безопасности. Определение причин, обстоятельств и условий дестабилизирующего воздействия на информацию. Оценка ущерба от потенциального дестабилизирующего воздействия (угрозы) на информацию.

Методика выявления каналов утечки и методов НСД к защищаемой информации. Оценка потенциальных последствий реализации НСД. Определение направлений и возможностей доступа нарушителей к защищаемой информации. Общая возможных злоумышленных действий в автоматизированной системе обработки данных (АСОД). Взаимосвязь объектов защиты, возможных проявлений злоумышленных действий и подразделений службы безопасности предприятия. Понятие зоны защиты, рубежей защиты. Семирубежная модель защиты.

Методология оценки уязвимости (защищенности) информации. Система показателей уязвимости (защищенности). Примеры постановки задач оценки уязвимости защищаемой информации в АСОД.

Понятие стратегии ЗИ, Ситуация (среда) ЗИ - потребности в защите - требуемый уровень ЗИ - ресурсы на ЗИ. Оборонительная, наступающая и упреждающая стратегии ЗИ. Функции защиты информации. Основные требования к выводу множества функций защиты. Структура и содержание множества функций обеспечения ЗИ.

Определение перечня и содержания задач ЗИ. Классификация задач ЗИ. Формирование репрезентативного множества задач ЗИ. Введение избыточности элементов системы. Регулирование доступа к элементам системы. Регистрация сведений. Уничтожение избыточной информации. Реагирование.

1.4 Методы и средства ЗИ

Формальные и не формальные методы и средства ЗИ. Общая характеристика различных методов и классов средств ЗИ. Технические, программные, программно-аппаратные, криптографические, организационные, законодательные (нормативно-правовые), морально-этические (психологические) средства ЗИ,

Общие требования, предъявляемые к построению СЗИ. Комплексность ЗИ. Уровни защиты (категории СЗИ), их влияние на выбор стратегии ЗИ. Рекомендуемые типы СЗИ: пассивные, полуактивные, активные СЗИ. Выбор уровня и типа СЗИ в зависимости от типа ЗИ (АСОД). Выбор типовых стандартных проектных решений СЗИ и ее подсистем. Отечественные и зарубежные стандарты в области построения СЗИ. Руководящие документы ГТК при Президенте РФ (Федеральной службы технического и экспортного контроля (ВСТЭК), их роль и место при проектировании КСЗИ.

1.5 Модели и методы оценки защищенности информации

Управление риском. Понятие риска. Принципы управления риском. Оценка степени риска. Цели моделирования ЗИ. Модели систем и процессов ЗИ. Общая модель процесса ЗИ. Оценка уровня защищенности (уязвимости) информации. Общая модель функционирования системы ЗИ. Модель общей оценки угроз информации. Модель оценки защищенности информации в случае злоумышленных действий. Модели анализ систем разграничения доступа к информации. Неформальные методы принятия решений в системах ЗИ. Метод экспертных оценок. Нечеткие алгоритмы принятия решений.

1.6 Проектирование СЗИ. Стандарты в области информационной безопасности

Общая характеристика процесса проектирования СЗИ. Определение условий функционирования СЗИ (объект ЗИ, среда функционирования, требования к системе). Многоуровневая организация СЗИ. Постановка задачи проектирования СЗИ.

Перечень концептуальных документов, важнейших федеральных нормативно-правовых актов и основных подзаконных актов в области защиты информации. Система государственных и отраслевых стандартов в области защиты информации. Нормативные документы ФСТЭК РОССИИ.

Аудит объектов информатизации. Система аудита, порядок проведения аудита. Объекты информатизации, подлежащие оценке соответствия требованиям ЗИ. Сертификация средств ЗИ по требованиям безопасности. Система сертификации, порядок проведения сертификации. Средства ЗИ, подлежащие обязательной сертификации.

1.7 Управление процессами функционирования СЗИ

Архитектура (структура) СЗИ. Автономные, интегрированные, интегральные, интеллектуальные системы ЗИ. Классификационная структура функций ЗИ в АСОД. Управление механизмами ЗИ (макропроцессы управления). Режимы управления. Макрозадачи управления. Разработка планов деятельности (планирование); руководство выполнением планов (оперативно-диспетчерское управление, календарно-плановое руководство); обеспечение повседневной деятельности органов управления СЗИ.

Политика безопасности организаций (предприятия). Уровни политики безопасности, их цели и задачи. План защиты организации. Функциональная схема СЗИ. Правила и положения, определяющие механизмы реализации политики безопасности.

Управление в нештатных ситуациях. Потенциально-аварийные, аварийные и чрезвычайные ситуации, соответствующие действия должностных лиц. Планирование действий в нештатных ситуациях. Отказоустойчивость, катастрофоустойчивость АСОД. Системы поддержки принятия решений, их функции и задачи. Ситуационные центры.

Основная учебная литература

1. Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Основы управления информационной безопасностью. Учебное пособие для вузов. – 2-е изд., испр. – М.: Горячая линия-Телеком, 2019. – 244.: ил.

2. Башлы П.Н. Информационная безопасность и защита информации: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 с.

3. Титов А.А. Инженерно-техническая защита информации: учебное пособие/ А.А. Титов— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, 2010.— 197 с.

4. Шаньгин В.Ф. Информационная безопасность и защита информации / Шаньгин В.Ф.— Электрон. текстовые данные.— М.: ДМК Пресс, 2014.— 702 с.

5. Управление безопасностью : учеб. пособие / Л.П. Гончаренко, Е.С. Куценко; Рос. экон. акад. им. Г.В. Плеханова.- М.: КноРус, 2010. - 272 с.

6. Инженерно-техническая защита информации: Учеб. пособие для вузов / А.А. Торокин.- М.: Гелиос АРВ, 2006. -958 с.

7. Информационное обеспечение управленческой деятельности: учеб. пособие для сред. спец. образования / Е.Е. Степанова, Н.В. Хмелевская.- М.: Форум , 2010. - 191 с.

8. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации. – Форум, 2009. – 256 с.

9. Клейменов С.А., Мельников В.П., Петраков А.М. Информационная безопасность и защита информации: учеб. пособие. – Академия, 2008. – 336 с.

10. Ковалева Н.Н. Информационное право России: учеб. пособие / Н.Н. Ковалева. – М.: Дашков и К, 2007. – 358 с.

11. Краковский Ю.М. Информационная безопасность и защита информации. – ИЦ МарТ ИКЦ МарТ, 2008. – 288 с.

12. Правовое обеспечение информационной безопасности: учебник / [авт.-ред.: В.А. Минаев и др.]. – Изд. 2-е, расш. и доп. – М.: Маросейка, 2008. – 368 с.

13. Программно-аппаратная защита информации [Текст] : учеб. пособие по направлениям "Информ. безопасность" и "Информатика и вычисл. техника" / П.Б. Хорев.- М.: Форум , 2009.-351

14. Организационное обеспечение информационной безопасности : учебник для высш. учеб. заведений по направлению "Информационная безопасность" / О.А. Романов, С.А. Бабин, С.Г. Жданов. - М.: Академия, 2008.-188 с.

15. Теоретические основы компьютерной безопасности: учеб. пособие для вузов по специальности 090100 "Информационная безопасность" / А.А. Грушо, Э.А. Применко, Е.Е. Тимонина. - М.: Академия, 2009. - 267 с.

16. Информационная безопасность и защита информации : учеб. пособие для студентов вузов по направлению 230200 "Информ. системы" специальности 230201 "Информ. системы и технологии" / Ю.Ю. Громов и др. - Старый Оскол: Тонкие наукоемкие технологии, 2010. - 383 с.

17. Тилборг Ван Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник [Текст] / Х.К.А. ван Тилборг ; пер. с англ. Д.С. Ананичева, И.О. Корякова ; под ред. И.О. Корякова. - М.: Мир, 2006.

18. Торстейнсон, П. Криптография и безопасность в технологии. NET [Текст] / П. Торстейнсон, Г. А. Ганеш ; пер. с англ. В.Д. Хорева ; под ред. С.М. Молявко.- М. : Бином. Лаборатория знаний , 2007.-479 с.

19. Фороузан, Б.А. Криптография и безопасность сетей: учеб. пособие / Б.А. Фороузан ; пер. с англ. под ред. А.Н. Берлина.- М.: Интернет-Университет Информационных Технологий: БИНОМ. Лаборатория знаний, 2010. - 783 с.

Дополнительная учебная литература

1. Галатенко В.А. Основы информационной безопасности/ Галатенко В.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2008.— 174 с.

2. ГОСТ Р-50922-2006. Защита информации. Основные термины и определения. М.: Гос-стандарт России, 2006.

3. Аникин П.П., Балыбердин А.Л., Вус М.А. Государственная тайна и ее защита в Российской Федерации: учеб. пособие (под ред. Вуса М.А., Федорова А.В.; предисл. Кропачева Н.М., Сидоровой Н.А.). – Изд. 2-е, перераб., доп. –изд-во Р. Асланова «Юридический Центр-Пресс«, 2005. – 623 с.

4. Правовое обеспечение информационной безопасности: учеб. пособие / под ред. С.Я. Казанцева. – 2-е изд., испр. и доп. – М.: Академия, 2007. – 238 с.

5. Компьютерные вирусы изнутри и снаружи / К. Касперски. .- СПб. и др. : Питер , 2007.-526 с.

6. Шаффер, М. Защита от шума и вибраций в системах ОВК: практ. руководство: пер. с англ. / М. Шаффер.- М.: Авок-Пресс, 2009.-231 с.

7. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. – СПб.: БХВ-Петербург, 2009.-564 с.