Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курганский государственный университет»
(КГУ)

Кафедра «Безопасность информационных и автоматизированных систем»

УТВЕРЖДАЮ:
Первый проректор
___ Т.Р. Змызгова
«__»_____ 2024 г.

Рабочая программа учебной дисциплины

ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

образовательной программы высшего образования –
программы бакалавриата

15.03.04 Автоматизация технологических процессов и производств

Направленность: Автоматизация технологических процессов и производств (в машиностроении)
Форма обучения: очная, заочная

Курган 2024

Рабочая программа дисциплины «Защита информации в компьютерных системах» составлена в соответствии с учебным планом по программе бакалавриата «Автоматизация технологических процессов и производств (в машиностроении)», утвержденной для очной и заочной формы обучения «28» июня 2024 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» «29» августа 2024, протокол № 1.

Рабочую программу составил:
канд.биол.наук А.В. Человечкова

Согласовано:

Заведующий кафедрой «БИАС»
канд. тех. наук, доцент Д.И. Дик

Заведующий кафедрой «АПП»
канд. тех. наук, доцент И.А. Иванова

Начальник Управления
образовательной деятельности И.В. Григоренко

Специалист по учебно-методической
работе Учебно-методического
отдела Г.В. Казанкова

1. ОБЪЕМ ДИСЦИПЛИНЫ

Очная форма

Всего: 3 зачетных единицы трудоемкости (108 академических часа)

Вид учебной работы	На всю дисциплину	Семестр
		3
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**32**	**32**
Лекции	16	16
Лабораторные работы	16	16
Самостоятельная работа, всего часов в том числе:	**76**	**76**
Подготовка к зачету	18	18
Другие виды самостоятельной работы (изучение тем, подготовка к лабораторным работам и рубежному контролю)	58	58
Вид промежуточной аттестации	**зачет**	**зачет**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**108**	**108**

Заочная форма

Всего: 3 зачетных единицы трудоемкости (108 академических часа)

Вид учебной работы	На всю дисциплину	курс	семестр
		2	4
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**6**	**6**	
Лекции	2	2	
Лабораторные работы	4	4	
Самостоятельная работа, всего часов в том числе:	**102**	**102**	
Подготовка к зачету	18	18	
Другие виды самостоятельной работы	66	66	
Контрольная работа	18	18	
Вид промежуточной аттестации	**зачет**	**зачет**	
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**108**	**108**	

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Защита информации в компьютерных системах» относится к части, формируемой участниками образовательных отношений, дисциплмина по выбору Блока 1.

Изучение дисциплины базируется на результатах обучения средней образовательной школы по дисциплине «Информатика».

Результаты обучения по дисциплине необходимы для изучения дисциплин «Проектирование автоматизированных систем», «Программное управление технологическим оборудованием», «Программное обеспечение систем управления», а также для выполнения разделов курсовых проектов по дисциплинам базовой части и выпускной квалификационной работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью дисциплины «Защита информации в компьютерных сетях» является формирование у студентов знаний и умений по защите компьютерных сетей с применением современных программно – аппаратных средств.

Задачи дисциплины – дать знания:

- о методах и средствах защиты информации в компьютерных сетях;
- о технологии межсетевого экранирования;
- о методах и средствах построения виртуальных частных сетей;
- о методах и средствах аудит уровня защищенности информационных систем.

Компетенции, формируемые в результате освоения дисциплины:

- Готов производить инсталляцию и настройку системного, прикладного и инструментального программного обеспечения систем автоматизации и управления (ПК-15).

Индикаторы и дескрипторы части соответствующей компетенции, формируемой в процессе изучения дисциплины «Защита информации в компьютерных системах», оцениваются при помощи оценочных средств.

Планируемые результаты обучения по дисциплине «Защита информации в компьютерных системах», индикаторы достижения компетенций ПК-15, перечень оценочных средств

№ п/п	Код индикатора достижения компетенции	Наименование индикатора достижения компетенции	Код планируемого результата обучения	Планируемые результаты обучения	Наименование оценочных средств
1.	ИД-1$_{ПК-15}$	Знать: возможности и особенности использования специализированных программно-аппаратных средств при проведении аудита информационной безопасности	З (ИД-1$_{ПК-15}$)	Знает: возможности и особенности использования специализированных программно-аппаратных средств при проведении аудита информационной безопасности	Вопросы теста
2.	ИД-2 $_{ПК-15}$	Уметь: применять механизмы защиты, реализованные в программно-аппаратных комплексах, с целью построения защищенных компьютерных сетей	У (ИД-2$_{ПК-15}$)	Умеет: применять механизмы защиты, реализованные в программно-аппаратных комплексах, с целью построения защищенных компьютерных сетей	Комплект имитационных задач
3.	ИД-3 $_{ПК-15}$	Владеть: средствами администрирования сетевых программно-аппаратных комплексов защиты информации и систем обнаружения компьютерных атак	В (ИД-3$_{ПК-15}$)	Владеет: средствами администрирования сетевых программно-аппаратных комплексов защиты информации и систем обнаружения компьютерных атак	Вопросы для сдачи зачета

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ
4.1. Учебно-тематический план.

Рубеж	Номер раздела, темы	Наименование раздела, темы	Количество часов контактной работы с преподавателем			
			Очная		Заочная	
			Лекции	Лабор.	Лекции	Лабор.
Рубеж 1	Тема 1	Основные понятия и определения теории компьютерной безопасности	1	-	-	-
	Тема 2	Структуризация методов, принципов, и механизмов теории компьютерной безопасности	1	-	0,4	-

	Тема 3	Методология построения систем защиты информации в компьютерных системах	2	4	0,4	1
	Тема 4	Основные виды атак на автоматизированные системы	2	5	0,4	1
	Тема 5	Технология межсетевого экранирования	2	2	0,4	1
Рубеж 2	Тема 6	Виртуальные частные сети	2	5	0,4	1
	Тема 7	Аудит информационной безопасности в компьютерных сетях	2	-	-	-
	Тема 8	Политики безопасности	2	-	-	-
	Тема 9	Основные критерии защищенности АС. Классы защищенности АС	2	-	-	-
Всего:			**16**	**16**	**2**	**4**

4.2. Содержание лекционных занятий

Тема 1. Основные понятия и определения теории компьютерной безопасности.

История развития теории и практики компьютерной безопасности. Информация как объект защиты. Конфиденциальность, целостность и доступность информации. Модели ценности информации. Информационный поток. Иерархические модели и модель взаимодействия открытых систем (OSI/ISO).

Угрозы. Классификация угроз безопасности. Модели угроз и модель нарушителя. Утечки информации. Каналы утечек информации. Классификация каналов утечек информации.

Тема 2. Структуризация методов, принципов, и механизмов теории компьютерной безопасности.

Основные направления обеспечения компьютерной безопасности. Основные уровни защиты информации. Принципы построения безопасных АС. Методология обследования и проектирования защиты АС.

Тема 3. Методология построения систем защиты информации в компьютерных системах.

Построение систем защиты от угрозы нарушения конфиденциальности, целостности, доступности информации и угрозы раскрытия параметров информационной системы: Системы идентификации и аутентификации, классификация таких систем. Криптографические средства защиты информации. Стеганографические методы защиты. Контроль целостности информации на МНИ. Цифровая подпись.

Тема 4. Основные виды атак на автоматизированные системы (АС).

Понятие и классификация атак на компьютерные сети. Основные типы сетевых атак. Средства реализации атак. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий.

Технологии обнаружения компьютерных атак и их возможности. Методы обнаружения атак. Классификация систем обнаружения атак /вторжений (СОА/СОВ).

Вредоносное программное обеспечение. Компьютерные вирусы. Классификация вирусов.

Антивирусное программное обеспечение. Классификация антивирусов. Требования к антивирусным программам. Методы обнаружения вредоносного ПО и устранения последствий заражения.

Тема 5. Технология межсетевого экранирования.

Понятие межсетевого экрана. Стратегии и средства межсетевого экранирования. Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов. Типы межсетевых экранов. Схемы межсетевого экранирования.

Фильтрация пакетов. Критерии и правила фильтрации. Реализация пакетных фильтров. Особенности фильтрации различных типов трафика. Шлюзы прикладного уровня. Контроль HTTP-трафика и электронной почты.

Тема 6. Виртуальные частные сети.

Понятие виртуальной частной сети, ее предназначение. Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне. Организация VPN средствами протокола PPTP. Установка и настройка VPN. Анализ защищенности передаваемой информации.

Защита данных на сетевом уровне. Защищенный обмен электронной почтой.

Тема 7. Аудит информационной безопасности в компьютерных сетях.

Цели и задачи проведения аудита безопасности. Этапы и методы проведения, результаты работ.

Нормативно-правовые и организационные основы проведения аудита безопасности компьютерных систем. Определение структуры информационно-телекоммуникационных сетей. Программные средства анализа топологии вычислительной сети. Определение маршрутов прохождения сетевых пакетов. Обнаружение объектов сети. Построение схемы сети. Выявление телекоммуникационного оборудования. Выявление и построение схемы информационных потоков защищаемой информации.

Тема 8. Политики безопасности

Понятие политики безопасности. Формальные модели политик безопасности. Основные типы политики безопасности. Разработка и реализация политики безопасности. Классификация моделей политик безопасности.

Политика и модели безопасности в распределенных компьютерных системах.

Семейство ДП-моделей политик безопасности логического управления доступом и информационными потоками.

Тема 9. Основные критерии защищенности АС. Классы защищенности АС.

Основные критерии оценки защищенности АС. Стандарт оценки безопасности компьютерных систем TCSEC («Оранжевая книга»). Концепция

защиты АС и СВТ по руководящим документам Гостехкомиссии РФ. Единые критерии безопасности информационных технологий (Common Criteria).

Определение уровня защищённости и требования по защите персональных данных. Требования по защите КИИ.

4.3 Лабораторные работы

Номер темы	Наименование темы	Наименование тем лабораторных работ	Норматив времени, час.	
			очная	заочная
3	Методология построения систем защиты информации в компьютерных системах	*Лабораторная работа* № 1. Криптографические средства защиты информации: GPG и Truecrypt.	4	1
4	Основные виды атак на автоматизированные системы	*Лабораторная работа №2.* Контроль настроек и работы антивирусных средств.	4	1
	1-ый рубежный контроль	***Тестирование***	***1***	**-**
5	Технология межсетевого экранирования	*Лабораторная работа №3.* Изучение настроек и работы межсетевых экранов.	2	1
6	Виртуальные частные сети	*Лабораторная работа №4.* Изучение изолированных программных сред на примере работы с виртуальными машинами.	4	1
	2-ой рубежный контроль	***Тестирование***	***1***	**-**
		Итого	**16**	**4**

4.4 Контрольная работа (для заочной формы).

Контрольная работа по дисциплине способствует овладению обучающимися знаний и умений по защите компьютерных сетей с применением современных программно-аппаратных средств. Обучающиеся выбирают тему контрольной работы из перечня тем, предложенных преподавателем.

Контрольная работа выполняется в соответствии с темой работы. Объем контрольной работы 20-25 страниц. К защите работы должна быть представлена пояснительная записка. Рекомендуемая структура пояснительной записки:

- титульный лист;
- информационная часть;
- введение;
- основная часть;
- заключение;
- список использованных источников.

Примерные темы контрольных работ

1. Угрозы безопасности информационной системе.
2. Организационные и физические меры защиты информации.

3. Биометрические средства ограничения доступа.
4. Пластиковые карты.
5. Кодирование и перекодирование информации.
6. Пароли.
7. Защита документов, подготовленных в текстовом редакторе Ms Word.
8. Защита документов, подготовленных в табличном процессоре Excel.
9. Защита html-документов и веб-сайтов.
10. Защита исполняемых программ.
11. Защита носителей информации.
12. Сетевые атаки и организация защиты в сети.
13. Электронная подпись и защита электронных сделок.
14. Защита персональных данных.
15. Основные приемы безопасной работы на компьютере.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

При прослушивании лекций рекомендуется в конспекте отмечать все важные моменты, на которых заостряет внимание преподаватель, в частности те, которые направлены на качественное выполнение соответствующей лабораторной работе.

Преподавателем запланировано использование при чтении лекций технологии учебной дискуссии. Поэтому рекомендуется фиксировать для себя интересные моменты с целью их активного обсуждения на дискуссии в конце лекции.

Залогом качественного выполнения лабораторных работ является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Рекомендуется подготовить вопросы по неясным моментам и обсудить их с преподавателем в начале лабораторной работы.

Преподавателем запланировано применение на лабораторных работах технологий развивающейся кооперации, коллективного взаимодействия, разбора конкретных ситуаций.

Настоятельно рекомендуется тщательно прорабатывать материал дисциплины при самостоятельной работе, участвовать во всех формах обсуждения и взаимодействия, как на лекциях, так и на лабораторных работах в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает самостоятельное изучение разделов дисциплины, подготовку к лабораторным работам, выполнение контрольной работы (для заочной формы), подготовку к рубежным контролям (для очной формы) и подготовку к зачету.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы
Очная форма

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Самостоятельное изучение тем:	**46**
Основные понятия и определения теории компьютерной безопасности	4
Структуризация методов, принципов, и механизмов теории компьютерной безопасности	3
Методология построения систем защиты информации в компьютерных системах	6
Основные виды атак на автоматизированные системы	6
Технология межсетевого экранирования	6
Виртуальные частные сети	5
Аудит информационной безопасности в компьютерных сетях	6
Политики безопасности	4
Основные критерии защищенности АС. Классы защищенности АС	6
Подготовка к лабораторным работам (по 2 часа на каждое занятие)	8
Подготовка к рубежным контролям (по 2 часа на каждый рубежный контроль)	4
Подготовка к зачету	18
Всего:	**76**

Заочная форма

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Самостоятельное изучение тем:	**62**
Основные понятия и определения теории компьютерной безопасности	6
Структуризация методов, принципов, и механизмов теории компьютерной безопасности	6
Методология построения систем защиты информации в компьютерных системах	6
Основные виды атак на автоматизированные системы	8
Технология межсетевого экранирования	8
Виртуальные частные сети	6
Аудит информационной безопасности в компьютерных сетях	8
Политики безопасности	6
Основные критерии защищенности АС. Классы защищенности АС	8
Подготовка к лабораторным работам (по 1 часу на каждое занятие)	4
Контрольная работа	18
Подготовка к зачету	18
Всего:	**102**

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Перечень оценочных средств

1. Балльно-рейтинговая система контроля и оценки академической активности обучающихся в КГУ (очная форма).
2. Отчеты обучающихся по лабораторным работам.
3. Банк тестовых заданий к рубежным контролям № 1, № 2 (очная форма).
4. Контрольная работа (заочная форма).
5. Вопросы к зачету.

6.2. Система балльно-рейтинговой оценки работы обучающихся по дисциплине

<table>
<tr><td>№</td><td>Наименование</td><td colspan="6">Содержание</td></tr>
<tr><td rowspan="3">1</td><td rowspan="3">Распределение баллов за семестр по видам учебной работы, сроки сдачи учебной работы (доводятся до сведения обучающихся на первом учебном занятии)</td><td colspan="6">Распределение баллов</td></tr>
<tr><td>Вид учебной работы:</td><td>Посещение лекций</td><td>Выполнение лабораторной работы</td><td>Рубежный контроль №1</td><td>Рубежный контроль №2</td><td>Зачет</td></tr>
<tr><td>Балльная оценка:</td><td>$2_б$ х 8= $16_б$</td><td>$7_б$ х 4 =$28_б$</td><td>13</td><td>13</td><td>30</td></tr>
<tr><td>2</td><td colspan="2">Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и зачета</td><td colspan="4">60 и менее баллов – неудовлетворительно; не зачтено;
61…73 – удовлетворительно; зачтено;
74… 90 – хорошо;
91…100 – отлично</td></tr>
</table>

3	Критерии допуска к промежуточной аттестации, возможности получения автоматического зачета (экзаменационной оценки) по дисциплине, возможность получения бонусных баллов	Для допуска к промежуточной аттестации по дисциплине за семестр обучающийся должен набрать по итогам текущего и рубежного контроля не менее 51 баллов. В случае если обучающийся набрал менее 51 балла, то к аттестационным испытаниям он не допускается. Для получения зачета без проведения процедуры промежуточной аттестации обучающемуся необходимо набрать в ходе текущего и рубежных контролей не менее 61 балла. В этом случае итог балльной оценки, получаемой обучающимся, определяется по количеству баллов, набранных им в ходе текущего и рубежного контролей. При этом, на усмотрение преподавателя, бальная оценка обучающегося может быть повышена за счет получения дополнительных баллов за академическую активность. Обучающийся, имеющий право на получение оценки без проведения процедуры промежуточной аттестации, может повысить ее путем сдачи аттестационного испытания. В случае получения обучающимся на аттестационном испытании 0 баллов итог бальной оценки по дисциплине не снижается. За академическую активность в ходе освоения дисциплины, участие в учебной, научно-исследовательской, спортивной, культурно-творческой и общественной деятельности обучающемуся могут быть начислены дополнительные баллы. Максимальное количество дополнительных баллов за академическую активность составляет 30. Основанием для получения дополнительных баллов являются: - выполнение дополнительных заданий по дисциплине; дополнительные баллы начисляются преподавателем; - участие в течение семестра в учебной, научно-исследовательской, спортивной, культурно-творческой и общественной деятельности КГУ.
4	Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) обучающихся для получения недостающих баллов в конце семестра	В случае если к промежуточной аттестации (зачету) набрана сумма менее 51 баллов, обучающемуся необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем.

6.3. Процедура оценивания результатов освоения дисциплины

Рубежные контроли проводятся в форме письменного тестирования.

Перед проведением каждого рубежного контроля преподаватель прорабатывает с обучающимися основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии. Варианты тестовых заданий состоят для 1 и 2 рубежного контроля из 13 вопросов. На каждое тестирование при рубежном контроле обучающемуся отводится 1 академический час.

Баллы оьбучающемуся выставляются в зависимости от числа правильно выбранных ответов. Итоговая оценка по тесту формируется путем суммирования набранных баллов и отнесения их к общему количеству вопросов в задании. Помножив полученное значение на 100%, можно привести итоговую оценку к традиционной следующим образом:

«неудовлетворительно» – менее 50%

«удовлетворительно» – 50% - 70%

«хорошо» – 70% - 90%

«отлично» – 90% - 100% .

Преподаватель оценивает в баллах результаты тестирования каждого обучающегося по количеству правильных ответов и заносит в ведомость учета текущей успеваемости.

Зачет проводится в форме ответов на вопросы билета. Билет состоит из 2 вопросов. Вопросы к зачету доводятся до обучающихся на последней лекции в семестре. На подготовку ответа обучающихся отводится 1 астрономический час. Каждый вопрос оценивается до 15 баллов.

Результаты успеваемости и зачета заносятся преподавателем в зачетную ведомость, которая сдается в организационный отдел института в день зачета, а также выставляются в зачетную книжку обучающегося.

6.4. Примеры оценочных средств для рубежного контроля и зачета

1-ый рубежный контроль

Вопрос 1. Доступ к информации, не нарушающий правила разграничения доступа, называется…

а) легальным;

б) нелегальным;

в) санкционированным;

г) вредоносным;

д) несанкционированным.

Вопрос 2. Субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на множество субъектов, имеющих доступ к данной информации

а) целостность;

б) доступность;

в) конфиденциальность;

г) своевременность.

Вопрос 3. Уязвимость информации — это:

а) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.

б) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

в) действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

2-ой рубежный контроль

Вопрос 1. К не преднамеренным угрозам относятся:

а) ошибки в разработке программных средств КС;

б) несанкционированный доступ к ресурсам КС со стороны пользователей КС и посторонних лиц, ущерб от которого определяется полученными нарушителем полномочиями;

в) угроза нарушения конфиденциальности, т.е. утечки информации ограниченного доступа, хранящейся в КС или передаваемой от одной КС к другой.

Вопрос 2. При парольной защите в качестве аутентификационного фактора субъекта выступает

а) то, что он знает;

б) то, чем он владеет;

в) то, что есть часть его самого.

Вопрос 3. Основные направления обеспечения КБ в зависимости от природы средств и методов:

а) компьютерное, криптографическое, бумажное

б) нормативное, формальное, практическое (экспериментальное)

в) нормативно-правовое, инженерно-техническое, организационное, аппаратно-программное

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Информация как объект защиты. Конфиденциальность, целостность и доступность информации.
2. Модели ценности информации. Информационный поток.
3. Иерархические модели и модель взаимодействия открытых систем (OSI/ISO).
4. Угрозы. Классификация угроз безопасности.
5. Модели угроз и модель нарушителя.
6. Утечки информации. Каналы утечек информации.
7. Классификация каналов утечек информации.
8. Основные направления обеспечения компьютерной безопасности.
9. Основные уровни защиты информации.
10. Принципы построения безопасных АС. Методология обследования и проектирования защиты АС.
11. Системы идентификации и аутентификации, классификация таких систем. Криптографические средства защиты информации.
12. Стеганографические методы защиты.
13. Контроль целостности информации на МНИ.
14. Цифровая подпись.
15. Понятие и классификация атак на компьютерные сети. Основные типы сетевых атак.
16. Средства реализации атак.

17. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий.

18. Технологии обнаружения компьютерных атак и их возможности.

19. Методы обнаружения атак. Классификация систем обнаружения атак /вторжений (СОА/СОВ).

20. Вредоносное программное обеспечение.

21. Компьютерные вирусы. Классификация вирусов.

22. Антивирусное программное обеспечение. Классификация антивирусов.

23. Требования к антивирусным программам. Методы обнаружения вредоносного ПО и устранения последствий заражения.

24. Понятие межсетевого экрана. Стратегии и средства межсетевого экранирования.

25. Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов.

26. Типы межсетевых экранов. Схемы межсетевого экранирования.

27. Фильтрация пакетов. Критерии и правила фильтрации.

28. Реализация пакетных фильтров. Особенности фильтрации различных типов трафика.

29. Шлюзы прикладного уровня. Контроль HTTP-трафика и электронной почты.

30. Понятие виртуальной частной сети, ее предназначение. Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне.

31. Организация VPN средствами протокола PPTP. Установка и настройка VPN. Анализ защищенности передаваемой информации.

32. Защита данных на сетевом уровне. Защищенный обмен электронной почтой.

33. Цели и задачи проведения аудита безопасности. Этапы и методы проведения, результаты работ.

34. Нормативно-правовые и организационные основы проведения аудита безопасности компьютерных систем.

35. Определение структуры информационно-телекоммуникационных сетей.

36. Программные средства анализа топологии вычислительной сети.

37. Определение маршрутов прохождения сетевых пакетов.

38. Обнаружение объектов сети. Построение схемы сети.

39. Выявление телекоммуникационного оборудования.

40. Выявление и построение схемы информационных потоков защищаемой информации.

41. Понятие политики безопасности. Основные типы политики безопасности.

42. Разработка и реализация политики безопасности. Классификация моделей политик безопасности.

43. Политика и модели безопасности в распределенных компьютерных системах.

44. Семейство ДП-моделей политик безопасности логического управления доступом и информационными потоками.

45. Основные критерии оценки защищенности АС.

46. Стандарт оценки безопасности компьютерных систем TCSEC («Оранжевая книга»).

47. Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ.

48. Единые критерии безопасности информационных технологий (Common Criteria).

49. Определение уровня защищённости и требования по защите персональных данных.

50. Требования по защите КИИ.

6.5. Фонд оценочных средств

Полный банк заданий для текущего контроля и промежуточной аттестации по дисциплине, показатели, критерии, шкалы оценивания компетенций, методические материалы, определяющие процедуры оценивания образовательных результатов, приведены в учебно-методическом комплексе дисциплины.

7. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

7.1. Основная учебная литература

7.1.1. Основная литература:

1. Грушо А.А., Применко Э.А., Тимонина Е.Е. Теоретические основы компьютерной безопасности. – М.: «Академия», 2009. - 272 с.

2. Галатенко, В.А. Основы информационной безопасности. / [Электронный ресурс]. - М.: Национальный Открытый Университет "ИНТУИТ", 2016 - 208 с. ISBN 5-9556-0052-3. - Доступ ЭБС «Консультант студента».

3. Шаньгин, В. Ф. Информационная безопасность и защита информации [Электронный ресурс] - Москва: ДМК Пресс, 2014. - 702 с. - ISBN 978-5-94074-768-0. - Доступ ЭБС «Консультант студента».

4. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учебное пособие для вузов 2-е изд., испр. и доп. [Электронный ресурс] - Москва: Горячая линия - Телеком, 2013. - 338 с. - ISBN 978-5-9912-0328-9. - Доступ ЭБС «Консультант студента».

7.1.2. Дополнительная литература:

1. Касперски, К. Техника сетевых атак. Т. 1 / Крис Касперски. – М.: Солон-Р, 2001. – 400 с.

2. Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: курс лекций: учебное пособие: для студентов вузов, обучающихся по специальности 510200 "Прикладная математика и информатика"/ О.Р. Лапонина; Интернет-университет информационных технологий. – М.: Интернет-Университет информационных технологий, 2005. – 605 с.

3. Олифер, В.Г. Компьютерные сети: Принципы, технологии, протоколы: учебное пособие для студентов вузов / В. Г. Олифер, Н. А. Олифер. – 3-е изд. – М.; СПб.; Нижний Новгород: Питер, 2007. – 957, с.

8. РЕСУРСЫ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Электронный фонд правовой и нормативно-технической документации - http://docs.cntd.ru;
2. ЭБС «Лань» - https://e.lanbook.com/;
3. ЭБС «Znanium» - https://znanium.com/;
4. ЭБС «Консультант студента» - https://www.studentlibrary.ru;
5. Национальный Открытый Университет «ИНТУИТ» - https://intuit.ru;
6. Единое окно доступа к образовательным ресурсам. – http://window.edu.ru/;
7. Научная электронная библиотека - http://elibrary.ru/;
8. Электронная библиотека КГУ - http://dspace.kgsu.ru/xmlui/;
9. Информационный онлайн портал ISO27000.ru - http://www.iso27000.ru/;
10. Безопасность - http://groteck.ru/security.

9. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1. ЭБС «Лань».
2. ЭБС «Консультант студента».
3. ЭБС «Znanium.com».
4. «Гарант» - справочно-правовая система.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Материально-техническое обеспечение по реализации дисциплины осуществляется в соответствии с требования ФГОС ВО по данной образовательной программе.

11. Для студентов, обучающихся с использованием дистанционных образовательных технологий

При использовании электронного обучения и дистанционных образовательных технологий (далее ЭО и ДОТ) занятия полностью или частично проводятся в режиме онлайн. Объем дисциплины и распределение нагрузки по видам работ соответствует п. 4.1. Распределение баллов соответствует п. 6.2 либо может быть изменено в соответствии с решением кафедры, в случае перехода на ЭО и ДОТ в процессе обучения. Решение кафедры об используемых технологиях и системе оценивания достижений, обучающихся принимается с учетом мнения ведущего преподавателя и доводится до сведения обучающихся.

ПРИЛОЖЕНИЕ 1

Аннотация к рабочей программе дисциплины

«Защита информации в компьютерных системах»

образовательной программы высшего образования –
программы бакалавриата

15.03.04 – Автоматизация технологических процессов и производств

Направленность:

Автоматизация технологических процессов и производств (в машиностроении)

Трудоемкость дисциплины: 3 з.е. (108 академических часа – очная и заочная формы обучения)

Семестр: 3 (очная форма обучения)

Семестр: 4 (заочная форма обучения)

Форма промежуточной аттестации: зачет

Содержание дисциплины. Основные разделы.

Информация как объект защиты. Информационная безопасность. Аппаратно-программные средства защиты информации. Критерии оценки безопасности компьютерных систем. Криптографические средства защиты информации. Защита от несанкционированного доступа. Типовые угрозы информационной безопасности. Технологии обеспечения безопасности в компьютерных сетях.

ЛИСТ
регистрации изменений (дополнений) в рабочую программу
учебной дисциплины
«Защита информации в компьютерных системах»

Изменения / дополнения в рабочую программу
на 20___ / 20___ учебный год:

_____
_____
_____
_____
_____
_____

Ответственный преподаватель _____ / Человечкова А.В. /

Изменения утверждены на заседании кафедры «___»_____20___ г.,
Протокол № ___

Заведующий кафедрой _____ «___»_____20___ г.

Изменения / дополнения в рабочую программу
на 20___ / 20___ учебный год:

_____
_____
_____
_____
_____
_____

Ответственный преподаватель _____ / Человечкова А.В. /

Изменения утверждены на заседании кафедры «___»_____20___ г.,
Протокол № ___

Заведующий кафедрой _____ «___»_____20___ г.