УТВЕРЖДЕНО

решением Ученого совета факультета математики, информационных и авиационных технологий
от «21» 05 2024г., протокол № 5/24
Председатель _____ Волков М.А.
«21» 05 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	**Профессиональный электив. Контроль состояния технической защиты конфиденциальной информации**
Факультет	Факультет математики, информационных и авиационных технологий
Кафедра	Кафедра информационной безопасности и теории управления
Курс	4

Направление (специальность): 10.05.03 Информационная безопасность автоматизированных систем
Направленность (профиль/специализация): Безопасность открытых информационных систем
Форма обучения: очная
Дата введения в учебный процесс УлГУ: 01.09.2024 г.
Программа актуализирована на заседании кафедры: протокол № 10 от 15.04 2024 г.
Программа актуализирована на заседании кафедры: протокол №_____ от _____ 20___г.
Программа актуализирована на заседании кафедры: протокол №_____ от _____ 20___г.

Сведения о разработчиках:

ФИО	КАФЕДРА	Должность, ученая степень, звание
Иванцов Андрей Михайлович	Кафедра информационной безопасности и теории управления	Доцент, Кандидат технических наук, Доцент

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

Дисциплина «Профессиональный электив. Контроль состояния технической защиты конфиденциальной информации» является важной составляющей общей профессиональной подготовки специалистов в области обеспечения информационной безопасности. Дисциплина реализует требования профессионального стандарта «Специалист по технической защите информации" и направлена на получение студентами знаний, умений и навыков по вопросам контроля состояния технической защиты конфиденциальной информации (ТЗКИ).

Задачи освоения дисциплины:

изучить основные методы и средства контроля состояния ТЗКИ;

обеспечить освоение студентами умений и навыков по вопросам контроля состояния ТЗКИ.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Профессиональный электив. Контроль состояния технической защиты конфиденциальной информации» относится к числу дисциплин блока Б1.В.1, предназначенного для студентов, обучающихся по направлению: 10.05.03 Информационная безопасность автоматизированных систем.

В процессе изучения дисциплины формируются компетенции: ПК-8.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: Профессиональный электив. Контроль состояния технической защиты конфиденциальной информации, Профессиональный электив. Методы и средства технической защиты конфиденциальной информации от несанкционированного доступа, Профессиональный электив. Организационно-правовые основы технической защиты конфиденциальной информации, Эксплуатационная практика, Подготовка к сдаче и сдача государственного экзамена.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ПК-8 Способен проводить работы по установке, настройке и испытаниям технических средств обработки информации	**знать**: Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и эксплуатации защищенных технических средств обработки информации. Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений от основных технических средств, за счет наводок информативных

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
	сигналов на цепи электропитания и заземления основных технических средств и систем, вспомогательные технические средства и системы, их кабельные коммуникации, а также создаваемые методом "высокочастотного облучения" основных технических средств и систем и за счет возможно внедренных электронных устройств перехвата информации в основных технических средствах и системах. Способы защиты информации от утечки по техническим каналам **уметь**: Проводить настройку защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами. Производить установку и монтаж защищенных технических средств обработки информации **владеть**: Навыками установки и монтажа защищенных технических средств обработки информации. Навыками настройки защищенных технических средств обработки информации

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего): 3 ЗЕТ

4.2. Объем дисциплины по видам учебной работы (в часах): 108 часов

Форма обучения: очная

Вид учебной работы	Количество часов (форма обучения очная)	
	Всего по плану	В т.ч. по семестрам
		7
1	2	3
Контактная работа обучающихся с преподавателем в соответствии с УП	54	54
Аудиторные занятия:	54	54
Лекции	18	18
Семинары и практические занятия	18	18
Лабораторные работы, практикумы	18	18
Самостоятельная работа	54	54
Форма текущего контроля знаний и контроля самостоятельной работы: тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)	Тестирование	Тестирование
Курсовая работа	Курсовая работа	Курсовая работа
Виды промежуточной аттестации	Зачет (0)	Зачет

Вид учебной работы	Количество часов (форма обучения очная)	
	Всего по плану	В т.ч. по семестрам
		7
1	2	3
(экзамен, зачет)		
Всего часов по дисциплине	108	108

4.3. Содержание дисциплины. Распределение часов по темам и видам учебной работы

Форма обучения: очная

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
Раздел 1. Основы организации контроля состояния ТЗКИ							
Тема 1.1. Основные задачи контроля состояния ТЗКИ	4	2	0	0	0	2	Тестирование
Тема 1.2. Организационный и технический контроль состояния ТЗКИ	10	2	4	0	0	4	Тестирование
Раздел 2. Методы и средства контроля защищенности конфиденциальной информации							
Тема 2.1. Методы и средства контроля защищенности конфиденциальной информации, обрабатываемой техническими	20	2	2	4	0	12	Тестирование

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
средствами, от утечки за счет ПЭМИН.							
Тема 2.2. Методы и средства контроля защищенности конфиденциальной акустической речевой информации и от утечки по техническим каналам	18	2	2	6	0	8	Тестирование
Тема 2.3. Методы и средства контроля защищенности конфиденциальной информации и от НСД	16	2	2	4	0	8	Тестирование
Раздел 3. Мониторинг информационной безопасности средств и систем информатизации							
Тема 3.1. Цели, задачи и функции мониторинга информационной безопасности средств и систем информатизации	8	2	2	0	0	4	Тестирование
Тема 3.2. Обнаружение и иденти	16	2	2	4	0	8	Тестирование

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
фикация инцидентов безопасности информации							
Тема 3.3. Планирование мер по устранению инцидентов безопасности информации	8	2	2	0	0	4	Тестирование
Тема 3.4. Документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации	8	2	2	0	0	4	Тестирование
Итого подлежит изучению	108	18	18	18	0	54	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Основы организации контроля состояния ТЗКИ

Тема 1.1. Основные задачи контроля состояния ТЗКИ

Основные термины и определения в области состояния ТЗКИ. Сущность и задачи контроля состояния ТКЗИ. Система документов по контролю состояния ТЗКИ. Вопросы, подлежащие проверке при контроле состояния ТКЗИ в организации.

Тема 1.2. Организационный и технический контроль состояния ТЗКИ

Классификация видов контроля состояния ТКЗИ. Организационный и технический контроль состояния ТЗКИ. Система документации по контролю состояния ТЗКИ

Раздел 2. Методы и средства контроля защищенности конфиденциальной информации

Тема 2.1. Методы и средства контроля защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН.

Основные методы и средства контроля защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН. Методика оценки защищенности информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН.

Тема 2.2. Методы и средства контроля защищенности конфиденциальной акустической речевой информации от утечки по техническим каналам

Обобщённая структура технического канала утечки. Основные методы контроля защищенности конфиденциальной акустической речевой информации от утечки. Основные средства контроля защищенности конфиденциальной акустической речевой информации от утечки

Тема 2.3. Методы и средства контроля защищенности конфиденциальной информации от НСД

Основные методы и средства контроля защищенности конфиденциальной информации от НСД. Документирование результатов контроля. Требования к средствам контроля защищенности конфиденциальной информации.

Раздел 3. Мониторинг информационной безопасности средств и систем информатизации

Тема 3.1. Цели, задачи и функции мониторинга информационной безопасности средств и систем информатизации

Цели, задачи и функции мониторинга информационной безопасности средств и систем информатизации. Состав и структура системы мониторинга информационной безопасности средств и систем информатизации. Порядок и методы мониторинга информационной безопасности средств и систем информатизации.

Тема 3.2. Обнаружение и идентификация инцидентов безопасности информации

Понятие события и инцидента ИБ. Система управления инцидентами ИБ. Этапы процесса управления инцидентами ИБ. Политика управления инцидентами ИБ. Обнаружение и идентификация инцидентов безопасности информации, а также событий, приводящих к возникновению инцидентов. Оценка последствий инцидентов безопасности информации.

Тема 3.3. Планирование мер по устранению инцидентов безопасности информации

Планирование мер по устранению инцидентов безопасности информации, в том числе по восстановлению систем информатизации, их сегментов и средств, входящих в их состав, в случае отказа в обслуживании или после сбоев. Устранение последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов. Общая характеристика планов управления инцидентами, обеспечения непрерывности бизнеса и восстановления бизнеса. Примерное содержание плана обеспечения непрерывности бизнеса. Контроль за событиями безопасности и действиями пользователей в средствах и системах информатизации.

Тема 3.4. Документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации

Документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в средствах и системах информатизации. Разработка предложений (рекомендаций) по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) систем защиты информации систем информатизации, повторной оценке эффективности систем защиты информации систем информатизации или проведении дополнительных работ по оценке эффективности систем защиты информации систем информатизации

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Раздел 1. Основы организации контроля состояния ТЗКИ

Тема 1.2. Организационный и технический контроль состояния ТЗКИ

Вопросы к теме:

Очная форма

1. Сущность и задачи контроля состояния ТКЗИ
2. Вопросы, подлежащие проверке при контроле состояния ТКЗИ в организации
3. Классификация видов контроля состояния ТКЗИ. Организационный и технический контроль состояния ТЗКИ
4. Система документации по контролю состояния ТЗКИ

Раздел 2. Методы и средства контроля защищенности конфиденциальной информации

Тема 2.1. Методы и средства контроля защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН.

Вопросы к теме:

Очная форма

1. Основные методы и средства контроля защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН
2. Методика оценки защищенности информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН

Тема 2.2. Методы и средства контроля защищенности конфиденциальной акустической речевой информации от утечки по техническим каналам

Вопросы к теме:

Очная форма

1. Обобщённая структура технического канала утечки
2. Основные методы контроля защищенности конфиденциальной акустической речевой информации от утечки
3. Основные средства контроля защищенности конфиденциальной акустической речевой информации от утечки

Тема 2.3. Методы и средства контроля защищенности конфиденциальной информации от НСД

Вопросы к теме:

Очная форма

1. Основные методы контроля защищенности конфиденциальной информации от НСД
2. Основные средства контроля защищенности конфиденциальной информации от НСД
3. Документирование результатов контроля. Требования к средствам контроля защищенности конфиденциальной информации.

Раздел 3. Мониторинг информационной безопасности средств и систем информатизации

Тема 3.1. Цели, задачи и функции мониторинга информационной безопасности средств и систем информатизации

Вопросы к теме:

Очная форма

1. Цели, задачи и функции мониторинга информационной безопасности средств и систем информатизации

2. Состав и структура системы мониторинга информационной безопасности средств и систем информатизации.

3. Порядок и методы мониторинга информационной безопасности средств и систем информатизации.

Тема 3.2. Обнаружение и идентификация инцидентов безопасности информации

Вопросы к теме:

Очная форма

1. Понятие события и инцидента ИБ
2. Система управления инцидентами ИБ
3. Этапы процесса управления инцидентами ИБ
4. Политика управления инцидентами ИБ

Тема 3.3. Планирование мер по устранению инцидентов безопасности информации

Вопросы к теме:

Очная форма

1. Общая характеристика планов управления инцидентами, обеспечения непрерывности бизнеса и восстановления бизнеса
2. Примерное содержание плана обеспечения непрерывности бизнеса

Тема 3.4. Документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации

Вопросы к теме:

Очная форма

1. Содержание протоколов аттестационных испытаний и заключения по результатам аттестационных испытаний информационных (автоматизированных) систем
2. Содержание протоколов аттестационных испытаний и заключения по результатам аттестационных испытаний выделенных (защищаемых) помещений
3. Оформление аттестата соответствия на выделенное (защищаемое) помещение

7. ЛАБОРАТОРНЫЕ РАБОТЫ, ПРАКТИКУМЫ

Изучение методов поиска и локализации специальных технических средств с использованием прибора ST-032 Пиранья

Цели: Изучить возможности прибора ST-032 «Пиранья» и научиться осуществлять поиск и локализацию специальных технических средств несанкционированного получения информации

Содержание: Работа проводится в игровом варианте попарно в два этапа. Первый студент – «злоумышленник» (З), второй – сотрудник службы безопасности (СБ). На первом этапе З изучает технические характеристики и правила эксплуатации многофункционального имитатора ИМФ-2, а СБ – технические характеристики, правила эксплуатации и методику поиска каналов утечки информации с помощью поискового комплекса «Пиранья ST-032». Перед началом практических действий оба игрока отвечают на контрольные вопросы преподавателя с целью проверки уровня их подготовки. Контрольные вопросы приведены ниже. Затем, СБ на некоторое время (1…2 мин) покидает аудиторию. За это время З должен включить ИМФ-2 в режим радиозакладки и где-либо замаскировать или спрятать в личных вещах присутствующих в аудитории студентов. Для создания акустического фона, вызывающего функционирование ИМФ-2 может использоваться магнитофонная запись или доклад одного из присутствующих студентов. Вошедший в аудиторию СБ начинает поиск радиозакладки с использованием ST-032. При этом фиксируется время начала и окончания поиска. На втором этапе игроки меняются ролями. Аналогично работает вторая и последующие пары игроков в группе. Победители определяются в двух номинациях: среди сотрудников службы безопасности и «злоумышленников». В первом случае лучшим признается тот студент, который затратил минимальное время на обнаружение и локализацию радиозакладки, во втором – тот, чью закладку искали максимальное время. Выполнение работы оценивается «зачет» – «не зачет». Изучение других режимов поиска осуществляется демонстрационным методом. Для этого ИМФ-2 последовательно переводится в различные режимы работы для имитации работы закладок по ИК-каналу, телефонной линии и сети электропитания. Переключением режимов работы ST-032 обнаруживаются каналы утечки. Для проверки детектора низкочастотных полей целесообразно продемонстрировать съем информации с наушников, подключенных к сотовому телефону в режиме воспроизведения музыкального файла.

Результаты: изучить прибор ST 032 «Пиранья» и основные методы поиска и локализации специальных технических средств несанкционированного получения информации; составить отчет о проделанной работе и отчитаться по нему у преподавателя.

Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/14064.

Защита каналов передачи информации генератором шума «Гром-ЗИ-4».

Цели: Ознакомление с техническими характеристиками генератора шума «Гром-ЗИ-4», изучение правил его эксплуатации и получение практических навыков работы с генератором шума Гром-ЗИ-4».

Содержание: При подготовке к использованию прибора по назначению необходимо выполнить следующие операции: - подключить антенну к прибору. Антенная система генератора шума "ГРОМ-ЗИ-4" излучает электромагнитное поле шума с поляризацией, близкой к эллиптической. При использовании "ГРОМ-ЗИ-4" дли зашумления малогабаритных, локально размещенных объектов, антенная система может не ориентироваться в пространстве. При зашумлении крупногабаритных объектов (вычислительных центров, терминальных залов мощных вычислительных комплексов) рекомендуется использовать несколько комплектов "ГРОМ-ЗИ-4", размещая антенные системы в трех перпендикулярных плоскостях; ВНИМАНИЕ! Запрещается эксплуатация прибора с отключенной антенной - подключить телефонный аппарат (ТА) и линию к гнездам "ТА" и "ЛИНИЯ" прибора; - подключить прибор к электросети 220 В 50 Гц. - включить прибор клавишей "СЕТЬ" и проконтролируйте включение по индикатору. При зашумлении радиоканала: - убедиться в

прохождении радиосигналов на различных частотах (например, при прослушивании радиопередач FM-диапазона); - для генерации прибором электромагнитного поля шума включите клавишу "РАДИОКАНАЛ" и проконтролируйте включение по индикатору; - проконтролируйте невозможность прослушивания радиопередач; - определите радиус зашумляемой зоны, постепенно удаляясь от прибора. Проведите замеры в здании, на открытой и полуоткрытой территориях. При зашумлении электросети или телефонной линии: - подключите прибор ИМФ-2 к электросети или телефонной линии; - убедитесь в утечке опасного сигнала с применением прибора ST-032; - для генерации прибором сигнала в электросеть включите клавишу "ЭЛЕКТРОСЕТЬ" и проконтролируйте включение по индикатору; - для генерации прибором сигнала в телефонную линию включите клавишу "ТЕЛЕФОННАЯ ЛИНИЯ" и проконтролируйте включение по индикатору; - проконтролируйте невозможность перехвата опасного сигнала в исследуемой цепи при подаче шума. Выключение прибора проводится в обратном порядке.
Результаты: ознакомиться с техническими характеристиками генератора шума «Гром-ЗИ-4», изучить правила его эксплуатации и получить практические навыки работы; составить отчет о проделанной работе и отчитаться по нему у преподавателя.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/14064.
Ознакомление с техническими характеристиками селективного микровольтметра В6-9
Цели: определение спектрально-энергетических характеристик случайных микрофонов, получение практических навыков в работе с селективным микровольтметром В6-9
Содержание: Перед проведением измерений подготовьте прибор к работе в соответствии с инструкцией по эксплуатации. Подключите к телефонной линии низкочастотную радиозакладку (с рабочей частотой до 100 кГц) в режиме микрофона. Подключите микровольтметр к линии и убедитесь в работе закладки путем измерения уровня опасного сигнала в линии в широкополосном режиме. Переведите микровольтметр в селективный режим работы и путем сканирования частотного диапазона найдите максимум опасного сигнала. Для контроля частоты измеряемого сигнала к выходному гнезду микровольтметра с помощью соединительного кабеля подключайте частотомер, а для наблюдения формы сигнала – осциллограф. На основе проведения ряда измерений на близких частотах строится спетрально-энергетическая характеристика закладки. Аналогичным методом исследуются характеристики случайных (паразитных) микрофонов. Хорошие результаты получаются при исследовании динамических громкоговорителей, входящих в состав систем радиотрансляции, оповещения, диспетчерской связи и т.п.
Результаты: Научиться определять спектрально-энергетические характеристики случайных микрофонов; получить практические навыки работы с селективным микровольтметром В6-9; составить отчет о проделанной работе и отчитаться по нему у преподавателя.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/14064.
Назначение, возможности и порядок работы с системой SecretNet Studio.
Цели: Изучить возможности и научиться работать с системой SecretNet Studio.
Содержание: 1. Ознакомление с теоретической частью «Secret Net Studio». 2. Установка программного обеспечения средства защиты информации «Secret Net Studio» на локальный ПК. 3. Подготовка средства защиты информации к инициализации. 4. Инициализация «Secret Net Studio». 5. Подготовка к эксплуатации. 6. Настройка и эксплуатация «Secret Net Studio». 7. Удаление программного обеспечения «Secret Net Studio».
Результаты: - изучить «Secret Net Studio» и научиться устанавливать, настраивать, эксплуатировать и корректно удалять СЗИ с компьютера; - подготовить письменный отчет о проделанной работе и защитить его у преподавателя.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/14064

Назначение и возможности системы защиты от НСД «Dallas Lock».
Цели: Назначение и возможности системы защиты от НСД «Dallas Lock».
Содержание: 1. Если на компьютере уже установлена система защиты, ее необходимо удалить. 2. Необходимо убедиться, что на диске С имеется необходимое свободное пространство для установки системы защиты. 3. Проверить состояние жестких дисков компьютера, например, при помощи приложения chkdsk.exe или служебной программы проверки диска из состава ОС Windows, и устранить выявленные дефекты. 4. Рекомендуется произвести дефрагментацию диска. 5. Проверить компьютер на отсутствие компьютерных вирусов. 6. Перед установкой системы защиты необходимо выгрузить из памяти все резидентные антивирусы. 7. Закрыть все запущенные приложения, так как установка системы потребует принудительной перезагрузки.
Результаты: - изучить и продемонстрировать основные возможности Dallas Lock как системы защиты информации от НСД. - составить отчет о проделанной работе и защитить его у преподавателя.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/14064.

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Темы курсовой работы

Тема 1. Контроль защищённости конфиденциальной информации с помощью селективного микровольтметра В6-9
Тема 2. Акустическое зашумление помещения с помощью прибора SI-3010
Тема 3. Акустическое зашумление помещения с помощью прибора Соната -АВ
Тема 4. Методика поиска и локализации специальных технических средств (СТС) с использованием прибора ST-032 «Пиранья»
Тема 5. Методика защиты каналов передачи информации с использованием генераторов шума
Тема 6. Методика поиска и локализации СТС с помощью детекторов поля
Тема 7. Методика поиска и локализации СТС с использованием поисковых приёмников
Тема 8. Методика использования встроенных межсетевых экранов (МЭ)
Тема 9. Методика работы с МЭ «Secret Net Studio»
Тема 10. Методика работы с системой обнаружения вторжений (СОВ) «Secret Net Studio» Методика работы с МЭ «Dallas Lock»
Тема 11. Методика работы с МЭ «Dallas Lock»
Тема 12. Методика работы с СОВ «Dallas Lock»
Тема 13. Методика использования СЗИ от НСД «Аккорд»
Тема 14. Методика использования СЗИ от НСД «Dallas Lock»
Тема 15. Методика использования СЗИ от НСД «Secret Net Studio»

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Основные задачи контроля состояния ТЗКИ

2. Нормативные и методические документы по контролю ТЗКИ

3. Вопросы, подлежащие проверке при контроле состояния ТЗКИ

4. Классификация видов контроля состояния ТЗКИ

5. Система документации по контролю состояния ТЗКИ

6. Методы и средства контроля защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН

7. Методика оценки защищенности конфиденциальной информации от утечки за счет ПЭМИН с использованием программно-аппаратных комплексов

8. Основные методы контроля защищенности акустической речевой конфиденциальной информации

9. Основные средства контроля защищённости конфиденциальной акустической речевой информации от утечки по техническим каналам

10. Основные методы и средства контроля защищенности конфиденциальной информации от НСД

11. Требования к средствам контроля защищенности акустической речевой информации.

12. Проведение контроля защищенности акустической речевой информации с использованием программно-аппаратных комплексов

13. Методы контроля защищенности конфиденциальной информации от НСД

14. Средства контроля защищенности конфиденциальной информации от НСД

15. Система управления инцидентами ИБ.

16. Способы обнаружения и идентификации инцидентов

17. Контроль за событиями безопасности и действиями в средствах и системах информатизации.

18. Задачи и функции мониторинга информационной безопасности средств и систем информатизации

19. Порядок и методы мониторинга информационной безопасности средств и систем информатизации

20. Контроль (анализ) защищенности информации, содержащейся в средствах и системах информатизации

21. Порядок и метода мониторинга информационной безопасности средств и систем

информатизации

10. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩИХСЯ

Содержание, требования, условия и порядок организации самостоятельной работы обучающихся с учетом формы обучения определяются в соответствии с «Положением об организации самостоятельной работы обучающихся», утвержденным Ученым советом УлГУ (протокол №8/268 от 26.03.2019г.).

По каждой форме обучения: очная/заочная/очно-заочная заполняется отдельная таблица

Форма обучения: очная

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
Раздел 1. Основы организации контроля состояния ТЗКИ			
Тема 1.1. Основные задачи контроля состояния ТЗКИ	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование
Тема 1.2. Организационный и технический контроль состояния ТЗКИ	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование
Раздел 2. Методы и средства контроля защищенности конфиденциальной информации			
Тема 2.1. Методы и средства контроля защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	12	Тестирование
Тема 2.2. Методы и средства контроля защищенности конфиденциальной акустической речевой информации от утечки по техническим каналам	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	8	Тестирование
Тема 2.3. Методы и средства контроля защищенности конфиденциальной информации от НСД	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	8	Тестирование

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
Раздел 3. Мониторинг информационной безопасности средств и систем информатизации			
Тема 3.1. Цели, задачи и функции мониторинга информационной безопасности средств и систем информатизации	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование
Тема 3.2. Обнаружение и идентификация инцидентов безопасности информации	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	8	Тестирование
Тема 3.3. Планирование мер по устранению инцидентов безопасности информации	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование
Тема 3.4. Документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

основная

1. Суворова Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. - 2-е изд. ; пер. и доп. - Москва : Юрайт, 2024. - 277 с. - (Высшее образование). - URL: https://urait.ru/bcode/544029 . - Режим доступа: Электронно-библиотечная система Юрайт, для авториз. пользователей. - ISBN 978-5-534-16450-3 : 1169.00. / .— ISBN 0_529150

2. Гродзенский Я.С. Информационная безопасность : учебное пособие / Я.С. Гродзенский ; Гродзенский Я.С. - Москва : РГ-Пресс, 2020. - 144 с. - URL: https://www.studentlibrary.ru/book/ISBN9785998808456.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-9988-0845-6. / .— ISBN 0_260443

дополнительная

1. Иванцов А. М. Основы информационной безопасности : курс лекций : учебное пособие для студентов специальностей «Компьютерная безопасность» и «Информационная безопасность

автоматизированных систем». Часть 2 / А. М. Иванцов, В. Г. Козловский ; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск : УлГУ, 2020. - Загл. с экрана. - Электрон. текстовые дан. (1 файл : 1,41 МБ). - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/8697. - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_42171

2. Техническая защита информации : учебное пособие / А. С. Раков, О. Н. Маслов, О. Ю. Губарева [и др.] ; Раков А. С.,Маслов О. Н.,Губарева О. Ю.,Почепцов А. О.,Гуреев В. О. - Самара : ПГУТИ, 2020. - 96 с. - Библиогр.: доступна в карточке книги, на сайте ЭБС Лань. - Книга из коллекции ПГУТИ - Информатика. - Режим доступа: ЭБС "Лань"; для авторизир. пользователей. / .— ISBN 0_473609

3. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам : учебное пособие / Г.А. Бузов ; Бузов Г.А. - Москва : Горячая линия - Телеком, 2015. - 586 с. - URL: https://www.studentlibrary.ru/book/ISBN9785991204248.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-9912-0424-8. / .— ISBN 0_251025

учебно-методическая

1. Иванцов А. М. Методические указания для самостоятельной работы студентов по дисциплине «Профессиональный электив. Контроль состояния технической защиты конфиденциальной информации» для студентов специалитета по специальностям 10.05.01 и 10.05.03 очной формы обучения / А. М. Иванцов. - 2022. - 19 с. - Неопубликованный ресурс. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/14064. - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_476683.

б) Программное обеспечение

- Операционная система "Альт образование"
- Офисный пакет "Мой офис"
- Академическая лицензия на УМК ViPNet "Защита сетей"
- Комплект «Максимальная защита» Средства защиты информации Secret Net Studio 8

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2024]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2024]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2024]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг. – Москва, [2024]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2024]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2024]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС **Znanium.com** : электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2024]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2024].

3. eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2024]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2024]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. Российское образование : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: http://www.edu.ru. – Текст : электронный.

6. Электронная библиотечная система УлГУ : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитории для проведения лекций, семинарских занятий, для выполнения лабораторных работ и практикумов, для проведения текущего контроля и промежуточной аттестации, курсового проектирования, групповых и индивидуальных консультаций *(выбрать необходимое)*

Аудитории укомплектованы специализированной мебелью, учебной доской. Аудитории для проведения лекций оборудованы мультимедийным оборудованием для представления информации большой аудитории. Помещения для самостоятельной работы оснащены компьютерный техникой с

возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде, электронно-библиотечной системе. Перечень оборудования, используемого в учебном процессе:

- Мультимедийное оборудование: компьютер/ноутбук, экран, проектор/телевизор
- Компьютерная техника

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации;
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей.

Разработчик	Доцент, Кандидат технических наук, Доцент	Иванцов Андрей Михайлович
	Должность, ученая степень, звание	ФИО