

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Луковникова Елена Ивановна
Должность: Проректор по учебной работе
Дата подписания: 10.06.2022 10:36:43
Уникальный программный ключ:
890f5aae3463de1924cbcf76ac5d7ab89e9fa3d2

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

"БРАТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ"

УТВЕРЖДАЮ

Проректор по учебной работе

Е.И. Луковникова

19

20 22 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.07.02 Программно-аппаратные средства защиты информации

Закреплена за кафедрой **Информатики, математики и физики**

Учебный план б010302_22_ИПОиЗИ.plx

Направление: 01.03.02 Прикладная математика и информатика

Квалификация **Бакалавр**

Форма обучения **очная**

Общая трудоемкость **7 ЗЕТ**

Виды контроля в семестрах:

Экзамен 7,8

Распределение часов дисциплины по семестрам

Семестр (<Курс>. <Семестр на курсе>)	7 (4.1)		8 (4.2)		Итого	
	Неделя		Неделя			
Вид занятий	уп	рп	уп	рп	уп	рп
Лекции	34	34	22	22	56	56
Лабораторные	34	34	33	33	67	67
В том числе инт.	16	16	8	8	24	24
В том числе в форме практ.подготовки	34	34	33	33	67	67
Итого ауд.	68	68	55	55	123	123
Контактная работа	68	68	55	55	123	123
Сам. работа	22	22	17	17	39	39
Часы на контроль	54	54	36	36	90	90
Итого	144	144	108	108	252	252

Программу составил(и):

к.т.н., доц., Сташок О.В.; б.с., Федорович Д.О. Сташок — Федоров

Рабочая программа дисциплины

Программно-аппаратные средства защиты информации

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 01.03.02 Прикладная математика и информатика (приказ Минобрнауки России от 10.01.2018 г. № 9)

составлена на основании учебного плана:

Направление: 01.03.02 Прикладная математика и информатика
 утвержденного приказом ректора от 08.02.2022 протокол № 45.

Рабочая программа одобрена на заседании кафедры

Информатики, математики и физики

Протокол от 12 апреля 2022 г. № 9

Срок действия программы: 2022 - 2026 уч.г.

Зав. кафедрой Горохов Денис Борисович

Председатель МКФ

11 18 апреля 2022 г.

Ответственный за реализацию ОПОП

Д.Б. Горохов
 (подпись)

Д.Б. Горохов
 (ФИО)

Директор библиотеки

Семин
 (подпись)

М.Ф. Семин
 (ФИО)

№ регистрации

42
 (методический отдел)

Визирование РПД для исполнения в очередном учебном году

Председатель МКФ

_____ 2023 г.

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2023-2024 учебном году на заседании кафедры
Информатики, математики и физики

Внесены изменения/дополнения (Приложение _____)

Протокол от _____ 2023 г. № ____
Зав. кафедрой Горохов Денис Борисович

Визирование РПД для исполнения в очередном учебном году

Председатель МКФ

_____ 2024 г.

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2024-2025 учебном году на заседании кафедры
Информатики, математики и физики

Внесены изменения/дополнения (Приложение _____)

Протокол от _____ 2024 г. № ____
Зав. кафедрой Горохов Денис Борисович

Визирование РПД для исполнения в очередном учебном году

Председатель МКФ

_____ 2025 г.

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2025-2026 учебном году на заседании кафедры
Информатики, математики и физики

Внесены изменения/дополнения (Приложение _____)

Протокол от _____ 2025 г. № ____
Зав. кафедрой Горохов Денис Борисович

Визирование РПД для исполнения в очередном учебном году

Председатель МКФ

_____ 2026 г.

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2026-2027 учебном году на заседании кафедры
Информатики, математики и физики

Внесены изменения/дополнения (Приложение _____)

Протокол от _____ 2026 г. № ____
Зав. кафедрой Горохов Денис Борисович

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	формирование у студентов знаний по основам инженерно-технической защиты информации, а также выработка навыков и умений в применении полученных знаний в условиях работы на конкретных объектах информационной безопасности; знаний по основам защиты информации в компьютерных системах, при помощи программных средств, а также навыков и умения в применении знаний для конкретных условий; развитие системного мышления, необходимого для решения задач защиты информации с учетом требований системного подхода.
-----	--

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Цикл (раздел) ООП:		Б1.В.07.02
2.1	Требования к предварительной подготовке обучающегося:	
2.1.1	Криптографические методы защиты информации	
2.1.2	Основы информационной безопасности *	
2.1.3	Проектирование программного обеспечения	
2.1.4	Операционные системы *	
2.2	Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:	
2.2.1	Производственная (преддипломная) практика	
2.2.2	Комплексное обеспечение безопасности объекта информатизации	
2.2.3	Защита в операционных системах	
2.2.4	Основы проектирования программных комплексов	

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

УК-2: Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

Индикатор 1	УК-2.1 Формулирует в рамках поставленной цели проекта совокупность задач, обеспечивающих ее достижение
Индикатор 2	УК-2.2 Выбирает оптимальный способ решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения
ПК-1 : Способен разрабатывать процедуры документирования, интеграции, преобразования программных модулей, миграции и конвертации данных согласно срокам выполнения поставленных задач	
Индикатор 1	ПК-1.1 Использует выбранную среду программирования для разработки процедур интеграции программных модулей согласно срокам выполнения поставленных задач
Индикатор 2	ПК-1.2 Применяет методы и средства разработки процедур для развертывания программного обеспечения, миграции и преобразования данных

В результате освоения дисциплины обучающийся должен

3.1	Знать:
3.1.1	способы достижения результатов в рамках поставленной цели; действующие правовые нормы, ресурсы, ограничения при решении задач в предметной области; языки, утилиты и среды программирования, средства пакетного выполнения процедур; методы и средства разработки программного обеспечения, миграции и преобразования данных.
3.2	Уметь:
3.2.1	проводить анализ поставленной цели и формулировать задачи, необходимые для ее достижения; анализировать альтернативные варианты; выбирать оптимальные способы решения задач предметной области в профессиональной деятельности с учетом действующих правовых норм, ресурсов и ограничений; внедрять и адаптировать программные модули согласно срокам выполнения поставленных задач; использовать процедуры для развертывания программного обеспечения, миграции и преобразования данных.
3.3	Владеть:
3.3.1	разработки цели и задач проекта; приемами планирования решения задач предметной области; проектирования решения конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений; программирования в современных средах; применения современных языков программирования; современных технологий разработки, внедрения, адаптации и настройки программного обеспечения и информационных систем.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Вид занятия	Наименование разделов и тем	Семестр / Курс	Часов	Компетенции	Литература	Инте ракт.	Примечание
-------------	-------------	-----------------------------	----------------	-------	-------------	------------	------------	------------

	Раздел	Раздел 1. Основы технических средств и методов защиты информации						
1.1	Лек	Концепции инженерно-технической защиты информации	7	4	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	2	лекция - беседа УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
1.2	Лаб	Концепции инженерно-технической защиты информации	7	2	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
1.3	Ср	Концепции инженерно-технической защиты информации	7	2	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
1.4	Экзамен	Концепции инженерно-технической защиты информации	7	10	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
1.5	Лек	Теоретические основы инженерно-технической защиты информации	7	8	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
1.6	Лаб	Теоретические основы инженерно-технической защиты информации	7	8	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	4	работа в малых группах УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
1.7	Ср	Теоретические основы инженерно-технической защиты информации	7	4	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
1.8	Экзамен	Теоретические основы инженерно-технической защиты информации	7	10	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
1.9	Лек	Физические основы защиты информации	7	6	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
1.10	Лаб	Физические основы защиты информации	7	6	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	4	работа в малых группах УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2

1.11	Ср	Физические основы защиты информации	7	4	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
1.12	Экзамен	Физические основы защиты информации	7	10	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
1.13	Лек	Технические средства добывания и инженерно-технической защиты	7	6	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	4	лекция - беседа УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
1.14	Лаб	Технические средства добывания и инженерно-технической защиты	7	6	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
1.15	Ср	Технические средства добывания и инженерно-технической защиты	7	4	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
1.16	Экзамен	Технические средства добывания и инженерно-технической защиты	7	10	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
1.17	Лек	Организационные основы инженерно-технической защиты информации	7	6	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
1.18	Лаб	Организационные основы инженерно-технической защиты информации	7	6	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
1.19	Ср	Организационные основы инженерно-технической защиты информации	7	3	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
1.20	Экзамен	Организационные основы инженерно-технической защиты информации	7	6	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
1.21	Лек	Методическое обеспечение инженерно технической защиты автоматизированных систем от вредоносных программных воздействий	7	4	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	2	лекция - беседа УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2

1.22	Лаб	Методическое обеспечение инженерно технической защиты автоматизированных систем от вредоносных программных воздействий	7	6	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
1.23	Ср	Методическое обеспечение инженерно технической защиты автоматизированных систем от вредоносных программных воздействий	7	5	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
1.24	Экзамен	Методическое обеспечение инженерно технической защиты автоматизированных систем от вредоносных программных воздействий	7	8	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
	Раздел	Раздел 2. Программно-аппаратные средства обеспечения информационной безопасности.						
2.1	Лек	Методы и средства защиты программного обеспечения.	8	8	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
2.2	Лаб	Методы и средства защиты программного обеспечения.	8	8	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
2.3	Ср	Методы и средства защиты программного обеспечения.	8	6	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
2.4	Экзамен	Методы и средства защиты программного обеспечения.	8	12	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
2.5	Лек	Построение изолированной программной среды.	8	8	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
2.6	Лаб	Построение изолированной программной среды.	8	16	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	работа в малых группах УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
2.7	Ср	Построение изолированной программной среды.	8	6	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2

2.8	Экзамен	Построение изолированной программной среды.	8	12	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
	Раздел	Раздел 3. Обеспечение информационной безопасности компьютерных сетей.						
3.1	Лек	Стандарты информационной безопасности.	8	6	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	4	лекция - беседа УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
3.2	Лаб	Стандарты информационной безопасности.	8	9	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	4	работа в малых группах УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
3.3	Ср	Стандарты информационной безопасности.	8	5	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2
3.4	Экзамен	Стандарты информационной безопасности.	8	12	УК-2 ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1	0	УК - 2.1; УК - 2.2; ПК - 1.1; ПК - 1.2

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Образовательные технологии с использованием активных методов обучения (лекция – беседа)

Технология коллективного взаимодействия (работа в малых группах) (самостоятельное изучение обучающимися нового материала посредством сотрудничества в малых группах, дает возможность всем участникам участвовать в работе, практиковать навыки сотрудничества, межличностного общения)

Традиционная (репродуктивная) технология (преподаватель знакомит обучающихся с порядком выполнения задания, наблюдает за выполнением и при необходимости корректирует работу обучающихся)

Технология компьютерного обучения(использование в учебном процессе компьютерных технологий и предоставляемых ими возможностей (электронные библиотеки))

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Контрольные вопросы и задания

Вопросы для проведения текущего контроля - 7 семестр.

Лекция - беседа №1. (2 часа).

Тема "Концепции инженерно-технической защиты информации".

Лекция - беседа №2. (4 часа).

Тема "Технические средства добывания и инженерно-технической защиты".

Лекция - беседа №3. (2 часа).

Тема "Методическое обеспечение инженерно технической защиты автоматизированных систем от вредоносных программных воздействий".

Лабораторная работа №1 (2 часа).

Тема "Концепции инженерно-технической защиты информации".

Задание: разработать концепцию инженерно - технической защиты информации на условном предприятии в соответствии с индивидуальным вариантом задания.

Вопросы для защиты:

1. Технические каналы утечки информации, общие понятия, технические каналы утечки речевой информации.
2. Воздушные каналы утечки речевой информации.

3. Вибрационные технические каналы.

Лабораторная работа №2 (8 часов). Интерактивная форма - работа в малых группах (4 часа)

Тема "Теоретические основы инженерно-технической защиты информации".

Задание: разработать концепцию инженерно - технической защиты информации на условном предприятии в соответствии с индивидуальным вариантом задания.

Вопросы для защиты:

1. Электроакустические каналы утечки информации.
2. Оптико-электронный технический канал утечки информации.
3. Параметрические каналы утечки информации .

Лабораторная работа №3 (6 часов). Интерактивная форма - работа в малых группах (4 часа)

Тема "Физические основы защиты информации".

Задание: разработать план физической защиты информации на условном предприятии в соответствии с индивидуальным вариантом задания.

Вопросы для защиты:

1. Электрические линии связи.
2. Электромагнитные каналы утечки информации: электромагнитные излучения элементов ТСПИ, электромагнитные излучения на частотах работы ВЧ-генераторов ТСПИ и ВТСС, электромагнитные излучения на частотах самовозбуждения УНЧ ТСПИ, ПЭМИ ПК.

Лабораторная работа №4 (6 часов).

Тема "Технические средства добывания и инженерно-технической защиты".

Задание: проанализировать технические средства обеспечения защиты информации на условном предприятии в соответствии с индивидуальным вариантом задания.

Вопросы для защиты:

1. Демаскирующие признаки объектов и акустических закладок: в видимом диапазоне электро-магнитного спектра, в инфрокрасном диапазоне электромагнитного спектра.
2. Демаскирующие признаки радиоэлектронных средств, демаскирующие признаки акустических закладок.
3. Средства акустической разведки: микрофоны, направленные микрофоны, проводные системы, портативные диктофоны и электронные стетоскопы, радиомикрофоны, лазерные микрофоны, гидроакустические датчики, СВЧ и ИК передатчики.
4. Средства радио и радиотехнической разведки: сканирующие компьютерные радиоприемники, радиопеленгаторы, анализаторы спектра, радиочастотметры.
5. Средства обеспечения информационной безопасности в компьютерных системах: соболев, secret net, аккорд, secret dist, крипто-про, астра.

Лабораторная работа №5 (6 часов).

Тема "Организационные основы инженерно-технической защиты информации".

Задание: разработать стратегию инженерно - технической защиты информации на условном предприятии в соответствии с индивидуальным вариантом задания.

Вопросы для защиты:

1. Технические средства радиомониторинга и обнаружения закладных устройств: индикаторы поля, комплексы обнаружения закладок и радиомониторинга.
2. Нелинейная локация: технология, эффект затухания, тип излучения промышленные образцы.
3. Средства защиты информации в телефонных системах (с использованием криптографических методов).

Лабораторная работа №6 (6 часов).

Тема "Методическое обеспечение инженерно технической защиты автоматизированных систем от вредоносных программных воздействий".

Задание: разработать методическое обеспечение сопровождения системы инженерно - технической защиты информации на условном предприятии в соответствии с индивидуальным вариантом задания.

Вопросы для защиты:

1. Какие существуют инженерно-технические средства обеспечения безопасности объектов
2. Угрозы утечки информации по техническим каналам в ИСПДн .
3. Виды, источники и носители защищаемой информации.

Вопросы для проведения текущего контроля - 8 семестр.

Лекция - беседа №1. (4 часа).

Тема "Стандарты информационной безопасности".

Лабораторная работа №1 (8 часов).

Тема "Методы и средства защиты программного обеспечения".

Задание: проанализировать программное обеспечение для защиты информации на условном предприятии в соответствии с индивидуальным вариантом задания.

Вопросы для защиты:

1. Основные положения методологии инженерно-технической защиты информации.
2. Основные свойства электромагнитного поля (ЭМП) элементарного электрического излучателя в ближней зоне.
3. Основные свойства электромагнитного поля (ЭМП) элементарного магнитного излучателя в ближней зоне.
4. Электрическое и магнитное поля однопроводных и двухпроводных линий.

Лабораторная работа №2 (16 часов). Интерактивная форма - работа в малых группах (16 часов)

Тема "Построение изолированной программной среды".

Задание: построить изолированную программную среду в соответствии с индивидуальным вариантом задания.

Вопросы для защиты:

1. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите.
2. Показатели защищенности средств вычислительной техники от несанкционированного доступа.
3. Классы защищенности автоматизированных систем.
4. Требования к процессу сертификации продукта информационных технологий
5. Понятие политики безопасности.
6. Описание типовых политик безопасности.
7. Угрозы безопасности компьютерных систем.
8. Методы и средства ограничения доступа к компонентам вычислительных систем
9. Модель компьютерной системы.
10. Понятие монитора безопасности.
11. Программно-аппаратные средства защиты информации в сетях передачи данных
12. Межсетевые экраны.
13. Свойства экранирующего субъекта.

Лабораторная работа №3 (9 часов). Интерактивная форма - работа в малых группах (9 часов)

Тема "Стандарты информационной безопасности".

Задание: проанализировать в сравнении стандарты информационной безопасности в соответствии с индивидуальным вариантом задания.

Вопросы для защиты:

1. Классификация требований к классам межсетевых экранов
2. Роль стандартов информационной безопасности.
3. Модель политики безопасности на основе дискретных компонент АДЕПТ-50.
4. Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.

Вариант теста для проведения текущего контроля по дисциплине

1. На каких частотах возможен перехват информации для мониторов?
А) до 10-15 гармоники тактовой частоты;
Б) до 50-60 гармоники тактовой частоты;
В) до 100-110 гармоники тактовой частоты.
2. На основе какого бытового телевизора был построен приемник визуального контроля излучений мониторов?
А) «Вега-3000» Б) «Горизонт 204» В) «Электроника-100»
3. Какие технические варианты применяются наряду с организационными, программными, криптографическими способами защиты информации для исключения возможностей ее перехвата по ПЭМИ?
А) доработка устройств вычислительной техники с целью минимизации излучений;
Б) электромагнитное экранирование устройств или помещений, в которых расположена вычислительная техника;
В) активная радиотехническая маскировка.
4. Генератор шума выполнен в виде отдельного блока с питанием от сети 220В и предназначен для общей маскировки ПЭМИ персональных компьютеров, компьютерных сетей и комплексов на объектах АСУ и ЭВТ первой, второй и третьей категорий?
А) ГШ-К-1000 Б) ГШ-1000 В) ГШ220-1000
5. Ежедневное техническое обслуживание ГШ-1000М включает:
А) внешний осмотр и проверку работоспособности по свечению индикатора;
Б) инструментальную проверку эффективности работы;
В) удаление пыли, грязи и влаги с поверхностей корпуса.
6. Длительность непрерывного функционирования генераторного блока ГШ-1000М не должна превышать:
А) 4 часа Б) 16 часов В) 24 часа
7. В программе RS turbo обнаруженные излучения автоматически классифицируются программой по следующим признакам:
А) «известные» и «неизвестные»; «обнаруженные ранее» и «вновь появившиеся»; «стандартные» и «нестандартные»;
Б) «старые» и «новые»; «обнаруженные ранее» и «вновь появившиеся»; «стандартные» и «нестандартные»;
В) «известные» и «неизвестные»; «обнаруженные ранее» и «вновь появившиеся»; «простые» и «сложные».
8. Какая операционная система по умолчанию стоит на портативном персональном компьютере комплекса RS turbo Mobile?
А) ОС LINUX Б) Fedora В) Windows XP
9. Диаграмма направленности генератора шума ГРОМ-ЗИ-4:
А) квазикруговая Б) псевдокруговая В) круговая
10. Основные функциональные возможности генератора шума ГРОМ-ЗИ-4:
А) Маскировка побочных электромагнитных излучений ПК и ЛВС;

- Б) Отсутствие необходимости подстройки под конкретные условия применения;
В) Генерация помех по эфиру, телефонной линии и электросети для блокировки несанкционированно установленных устройств, передающих информацию.
11. Максимальный радиус подавления 300УК:
А) Около 30-40 м. Б) Около 300-400 м. В) Около 3000-4000 м.
12. Для увеличения выходной мощности 300УК ...
А) поверните регулировочный резистор против часовой стрелки;
Б) поверните регулировочный резистор по часовой стрелке;
В) поверните регулировочный резистор сверху вниз.
13. Как называют высокочувствительные микрофоны?
А) «микрик» Б) «телефонное ухо» В) «петличка»
14. Физический путь переноса информации от ее источника к несанкционированному получателю называется...
А) каналом распространения; Б) каналом передачи; В) каналом утечки.
15. В качестве источника сигнала могут выступать:
А) объект наблюдения, отражающий электромагнитные и акустические волны; объект наблюдения, излучающий собственные (тепловые) электромагнитные волны;
Б) передатчик функционального канала связи; закладное устройство;
В) источник опасного сигнала; источник акустических волн, модулированных информацией.
16. В структуру канала передачи информации входят:
А) источник сигнала, среда распространения носителя, приемник.
Б) источник сигнала, среда распространения носителя, помехи, приемник.
В) источник сигнала, приемник.
17. Классификацию каналов утечки информации делят по:
А) Информативности Б) Эпизодам В) Структуре
18. В акустических каналах утечки информации ...
А) средой распространения речевых сигналов является вода;
Б) средой распространения речевых сигналов является воздух;
В) средой распространения речевых сигналов являются стены.
19. Какой канал утечки информации может быть реализован и путем «высокочастотного облучения»?
А) Оптико-электронный Б) Параметрический В) Электроакустический
20. В вибрационных (структурных) технических каналах утечки информации средой распространения акустических сигналов являются:
А) Твердые тела; Б) Жидкость; В) Газ.
21. Эффект электроакустического преобразования акустических колебаний в электрические часто называют ...
А) микрофонным эффектом;
Б) лазерным эффектом;
В) электроакустическим эффектом.
22. Технический канал утечки информации путем ... может быть осуществлен путем несанкционированного контактного введения токов.
А) «низкочастотного навязывания»;
Б) «среднечастотного навязывания»;
В) «высокочастотного навязывания».
23. Оптико-электронный канал утечки акустической информации образуется ...
А) при облучении лазерным лучом вибрирующих в акустическом поле стекол;
Б) при изменении взаимно расположенных элементов схем;
В) за счет электроакустических преобразований акустических сигналов в электрические.
24. Для перехвата речевой информации по оптико-электронному каналу используются ...
А) «оптические микрофоны» Б) «лазерные микрофоны» В) «электронные микрофоны»
25. Параметрический канал утечки информации может быть реализован и путем...
А) «высокочастотного навязывания»
Б) «высокочастотного лазера»
В) «высокочастотного облучения»

26. Закладки, которые обеспечивают амплитудную, фазовую или частотную модуляцию переотраженного сигнала по закону изменения речевого сигнала называют...

А) полуактивными; Б) малоактивными; В) среднеактивными.

27. К вспомогательными техническими средствами и системами (ВТСС) относят:

А) технические средства открытой телефонной, громкоговорящей связи;

Б) радиофикации, часофикации, электробытовые приборы;

В) системы пожарной и охранной сигнализации, электрификации.

28. В качестве канала утечки информации наибольший интерес представляют ВТСС, имеющие выход за пределы:

А) контролируемой зоны (КЗ); Б) неконтролируемой зоны (НЗ); В) зоны подконтроля(ЗП).

29. Сигналы помехи радиодиапазона принято делить на...

А) заградительные Б) прицельные В) инфракрасные

30. Для уменьшения магнитной и электрической связи между проводами необходимо сделать следующее:

А) уменьшить напряжение источника сигнала или тока; уменьшить площадь петли; максимально разнести цепи; передавать сигналы постоянным током или на низких частотах; использовать провод в магнитном экране с высокой проницаемостью; включить в цепь дифференциальный усилитель.

Б) уменьшить напряжение источника сигнала или тока; передавать сигналы постоянным током или на низких частотах; использовать провод в магнитном экране с высокой проницаемостью; включить в цепь дифференциальный усилитель.

В) уменьшить напряжение источника сигнала или тока; уменьшить площадь петли; максимально разнести цепи; передавать сигналы постоянным током или на низких частотах; использовать провод в магнитном экране с высокой проницаемостью; включить в цепь дифференциальный усилитель.

6.2. Темы письменных работ

не предусмотрено учебным планом

6.3. Фонд оценочных средств

Экзаменационные вопросы, 7 семестр

Раздел 1. Основы технических средств и методов защиты информации.

1.1. Технические каналы утечки информации, общие понятия, технические каналы утечки речевой информации.

1.2. Воздушные каналы утечки речевой информации.

1.3. Вибрационные технические каналы.

1.4. Электроакустические каналы утечки информации.

1.5. Оптико-электронный технический канал утечки информации.

1.6. Параметрические каналы утечки информации .

1.7. Технические каналы утечки информации, обрабатываемой ТСПИ и передаваемой по каналам связи.

1.8. Электрические линии связи.

1.9. Электромагнитные каналы утечки информации: электромагнитные излучения элементов ТСПИ, электромагнитные излучения на частотах работы ВЧ-генераторов ТСПИ и ВТСС, электромагнитные излучения на частотах самовозбуждения УНЧ ТСПИ, ПЭМИ ПК.

1.10. Электрические каналы утечки информации.

1.11. Способы скрытого видеонаблюдения и съемки.

1.12. Демаскирующие признаки объектов и акустических закладок: в видимом диапазоне электро-магнитного спектра, в инфрокрасном диапазоне электромагнитного спектра.

1.13. Демаскирующие признаки радиоэлектронных средств, демаскирующие признаки акустических закладок.

1.14. Средства акустической разведки: микрофоны, направленные микрофоны, проводные системы, портативные диктофоны и электронные стетоскопы, радиомикрофоны, лазерные микрофоны, гидроакустические датчики, СВЧ и ИК передатчики.

1.15. Средства радио и радиотехнической разведки: сканирующие компьютерные радиоприемники, радиопеленгаторы, анализаторы спектра, радиочастотметры.

1.16. Средства обеспечения информационной безопасности в компьютерных системах: собошь, secret net, аккорд, secret dist, крипто-про, астра.

1.17. Технические средства радиомониторинга и обнаружения закладных устройств: индикаторы поля, комплексы обнаружения закладок и радиомониторинга.

1.18. Нелинейная локация: технология, эффект затухания, тип излучения промышленные образцы.

1.19. Средства защиты информации в телефонных системах (с использованием криптографических методов)

1.20. Металлодетекторы

1.21. Контроль слаботочных линий

1.22. Защита слаботочных линий

1.23. Системы слежения за транспортными средствами

1.24. Контроль телефонных каналов связи

1.25. Прослушивание телефонных каналов связи

1.26. Экранирование электромагнитных волн

1.27. Экранирование соединительных проводников

1.28. Безопасность оптоволоконных линий связи

1.29. Заземление технических средств

- 1.30. Фильтрация информационных сигналов
- 1.31. Основные сведения и выбор помехоподавляющих фильтров
- 1.32. Какие существуют инженерно-технические средства обеспечения безопасности объектов
- 1.33. Угрозы утечки информации по техническим каналам в ИСПДн .
- 1.34. Виды, источники и носители защищаемой информации.
- 1.35. Характеристика государственной системы противодействия технической разведке.
- 1.36. Основные положения методологии инженерно-технической защиты информации.
- 1.37. Основные свойства электромагнитного поля (ЭМП) элементарного электрического излучателя в ближней зоне.
- 1.38. Основные свойства электромагнитного поля (ЭМП) элементарного магнитного излучателя в ближней зоне.
- 1.39. Электрическое и магнитное поля однопроводных и двухпроводных линий.
- 1.40. Акустоэлектрические технических каналов утечки акустической информации(ТКУАИ).
- 1.41. Характеристика зонного принципа защиты информации.
- 1.42. Защита информации, обрабатываемой ТСПИ, методом экранирования.
- 1.43. Защита информации, обрабатываемой ТСПИ, методом фильтрации.
- 1.44. Пассивные методы защиты акустической информации.
- 1.45. Активные методы защиты акустической информации.
- 1.46. Классификация объектов охраны, особенности задач охраны различных типов объектов.

Экзаменационные вопросы, 8 семестр

Раздел 2. Программно-аппаратные средства обеспечения информационной безопасности.

- 2.1. Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности
- 2.2. Концепция диспетчера доступа.
- 2.3. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите.

Раздел 3. Обеспечение информационной безопасности компьютерных сетей.

- 3.1. Показатели защищенности средств вычислительной техники от несанкционированного доступа.
- 3.2. Классы защищенности автоматизированных систем.
- 3.3. Требования к процессу сертификации продукта информационных технологий
- 3.4. Понятие политики безопасности.
- 3.5. Описание типовых политик безопасности.
- 3.6. Угрозы безопасности компьютерных систем..
- 3.7. Методы и средства ограничения доступа к компонентам вычислительных систем
- 3.8. Модель компьютерной системы.
- 3.9. Понятие монитора безопасности.
- 3.10. Программно-аппаратные средства защиты информации в сетях передачи , данных
- 3.11. Межсетевые экраны.
- 3.12. Свойства экранирующего субъекта.
- 3.13. Классификация требований к классам межсетевых экранов
- 3.14. Роль стандартов информационной безопасности.
- 3.15. Модель политики безопасности на основе дискретных компонент АДЕПТ-50.
- 3.16. Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.
- 3.17. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности.

6.4. Перечень видов оценочных средств

Лекция - беседа, лабораторные работы, тестовое задание; экзаменационные вопросы.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
ЛП. 1	Долозов Н. Л., Гулятьева Т. А.	Программные средства защиты информации: конспект лекций	Новосибирск: Новосибирский государственный технический университет, 2015	1	http://biblioclub.ru/index.php?page=book&id=438307
ЛП. 2	Титов А. А.	Технические средства защиты информации: учебное пособие	Томск: Томский государственный университет систем управления и радиоэлектроники, 2010	1	http://biblioclub.ru/index.php?page=book&id=208661

7.1.2. Дополнительная литература

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
--	---------	----------	---------------	--------	-----------

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
Л2. 1	Моргунов А. В.	Информационная безопасность: учебно-методическое пособие	Новосибирск: Новосибирский государственный технический университет, 2019	1	http://biblioclub.ru/index.php?page=book&id=576726
Л2. 2	Басыня Е. А.	Системное администрирование и информационная безопасность: учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2018	1	http://biblioclub.ru/index.php?page=book&id=575325
Л2. 3	Ищейнов В. Я.	Информационная безопасность и защита информации: теория и практика: учебное пособие	Москва Берлин: Директ-Медиа, 2020	1	http://biblioclub.ru/index.php?page=book&id=571485
Л2. 4	Ковалев Д. В., Богданова Е. А.	Информационная безопасность: учебное пособие	Ростов-на-Дону: Южный федеральный университет, 2016	1	http://biblioclub.ru/index.php?page=book&id=493175
Л2. 5	Прохорова О. В.	Информационная безопасность и защита информации: учебник	Самара: Самарский государственный архитектурно- строительный университет, 2014	1	http://biblioclub.ru/index.php?page=book&id=438331
Л2. 6	Хахаев И. А.	Практикум по алгоритмизации и программированию на Python: курс	Москва: Национальный Открытый Университет «ИНТУИТ», 2016	1	http://biblioclub.ru/index.php?page=book&id=429256

7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Электронный каталог библиотеки БрГУ	http://ecat.brstu.ru/catalog
----	-------------------------------------	---

7.3.1 Перечень программного обеспечения

7.3.1.1	Microsoft Office 2007 Russian Academic OPEN No Level
7.3.1.2	Chrome
7.3.1.3	Visual Studio Community
7.3.1.4	Python IDLE

7.3.2 Перечень информационных справочных систем

7.3.2.1	Научная электронная библиотека eLIBRARY.RU
7.3.2.2	Электронная библиотека БрГУ
7.3.2.3	Электронный каталог библиотеки БрГУ
7.3.2.4	«Университетская библиотека online»
7.3.2.5	Издательство "Лань" электронно-библиотечная система

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

A1207	Лаборатория технических средств защиты информации	<p>Основное оборудование:</p> <ul style="list-style-type: none"> - ПК i5-2500/H67/4Gb/500Gb - 11 шт.; -монитор TFT19 Samsung E1920NR- 11 шт.; -комплекс учебно-лабораторного оборудования “Технические средства и методы защиты информации”; -управляемый коммутатор 2 уровня D-Link DES-3028. <p>Дополнительно:</p> <ul style="list-style-type: none"> - интерактивная доска SMART Board X885ix со встроенным проектором UX 60 - 1 шт. <p>Учебная мебель:</p> <ul style="list-style-type: none"> - комплект мебели (посадочных мест /APM) - 24 /11 шт. - комплект мебели (посадочных мест/APM) для преподавателя - 1/1 шт. <p>ПК i5-2500/H67/4Gb/500Gb; монитор TFT19 Samsung E1920NR.</p>
-------	---	--

A1207	Лаборатория технических средств защиты информации	<p>Основное оборудование:</p> <ul style="list-style-type: none"> - ПК i5-2500/H67/4Gb/500Gb - 11 шт.; -монитор TFT19 Samsung E1920NR- 11 шт.; -комплекс учебно-лабораторного оборудования “Технические средства и методы защиты информации”; -управляемый коммутатор 2 уровня D-Link DES-3028. <p>Дополнительно:</p> <ul style="list-style-type: none"> - интерактивная доска SMART Board X885ix со встроенным проектором UX 60 - 1 шт. <p>Учебная мебель:</p> <ul style="list-style-type: none"> - комплект мебели (посадочных мест /АРМ) - 24 /11 шт. - комплект мебели (посадочных мест/АРМ) для преподавателя - 1/1 шт. <p>ПК i5-2500/H67/4Gb/500Gb; монитор TFT19 Samsung E1920NR.</p>
2201	читальный зал №1	<p>Комплект мебели (посадочных мест)</p> <p>Стеллажи</p> <p>Комплект мебели (посадочных мест) для библиотекаря</p> <p>Выставочные шкафы</p> <p>ПК i5-2500/H67/4Gb (монитор TFT19 Samsung) (10шт.); принтер HP Laser Jet P2055D (1шт.)</p>
A1207	Лаборатория технических средств защиты информации	<p>Основное оборудование:</p> <ul style="list-style-type: none"> - ПК i5-2500/H67/4Gb/500Gb - 11 шт.; -монитор TFT19 Samsung E1920NR- 11 шт.; -комплекс учебно-лабораторного оборудования “Технические средства и методы защиты информации”; -управляемый коммутатор 2 уровня D-Link DES-3028. <p>Дополнительно:</p> <ul style="list-style-type: none"> - интерактивная доска SMART Board X885ix со встроенным проектором UX 60 - 1 шт. <p>Учебная мебель:</p> <ul style="list-style-type: none"> - комплект мебели (посадочных мест /АРМ) - 24 /11 шт. - комплект мебели (посадочных мест/АРМ) для преподавателя - 1/1 шт. <p>ПК i5-2500/H67/4Gb/500Gb; монитор TFT19 Samsung E1920NR.</p>

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Обучающийся должен разработать собственный режим равномерного освоения дисциплины. Подготовка студента к предстоящей лекции включает в себя ряд важных познавательно-практических этапов:

- чтение записей, сделанных в процессе слушания и конспектирования предыдущей лекции, вынесение на поля всего, что требуется при дальнейшей работе с конспектом и учебником;
- техническое оформление записей (подчеркивание, выделение главного, выводов, доказательств);
- выполнение заданий преподавателя;
- знакомство с материалом предстоящей лекции по учебнику и дополнительной литературе.

Успешность выполнения лабораторных работ определяется подготовкой к ним.

Подготовка к лабораторным работами содержит:

- изучение теоретического материала, содержащегося в учебной литературе, изучение лекционного материала;
- знакомство с заданиями на лабораторную работу;
- составление плана выполнения лабораторной работы и практического задания.

Наиболее продуктивной является самостоятельная работа в библиотеке, где доступны основные и дополнительные печатные и электронные источники.

При выполнении приведенных выше рекомендаций подготовка к экзамену сведется к повторению изученного и совершенствованию навыков применения теоретических положений и различных методов решения к стандартным и нестандартным заданиям.