МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования

**«УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Кафедра вычислительной техники и защиты информации

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ

УЧЕБНОЙ ДИСЦИПЛИНЫ

«КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ»

Уровень подготовки: высшее образование – бакалавриат

Направление подготовки
10.03.01 Информационная безопасность
(код и наименование направления подготовки)

Направленность подготовки (профиль)
Безопасность автоматизированных систем
(наименование профиля подготовки)

Квалификация (степень) выпускника
бакалавр

Форма обучения
очная

Год начала подготовки – 2015

Уфа 2016

Место дисциплины в структуре образовательной программы

Дисциплина «Комплексная система защиты информации на предприятии» является обязательной дисциплиной вариативной части основной профессиональной образовательной программы (ОПОП).

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 090900 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации 28 октября 2009 г. № 496, а также в соответствии с Приказом Министерства образования и науки Российской Федерации от 19 декабря 2013 г. N 1367 г. «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры» и актуализирована в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации 01 декабря 2016 г. № 1515. Является неотъемлемой частью основной профессиональной образовательной программы.

Целью освоения дисциплины является формирование систематизированных знаний о теоретических, методических и технологических основах построения комплексных систем защиты информации на предприятии.

Задачи:

- **с**формировать комплекс базовых теоретических знаний в области комплексных систем защиты информации (КСЗИ);
- **с**формировать и развить компетенции, знания, практические навыки и умения, способствующие всестороннему и эффективному применению современных методов анализа и проектирования комплексных систем защиты информации, включая методы системного моделирования, анализа и управления рисками.

Перечень результатов обучения

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций.

Планируемые результаты обучения по дисциплине:

№	Формируемые компетенции	Код	Знать	Уметь	Владеть
1	Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	ОПК-7	• технологию определения состава защищаемой информации и объектов защиты; • методы анализа и оценки угроз безопасности защищаемой информации	• использовать методы анализа и оценки угроз безопасности защищаемой информации	• навыками определения состава защищаемой информации и объектов защиты; • навыками выявления угроз безопасности защищаемой информации и степени их опасности
2	Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	ПК-4	• мероприятия и условия функционирования КСЗИ	• определять состав защитных мероприятий	• навыками выбора структуры КСЗИ с учетом условий ее функционирования

3	Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	ПК-13	• принципы организации и проектирования КСЗИ; • мероприятия и условия функционирования КСЗИ; • методы анализа эффективности функционирования КСЗИ; • технологию управления КСЗИ	• планировать и реализовать мероприятия по повышению эффективности функционирования КСЗИ	• навыками определения состава кадрового, нормативно-методического и материально-технического обеспечения функционирования КСЗИ; • навыками выбора методов и средств, необходимых для организации и функционирования КСЗИ

Содержание разделов дисциплины

№	Наименование и содержание разделов
1	**Введение в дисциплину.** Предмет и задачи дисциплины. Значение и место дисциплины в подготовке кадров по направлению подготовки 10.03.01 «Информационная безопасность». Структура дисциплины. Разделы и темы дисциплины, их распределение по семестрам и видам аудиторных занятий. Источники и литература по дисциплине. Методика самостоятельной работы студентов по изучению дисциплины. Понятийный аппарат в области обеспечения безопасности информации. Информация как объект защиты. Цели и принципы защиты информации (ЗИ).
2	**Сущность и задачи комплексной системы защиты информации.** Понятие и сущность КСЗИ. Назначение КСЗИ. Задачи, решаемые с помощью КСЗИ. КСЗИ как составная часть комплексной системы безопасности. Предприятие как объект защиты. Система управления информационной безопасностью предприятия. Общие требования, предъявляемые к КСЗИ. Основные факторы, влияние на организацию КСЗИ. Характер и степень влияния различных факторов на организацию КСЗИ. Унифицированная концепция ЗИ.
3	**Определение состава защищаемой информации и объектов.** Структура и основные компоненты объектов информатизации. Объекты защиты. Методика определения состава защищаемой информации. Этапы работ по выявлению состава защищаемой информации. Функции руководства и подразделений предприятия в области защиты информации. Нормативное закрепление состава защищаемой информации; структура перечня сведений, относимых к различным видам тайны.
4	**Анализ и оценка угроз безопасности защищаемой информации.** Классификация видов и источников угроз. Определение причин, обстоятельств и условий дестабилизирующего воздействия на информацию. Оценка ущерба от потенциального дестабилизирующего воздействия на информацию. Источники угроз в информационных системах предприятия. Персонал как фактор, влияющий на информационную безопасность. Методика выявления каналов несанкционированного доступа (НСД) к информации. Определение возможных каналов утечки и методов НСД к защищаемой информации. Оценка потенциальных последствий реализации НСД. Определение направлений и возможностей доступа нарушителей к защищаемой информации. Модель действий злоумышленника. Взаимосвязь объектов защиты, возможных проявлений злоумышленных действий и подразделений службы безопасности предприятия. Понятие зоны защиты, рубежей защиты. Многорубежная модель защиты. Методика оценки уязвимости (защищенности) информации. Система показателей уязвимости (защищенности). Постановка задачи по оценке уязвимости защищаемой информации в автоматизированных системах обработки данных (АСОД). Понятие риска. Методы анализа и управления риском.
5	**Определение требований к структуре и технологии функционирования КСЗИ.** Понятие стратегии ЗИ. Оборонительная, наступательная и упреждающая стратегии. Функции защиты информации, их структура и содержание. Классификация задач ЗИ. Определение перечня и содержания задач ЗИ.

№	Наименование и содержание разделов
	Общая характеристика различных классов средств ЗИ. Формальные и неформальные средства ЗИ. Технические, программные, криптографические, организационные, законодательные (нормативно-правовые) средства ЗИ. Общие требования, предъявляемые к построению КСЗИ. Комплексность ЗИ. Уровни защиты, их влияние на выбор стратегии ЗИ. Выбор типовых стандартных проектных решений КСЗИ и ее подсистем. Руководящие документы в сфере защиты информации, их роль и место при проектировании КСЗИ.
6	**Этапы проектирования и системного моделирования КСЗИ.** Общая характеристика процесса проектирования КСЗИ. Определение условий функционирования КСЗИ. Многоуровневая организация КСЗИ. Постановки задачи и этапы проектирования КСЗИ. Методологии проектирования и моделирования КСЗИ.
7	**Стандарты и аудит в области информационной безопасности.** Роль стандартов в области информационной безопасности. Международные и российские стандарты в области информационной безопасности, их общая характеристика. Понятие, цели и виды аудита информационной безопасности.
8	**Управление процессами функционирования КСЗИ.** Архитектура (структура) КСЗИ. Автономные, интегрированные, интегральные, интеллектуальные системы ЗИ. Структура функций ЗИ в АСОД. Управление механизмами ЗИ (макропроцессы управления). Режимы управления: быстротекущими процессами, текущее, перспективное. Макрозадачи управления: разработка планов деятельности (планирование); руководство выполнением планов (оперативно-диспетчерское управление, календарно-плановое руководство); обеспечение повседневной деятельности органов управления; сущность и содержание контроля функционирования КСЗИ. Организационное, кадровое, материально-техническое и нормативно-методическое обеспечение функционирования КСЗИ. Политика безопасности организации (предприятия). Уровни политики безопасности, их цели и задачи. Особенности реализации политики безопасности среднего уровня. План защиты организации. Функциональная схема КСЗИ. Правила и положения, определяющие механизмы реализации политики безопасности. Управление в нештатных ситуациях. Потенциально-аварийные, аварийные и чрезвычайные ситуации, соответствующие действия должностных лиц. Планирование нештатных ситуаций. Системы поддержки принятия решений, их функции и задачи. Интеллектуальное здание. Ситуационные центры. Перспективы развития КСЗИ.

Подробное содержание дисциплины, структура учебных занятий, трудоемкость изучения дисциплины, входные и исходящие компетенции, уровень освоения, определяемый этапом формирования компетенций, учебно-методическое, информационное, материально-техническое обеспечение учебного процесса изложены в рабочей программе дисциплины.