МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО «УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

ФАКУЛЬТЕТ ИНФОРМАТИКИ И РОБОТОТЕХНИКИ

ПРИНЯТО
На заседании кафедры вычислительной техники и защиты информации
факультета информатики и робототехники
Протокол от «16» 12 2022 г. № 4

Зав. кафедрой _____ / В.М. Картак

УТВЕРЖДЕНО
Проректор по учебно-методической работе

_____ А.Б. Галимханов
м.п.
«28» 12 2022 г.

УРОВЕНЬ ВЫСШЕГО ОБРАЗОВАНИЯ
ПОДГОТОВКА КАДРОВ ВЫСШЕЙ КВАЛИФИКАЦИИ

ПРОГРАММА
вступительного экзамена по научной специальности
2.3.6. Методы и системы защиты информации, информационная безопасность

Разработчик (разработчики):

_____ / к.т.н., старший преподаватель кафедры ВТиЗИ В.В. Сагитова
(подпись) (ученая степень, ученое звание, должность, фамилия и.о.)

Уфа – 2022

ПРОГРАММА

вступительного испытания по специальной дисциплине при приеме на обучение по образовательной программе высшего образования – программе подготовки научных и научно-педагогических кадров в аспирантуре по научной специальности 2.3.6 Методы и системы защиты информации, информационная безопасность

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.

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.

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 схема 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.

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.

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 анализа систем разграничения доступа к информации. Неформальные методы принятия решений в системах ЗИ. Метод экспертных оценок. Нечеткие алгоритмы принятия решений.

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.

SADT - методология проектирования. ГОСТ 34.601-90 “Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы”. Методология функционального моделирования IDEFO. Иерархия диаграмм. Методология информационного

моделирования IDEF1X. Диаграммы “сущность-связь”. Методология динамического моделирования IDEF/CPN. Сети Петри. Базис построения ИС: CASE - технологии системного моделирования, CALS - технологии.

Стандарты информационной безопасности (ИСО/ИЭК 15408, 17799, 27001, 27005, 13335), СТО БР «Информационная безопасность автоматизированных банковских систем».

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.

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 литература

1.Обеспечение информационной безопасности машиностроительных предприятий : [в 2-х ч.] : [учебник для студентов высших учебных заведений] / С. А. Клейменов [и др.] .— Старый Оскол : ТНТ, Ч. 1 . Ч.2 — 2014 .— 360 с.

2.Шаньгин, В. Ф. Информационная безопасность [Электронный ресурс]: / Шаньгин В.Ф. — Москва: ДМК Пресс, 2014

3.Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : [учебное пособие для студентов учреждений среднего профессионального образования, обучающихся по группе специальностей "Информатика и вычислительная техника"] / В. Ф. Шаньгин .— М. : Форум : Инфра-М, 2013 .— 415, [1] с.

4.Соболев, А. Н. Физические основы перспективной вычислительной техники и обеспечение информационной безопасности : [учебное пособие для студентов высших учебных заведений, обучающихся по специальности "Комплексное обеспечение информационной безопасности автоматизированных систем"] / А. Н. Соболев, В. М. Кириллов, А. В. Киселев .— Москва : Гелиос АРВ, 2012 .— 256 с.

5. Милославская, Н. Г. Вопросы управление информационной безопасностью [Электронный ресурс]: / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. — Москва : Горячая линия-Телеком, 2012 .— "Допущено Учебно-методическим объединением высших учебных заведений России по образованию в области информационной безопасности в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению подготовки 090900 – ""Информационная безопасность""

(уровень - магистр) "

6.Бабаш, А. В. Информационная безопасность. История защиты информации в России : учебное пособие / А. В. Бабаш, Е. К. Баранова, Д. А. Ларин .— Москва : КДУ, 2015 .— 736 с. : ил. ; 21 см.

7.Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : [учебное пособие для студ. вузов, обуч. по спец. 090103 "Организация и технология защиты информации", 090104 "Комплексная защита объектов информатизации"] / В. Я. Ищейнов, М. В. Мецатунян .— 2-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2014 .— 256 с. : ил.

Дополнительная литература

1. Анисимов, А. А. Менеджмент в сфере информационной безопасности : учебное пособие / А. А. Анисимов. – М.: Интернет-Университет Информационных Технологий: БИНОМ. Лаборатория знаний, 2010.

2. Галатенко, В. А. Основы информационной безопасности: учебное пособие / В. А. Галатенко; под ред. В. Б.Бетелина. – М. : ИНТУИТ.РУ, Интернет-университет Информационных Технологий: БИНОМ. Лаборатория знаний, 2008.

3. Грибунин, В. А., Чудовский, В. В. Комплексная система защиты информации на предприятии: учебное пособие / В. А. Грибунин, В. В. Чудовский. – М.: Академия, 2009.

4. Гришина, Н. В. Комплексная система защиты информации на предприятии : [учебное пособие для студентов высших учебных заведений, обучающихся по специальности 090103 "Организация и технология защиты информации" и 090104 "Комплексная защита объектов информации"] / Н. В. Гришина .— Москва : ФОРУМ, 2014 .— 240 с.

5. Садердинов, А. А., Трайнёв, В. А., Федулов, А. А. Информационная безопасность предприятия: учебное пособие / А. А. Садердинов, В. А. Трайнёв, А. А. Федулов. – М.: Дашков и К°, 2005.

6. Романов, О. А. Организационное обеспечение информационной безопасности: учебник / О. А. Романов, С. А. Бабин, С. Г. Жданов. – М.: Академия, 2008.

7. Ярочкин, В. И. Информационная безопасность: учебник / В. И. Ярочкин. – М.: Академический проект; Гаудеамус. – 2000.

Интернет-ресурсы
(электронные учебно-методические издания, лицензионное программное обеспечение)

На сайте библиотеки http://library.ugatu.ac.ru/ в разделе «Информационные ресурсы», подраздел «Доступ к БД» размещены ссылки на интернет – ресурсы.