МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное учреждение высшего образования "Пермский государственный национальный исследовательский университет"

Кафедра радиоэлектроники и защиты информации

Авторы-составители: **Лунегов Игорь Владимирович**
Федоренко Андрей Анатольевич

Рабочая программа дисциплины

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Код УМК 94148

Утверждено
Протокол №4
от «24» июня 2021 г.

Пермь, 2021

1. Наименование дисциплины

Техническая защита информации

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в обязательную часть Блока « С.1 » образовательной программы по направлениям подготовки (специальностям):

Специальность: **10.05.03** Информационная безопасность автоматизированных систем
направленность Безопасность открытых информационных систем

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Техническая защита информации** у обучающегося должны быть сформированы следующие компетенции:

10.05.03 Информационная безопасность автоматизированных систем (направленность : Безопасность открытых информационных систем)

УК.1 Способен осуществлять анализ проблемных ситуаций и вырабатывать решение на основе системного подхода

Индикаторы

УК.1.1 Осуществляет поиск информации, производит критическую оценку надежности ее источников

УК.2 Способен управлять проектом, организовывать и руководить работой команды

Индикаторы

УК.2.1 Формулирует на основе поставленной проблемы проектную задачу и предлагает способы ее решения

УК.3 Способен осуществлять коммуникации в рамках академического и профессионального взаимодействия на русском и иностранном языках

Индикаторы

УК.3.3 Представляет результаты деятельности на публичных мероприятиях в устной и письменной формах

УК.3.4 Устанавливает и поддерживает контакты в академическом и профессиональном взаимодействии с использованием современных коммуникативных технологий

ОПК.7 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации

Индикаторы

ОПК.7.2 Применяет методы и средства защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки по техническим каналам, сетей и систем передачи информации при решении профессиональных задач, учитывая текущее состояние и тенденции развития методов и средств обеспечения защиты информации

ОПК.15 Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности

Индикаторы

ОПК.15.1 Анализирует физические явления и процессы, идентифицирует и формулирует проблемы в профессиональной области

ОПК.15.2 Применяет знания физических основ современных информационно-телекоммуникационных технологий для решения профессиональных задач

ПК.6 Способен проводить контроль защищенности информации от утечки по техническим каналам

Индикаторы

ПК.6.1 Проводит специальные исследования на утечку информации по техническим каналам

ПК.6.2 Подготавливает отчетные материалы по результатам специальных исследований

ПК.6.3 Проводит контроль защищенности информации от несанкционированного доступа и специальных воздействий

ОПСК.3 Способен осуществлять контроль обеспечения информационной безопасности и проводить

верификацию данных в открытых информационных системах

Индикаторы

ОПСК.3.2 Определяет источники и причины возникновения инцидентов безопасности в автоматизированных системах

4. Объем и содержание дисциплины

Специальность	10.05.03 Информационная безопасность автоматизированных систем (направленность: Безопасность открытых информационных систем)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	11
Объем дисциплины (з.е.)	5
Объем дисциплины (ак.час.)	180
Контактная работа с преподавателем (ак.час.), в том числе:	70
Проведение лекционных занятий	28
Проведение лабораторных работ, занятий по иностранному языку	42
Самостоятельная работа (ак.час.)	110
Формы текущего контроля	Входное тестирование (1) Защищаемое контрольное мероприятие (3) Итоговое контрольное мероприятие (1)
Формы промежуточной аттестации	Экзамен (11 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Техническая защита информации

Характеристика каналов утечки информации.

Учечки речевой информации. Виброакустический канал утечки информации.
Классификация технических каналов утечки информации: Речевой канал, вибрационно-акустический канал, Канал побочных электромагнитных излучений и наводок (ПЭМИН), радиоканал, канал утечки информации при её транспорте, утечка видовой информации. Краткие технические характеристики каналов утечки информации и природа их возникновения.Особенности утечки речевой информации. Утечка информации по вибрационно-акустическому каналу. Среды передачи информации. Разборчивость речи. Организационно-технические мероприятия по пассивной и активной защите информации от утечек по речевому и вибрационному каналу. Защита от диктофонов и скрытых микрофонов, в том числе и радиомикрофонов.

Утечка информации при передаче по каналам связи.
Утечка информации при передаче по каналам связи. Направленная передача информации. Шифрование. Маскирование сообщений. Применение специальных протоколов обмена информацией. Защищенность радиосети, защищенность радионаправления. Методы борьбы с утечками информации при её транспорте по проводным линиям связи. Утечка информации по телефонным линиям за счет микрофонных эффектов проводных линий и электронных устройств абонентских аппаратов.

Утечка информации по каналам ПЭМИН.
Побочные электромагнитные излучения как источник информации. Примеры ПЭМИН,. потенциально опасных носителей информации. Методы защиты от ПЭМИН.

Закладные устройства и защита от них.
Закладные устройства. Скрытые радиомикрофоны, микрофоны и диктофоны, средства борьбы с закладными устройствами. Средства радиомониторинга, организационно-технические меры.

Средства обнаружения каналов утечки информации.

Индикаторы электромагнитного поля. Радиоприёмные устройства.
Принцип действия индикаторов электромагнитного поля и специальных измерительных радиоприемных устройств, селективных радиочастотных микровольтметров и панорамных анализаторов спектра. Технические характеристики устройств радиомониторинга. Специфика их применения для обнаружения каналов утечки информации.

Автоматизированные поисковые системы.
Специальные комплексы для проведения радиомониторинга. Программно-аппаратные комплексы Крона. СЗИ Касандра. СЗИ Филин. Принцип корреляционного анализа для идентификации источника утечки информации.

Нелинейные локаторы.
Поиск срытых средств передачи информации с помощью нелинейных локаторов. Принцип действия нелинейных локаторов.

Досмотровая техника.
Нелинейные локаторы, рентгеновские установки, металлоискатели и металлодетекторы. принципы действия и практика применения.

Организация технической защиты информации.

Организационно-методические основы защиты информации.

Организация защиты информации на предприятиях. Комплекс мер по защите информации. политика Информационной безопасности предприятия.

Методика принятия решения на защиту информации.

Анализ возможных угроз утечки информации. Выявление каналов утечки информации. Определения наиболее эфФективных средств защиты информации.

Организация защиты информации.

Рекомендации по защите информации для предприятия. Определение угроз и рисков информационной безопасности предприятия. Выявление каналов утечки информации. Аттестационная и лицензионная деятельность. Работа с персоналом.

Методы защиты информации.

Организация защиты речевой информации.

Защита речевой информации. Пассивная защита. Организационные меры по защите речевой информации. . Активная защита речевой информации.

Защита от утечек по ПЭМИН.

Защита от ПЭМИН. Применение аттестованных средств обработки информации. Снижение ПЭМИН. Активная защита от ПЭМИН. Организационные меры по защите информации от утечек по каналу ПЭМИН.

Защита от утечек информации при транспортировке информации.

Методы защиты информации при её передаче по каналам связи. Направленная радиосвязь. Маскирование.Шифрование.

Мероприятия по выявлению технических каналов утечки информации.

Специальные проверки.Специальные обследования.Специальные исследования.

Методика проведения специальных проверок для выявления угроз утечки информации. Обследования помещений, и средств передачи, обработки и хранения информации, на предмет возможных утечек информации. Проведение специальных исследований. Экспериментальное обнаружение источника утечки информации.

6. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы. Обучающемуся важно помнить, что контактная работа с преподавателем эффективно помогает ему овладеть программным материалом благодаря расстановке необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации.

Самостоятельная работа преследует следующие цели:

– закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;

- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;

- совершенствование навыков поиска научных публикаций и образовательных ресурсов, размещенных в сети Интернет;

- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем во время проведения мероприятий текущего контроля и учитываются при промежуточной аттестации.

Обучающимся с ОВЗ и инвалидов предоставляется возможность выбора форм проведения мероприятий текущего контроля, альтернативных формам, предусмотренным рабочей программой дисциплины. Предусматривается возможность увеличения в пределах 1 академического часа времени, отводимого на выполнение контрольных мероприятий.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации.

При проведении текущего контроля применяются оценочные средства, обеспечивающие передачу информации, от обучающегося к преподавателю, с учетом психофизиологических особенностей здоровья обучающихся.

7. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

При самостоятельной работе обучающимся следует использовать:

– конспекты лекций;

– литературу из перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля);

– текст лекций на электронных носителях;

– ресурсы информационно-телекоммуникационной сети "Интернет", необходимые для освоения дисциплины;

– лицензионное и свободно распространяемое программное обеспечение из перечня информационных технологий, используемых при осуществлении образовательного процесса по дисциплине;

– методические указания для обучающихся по освоению дисциплины.

8. Перечень основной и дополнительной учебной литературы

Основная:

1. Титов, А. А. Инженерно-техническая защита информации : учебное пособие / А. А. Титов. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. — 197 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/13931

2. Голиков, А. М. Защита информации от утечки по техническим каналам : учебное пособие / А. М. Голиков. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. — 256 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/72090.html

Дополнительная:

1. Методические указания и контрольные задания по дисциплине Инженерно-техническая защита информации / составители А. С. Большаков, Т. Б. К. Режеб. — Москва : Московский технический университет связи и информатики, 2013. — 149 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. http://www.iprbookshop.ru/61734.html

2. Титов, А. А. Инженерно-техническая защита информации : учебное пособие / А. А. Титов. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. — 197 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/13931

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

ttps://studopedia.ru/11_70141_tehnicheskie-sredstva-zashchiti-informatsii.html Определения

https://dic.academic.ru/dic.nsf/ruwiki/200171 Основные понятия

https://www.intuit.ru/studies/courses/3649/891/lecture/32330 Технические каналы утечки

https://allgosts.ru/35/020/gost_r_56546-2015 ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем

https://studfile.net/preview/5274317/page:2/ Классификация каналов утечки информации

https://studopedia.ru/7_139964_kanali-utechki-rechevoy-informatsii.html Каналы утечки речевой информации

http://www.delphiplus.org/zashchita-informatsii-vas-podslushivayut-zashchishchaites/akusticheskii-i-vibroakusticheskii-kanaly-utechki-informatsii.html акустический и вибрационный каналы утечки информации

https://itsec2012.ru/kanaly-utechki-informacii-pri-ee-peredache-po-kanalam-svyazi Утечка информации при передаче по каналам связи.

https://studfile.net/preview/2140979/page:34/ Методы защиты информации при передаче по каналам связи

https://studopedia.ru/7_139967_obshchie-harakteristiki-zakladnih-ustroystv.html Классификация закладных устройств

https://studopedia.ru/18_70432_i-lokalizatsii-zakladnih-podslushivayushchih-ustroystv.html Обнаружение закладных устройств

https://www.intuit.ru/studies/courses/2291/591/lecture/12705 Средства обнаружения каналов утечки информации.

https://studopedia.org/5-112986.html Индикаторы электромагнитного поля.

https://studopedia.ru/5_3743_radiopriemnie-ustroystva.html Измерительные радиоприемные устройства.

https://bstudy.net/650396/informatika/sredstva_poiska_zakladnyh_ustroystv_sema_informatsii Средства поиска закладных устройств съема информации

https://www.vbkom.ru/catalog/antiterroresticheskoe-oborudovanie/search-spy-gadgets-/automated-systems-of-radio-monitoring-search-eavesdropping-devices/ Актуальная техника поиска закладных устройств

https://studopedia.ru/7_139970_nelineynie-lokatori.html Нелинейные локаторы

https://studfile.net/preview/4328973/ Нелинейные локаторы. Принцип действия и основные характеристики

https://studopedia.ru/9_84193_ponyatie-i-klassifikatsiya-dosmotrovo-poiskovoy-tehniki.html Понятие и классификация досмотрово-поисковой техники

http://www.bnti.ru/showart.asp?aid=738&lvl=03. История развития досмотровой техники

https://studopedia.ru/18_70441_organizatsiya-inzhenerno-tehnicheskoy-zashchiti-informatsii-na-predpriyatiyah-v-organizatsiyah-uchrezhdeniyah.html Организация технической защиты информации.

https://moodle.kstu.ru/pluginfile.php/106824/mod_resource/content/1/Тема%209%20Лекция%209.docx Лекция. Организация зашиты информации.

https://infopedia.su/17x8d52.html Организационно-методические основы защиты информации

https://studopedia.ru/3_2172_lektsiya--metodologicheskie-osnovi-kompleksnoy-sistemi-zashchiti-informatsii.html Методологические основы комплексной системы защиты информации.

http://www.delphiplus.org/zashchita-ot-utechki-informatsii-po-tekhnicheskim-kanalam/metodika-

prinyatiya-resheniya-na-zashchitu-ot-utechki-informatsii-v-organizatsii.html Методика принятия решения о мерах по защите информации

https://studopedia.ru/3_36997_organizatsiya-zashchiti-informatsii-na-predpriyatii.html Организация защиты информации на предприятии

https://pandia.ru/text/77/158/16343.php Защита информации на предприятиях

http://www.consultant.ru/document/cons_doc_LAW_97942/6c8c47dee62ef44bc96df707618c35c8ae9de642/ Приказ ФСТЭК РФ от 05.02.2010 N 58 "Об утверждении Положения о методах и способах защиты информации в информационных системах персональн

http://www.delphiplus.org/zashchita-ot-utechki-informatsii-po-tekhnicheskim-kanalam/organizatsiya-zashchity-rechevoi-informatsii.html Организация защиты речевой информации.

http://www.bnti.ru/showart.asp?aid=814&lvl=04.03.01. Защита речевой информации руководителя организации от скрытой записи посетителем.

http://www.delphiplus.org/zashchita-ot-utechki-informatsii-po-tekhnicheskim-kanalam/organizatsiya-zashchity-informatsii-ot-utechki-voznikayushchei-pri-rabote-vychislitelnoi-tekhniki-za-schet-pemin.html Защита от утечек по ПЭМИН.

https://fstec.ru/component/attachments/download/296 Руководязий документ. ФСТЕК.

https://www.intuit.ru/studies/courses/3649/891/lecture/32349 Защита информации от НСД

https://studfile.net/preview/5868802/page:21/ Специальные исследования в области защиты информации.

https://studopedia.ru/9_84224_spetsialnie-issledovaniya-pomeshcheniy.html Специальные исследования помещений

https://studbooks.net/2206208/informatika/organizatsionno_tehnicheskie_meropriyatiya_tehnicheskie_sposoby_zaschity_informatsii_zaschischaemogo_pomescheniya Организационно-технические мероприятия и технические способы защиты информации защищаемого помещения

https://studfile.net/preview/7005592/page:59/ Порядок проведения специальной проверки технических средств

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Образовательный процесс по дисциплине **Техническая защита информации** предполагает использование следующего программного обеспечения и информационных справочных систем:
Образовательный процесс по дисциплине предполагает использование следующего информационных технологий, программного обеспечения и информационных справочных систем:
-презентационные материалы (слайды по темам лекционных и практических занятий);
- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательной среду университета (ЕТИС ПГНИУ);
- интернет-сервисы и электронные ресурсы (поисковые системы, электронная почта, профессиональные тематические чаты и форумы, системы аудио и видео конференций, онлайн энциклопедии и т.д.).
Перечень используемого программного обеспечения:
- открытая система "ALT Linux"
- офисный пакет приложений "Libreoffice";
- приложение позволяющее просматривать и воспроизводить медиа контент PDF-файлов "AdobeAcrobatReader DC";

- программы демонстрации видео материалов (проигрыватель) "WindowsMediaPlaer";
- программа просмотра интернет контента (браузер) "GoogleChrome

При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ (**student.psu.ru**).

При организации дистанционной работы и проведении занятий в режиме онлайн могут использоваться:

система видеоконференцсвязи на основе платформы BigBlueButton (https://bigbluebutton.org/).

система LMS Moodle (http://e-learn.psu.ru/), которая поддерживает возможность использования текстовых материалов и презентаций, аудио- и видеоконтент, а так же тесты, проверяемые задания, задания для совместной работы.

система тестирования Indigo (https://indigotech.ru/).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия, занятия семинарского типа (семинары, практические занятия), групповые (индивидуальные) консультации, мероприятия текущего контроля и промежуточной аттестации проводятся в аудитории, оснащенной презентационной техникой (проектор, экран для проектора,компьютер/ноутбук), а также меловой (и) или маркерной доской.

Лабораторные занятия проводятся в лаборатории радиотехнических средств зашиты информации с техническим оснащением, представленным в паспорте лаборатории с учебными местами:
цифровые вольтметры, генераторы сигналов, лабораторные источники питания, осциллографы, анализаторы спектра, измерительные приёмники, измерительные антенны. Нелинейный локатор, СЗИ Барон, Программно-аппаратные комплексы: Касандра, Крона, Пиранья.

Самостоятельная работа. Лаборатория радиотехнических средств зашиты информации, помещения Научной библиотеки ПГНИУ, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет», обеспеченные доступом в электронную информационно-образовательную среду университета

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:

1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютера с доступом к локальной и глобальной компьютерным сетям.
2. Читальный зал гуманитарной литературы, корп. 2, ауд. 418. Оборудован 7 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
3. Читальный зал естественной литературы, корп.6, ауд. 107а. Оборудован 5 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
4. Отдел иностранной литературы, корп.2 ауд. 207. Оборудован 1 персональным компьютером с доступом к локальной и глобальной компьютерным сетям.
5. Библиотека юридического факультета, корп.9, ауд. 4. Оборудована 11 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
6. Читальный зал географического факультета, корп.8, ауд. 419. Оборудован 6 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

Все компьютеры, установленные в помещениях научной библиотеки, оснащены следующим программным обеспечением:

Операционная система ALT Linux;
Офисный пакет Libreoffice.
Справочно-правовая система «КонсультантПлюс»

Фонды оценочных средств для аттестации по дисциплине
Техническая защита информации

Планируемые результаты обучения по дисциплине для формирования компетенции. Индикаторы и критерии их оценивания

ОПК.15

Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.15.1 Анализирует физические явления и процессы, идентифицирует и формулирует проблемы в профессиональной области	Знать физические законы и явления, наблюдаемые в задачах, связанных с утечками информации по техническим каналам, уметь распознавать, классифицировать каналы утечки информации, владеть методами обнаружения утечек по техническим каналам и методами устранения утечек информации.	**Неудовлетворител** Не знает физические законы и явления, наблюдаемые в задачах, связанных с утечками информации по техническим каналам, не умеет распознавать, классифицировать каналы утечки информации, не владеет методами обнаружения утечек по техническим каналам и методами устранения утечек информации. **Удовлетворительн** Знает некоторые физические законы и явления, наблюдаемые в задачах, связанных с утечками информации по техническим каналам, в основном умеет распознавать, классифицировать каналы утечки информации, владеет методами обнаружения утечек по некоторым техническим каналам и некоторыми методами устранения утечек информации. **Хорошо** В основном знает физические законы и явления, наблюдаемые в задачах, связанных с утечками информации по техническим каналам, умеет распознавать, классифицировать каналы утечки информации, в основном владеет методами обнаружения утечек по техническим каналам и методами устранения утечек информации. **Отлично** Знает физические законы и явления, наблюдаемые в задачах, связанных с утечками информации по техническим каналам, умеет распознавать, классифицировать каналы утечки информации, владеет методами обнаружения

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично утечек по техническим каналам и методами устранения утечек информации.
ОПК.15.2 Применяет знания физических основ современных информационно-телекоммуникационных технологий для решения профессиональных задач	Студент знает физические основы современных информационно-телекоммуникационных технологий, умеет решать задачи в сфере информационной безопасности, владеет методами анализа проблем и их решения.	**Неудовлетворител** Студент не знает физические основы современных информационно-телекоммуникационных технологий, не умеет решать задачи в сфере информационной безопасности, не владеет методами анализа проблем и их решения **Удовлетворительн** Студент знает некоторые физические основы современных информационно-телекоммуникационных технологий, в основном умеет решать задачи в сфере информационной безопасности, владеет некоторыми методами анализа проблем и их решения **Хорошо** Студент знает физические основы современных информационно-телекоммуникационных технологий, умеет решать задачи в сфере информационной безопасности, владеет методами анализа проблем и их решения **Отлично** Студент знает физические основы современных информационно-телекоммуникационных технологий, умеет решать задачи в сфере информационной безопасности, владеет методами анализа проблем и их решения. Способен организовать работу коллектива.

ОПК.7

Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.7.2 Применяет методы и средства защиты	Студент знает методы и средства защиты информации в операционных системах,	**Неудовлетворител** Студент не знает методы и средства защиты информации, не умеет использовать методы

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки по техническим каналам, сетей и систем передачи информации при решении профессиональных задач, учитывая текущее состояние и тенденции развития методов и средств обеспечения защиты информации	компьютерных сетях и системах управления базами данных, умеет использовать методы и средства защиты информации от утечки по техническим каналам, сетей и систем передачи информации, владеет методами решения профессиональных задач, учитывая текущее состояние и тенденции развития методов и средств обеспечения защиты информации	**Неудовлетворител** и средства защиты информации от утечки по техническим каналам, не владеет методами решения профессиональных задач. **Удовлетворительн** Студент в основном знает методы и средства защиты информации, умеет использовать методы и средства защиты информации от утечки по техническим каналам, владеет некоторыми методами решения задач информационной безопасности. **Хорошо** Студент знает методы и средства защиты информации, компьютерных сетях, умеет использовать методы и средства защиты информации от утечки по техническим каналам, , владеет методами решения профессиональных задач в сфере защиты информации. **Отлично** Студент в совершенстве знает методы и средства защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, умеет использовать методы и средства защиты информации от утечки по техническим каналам, сетей и систем передачи информации, владеет методами поиска, исследования технических каналов утечки информации и методы их нейтрализации или устранения.

ОПСК.3

Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПСК.3.2 Определяет источники и причины возникновения инцидентов безопасности в автоматизированных	Должен знать основные причины возникновения угроз безопасности, уметь анализировать уязвимости систем обработки и передачи информации, владеть методами оценки вероятности угроз.	**Неудовлетворител** Студент не знает основные причины возникновения угроз безопасности, не умеет анализировать уязвимости систем обработки и передачи информации, не владеет методами оценки вероятности угроз. **Удовлетворительн**

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
системах		**Удовлетворительн** Студент в основном знает основные причины возникновения угроз безопасности, в основном умеет анализировать уязвимости систем обработки и передачи информации не, владеет методами оценки вероятности угроз. **Хорошо** Студент знает основные причины возникновения угроз безопасности, умеет анализировать уязвимости систем обработки и передачи информации, владеет методами оценки вероятности угроз. **Отлично** Студент знает основные причины возникновения угроз безопасности, умеет анализировать уязвимости систем обработки и передачи информации, владеет методами оценки вероятности угроз. Студент обладает способностью организации работ по информационной безопасности.

ПК.6

Способен проводить контроль защищенности информации от утечки по техническим каналам

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.6.2 Подготавливает отчетные материалы по результатам специальных исследований	Студент знает основные правила подготовки технической документации по результатам специальных исследований, умеет оформлять материалы в соответствие с установленными требованиями, владеет приёмами делопроизводителя и оформительскими приемами.	**Неудовлетворител** Студент не знает основные правила подготовки технической документации по результатам специальных исследований, не умеет оформлять материалы в соответствие с установленными требованиями, не владеет приёмами делопроизводителя и оформительскими приемами. **Удовлетворительн** Студент знает некоторые правила подготовки технической документации по результатам специальных исследований, в основном умеет оформлять материалы в соответствие с установленными требованиями, не владеет приёмами делопроизводителя и оформительскими приемами. **Хорошо**

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо Студент знает основные правила подготовки технической документации по результатам специальных исследований, умеет оформлять материалы в соответствие с установленными требованиями, владеет некоторыми приёмами делопроизводителя и оформительскими приемами. **Отлично** Студент знает основные правила подготовки технической документации по результатам специальных исследований, умеет оформлять материалы в соответствие с установленными требованиями, владеет приёмами делопроизводителя и оформительскими приемами.
ПК.6.3 Проводит контроль защищенности информации от несанкционированного доступа и специальных воздействий	Студент знает методы оценки и контроля защищенности информации от несанкционированного доступа и специальных воздействий, владеет приёмами оценки рисков, угроз и уязвимостей информационных систем, умеет выбирать решения по снижению рисков и ликвидации угроз информационным системам.	**Неудовлетворител** Студент не знает методы оценки и контроля защищенности информации от несанкционированного доступа и специальных воздействий, не владеет приёмами оценки рисков, угроз и уязвимостей информационных систем, не умеет выбирать решения по снижению рисков и ликвидации угроз информационным системам. **Удовлетворительн** Студент знает некоторые методы оценки и контроля защищенности информации от несанкционированного доступа и специальных воздействий, не владеет приёмами оценки рисков, угроз и уязвимостей информационных систем, умеет выбирать решения по снижению рисков и ликвидации угроз информационным системам. **Хорошо** Студент знает основные методы оценки и контроля защищенности информации от несанкционированного доступа и специальных воздействий, владеет приёмами оценки рисков, угроз и уязвимостей информационных систем, умеет выбирать решения по снижению рисков и ликвидации угроз информационным системам.

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично Студент в совершенстве знает методы оценки и контроля защищенности информации от несанкционированного доступа и специальных воздействий, владеет приёмами оценки рисков, угроз и уязвимостей информационных систем, умеет выбирать решения по снижению рисков и ликвидации угроз информационным системам.
ПК.6.1 Проводит специальные исследования на утечку информации по техническим каналам	Студент знает основные соотношения между физическими величинами и физические явления, связанные с информационной безопасностью, умеет применять контрольно-измерительную аппаратуру при проведении специальных исследований, владеет приемами проведения специальных исследований.	**Неудовлетворител** Студент не знает основные соотношения между физическими величинами и физические явления, связанные с информационной безопасностью, не умеет применять контрольно-измерительную аппаратуру при проведении специальных исследований, не владеет приемами проведения специальных исследований. **Удовлетворительн** Студент знает основные соотношения между физическими величинами и физические явления, связанные с информационной безопасностью, в основном умеет применять контрольно-измерительную аппаратуру при проведении специальных исследований, владеет некоторыми приемами проведения специальных исследований. **Хорошо** Студент знает основные соотношения между физическими величинами и физические явления, связанные с информационной безопасностью, умеет применять контрольно-измерительную аппаратуру при проведении специальных исследований, владеет приемами проведения специальных исследований. **Отлично** Студент знает основные соотношения между физическими величинами и физические явления, связанные с информационной безопасностью, умеет применять контрольно-измерительную аппаратуру при проведении специальных исследований, владеет приемами проведения специальных

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично исследований. Владеет поиском и подготовкой документации, и умеет организовывать специальные исследования.

УК.1

Способен осуществлять анализ проблемных ситуаций и вырабатывать решение на основе системного подхода

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
УК.1.1 Осуществляет поиск информации, производит критическую оценку надежности ее источников	Студент знает основные приёмы, позволяющие получить информацию, умеет оценивать достоверность информации и надежность источников, владеет приёмами проверки информации.	**Неудовлетворител** Студент не знает основные приёмы, позволяющие получить информацию, доверяет сомнительной информации из ненадёжных источников, не умеет оценивать достоверность информации и надежность источников, не владеет приёмами проверки информации. **Удовлетворительн** Студент знает основные приёмы, позволяющие получить информацию, но иногда не в состоянии критически её оценивать, не умеет оценивать достоверность информации и надежность источников, владеет некоторыми приёмами проверки информации. **Хорошо** Студент знает основные приёмы, позволяющие получить информацию, умеет оценивать достоверность информации и надежность источников, доверяет только надёжным источникам , т.к. слабо владеет приёмами проверки информации. **Отлично** Студент знает основные приёмы, позволяющие получить информацию, умеет оценивать достоверность информации и надежность источников, владеет приёмами проверки информации.

УК.2

Способен управлять проектом, организовывать и руководить работой команды

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
УК.2.1 Формулирует на основе поставленной проблемы проектную задачу и предлагает способы ее решения	Студент знает способы решения проектных задач, умеет ставить задачи, умеет структурировать проектную деятельность, владеет приемами организации проектной задачи.	**Неудовлетворител** Студент не знает способы решения проектных задач, не умеет ставить задачи, не умеет структурировать проектную деятельность, не владеет приемами организации проектной задачи. **Удовлетворительн** Студент знает способы решения отдельных проектных задач, умеет ставить задачи, не умеет структурировать проектную деятельность, не владеет приемами организации проектной задачи. **Хорошо** Студент знает способы решения проектных задач, умеет ставить задачи, умеет структурировать проектную деятельность, владеет приемами организации проектной задачи. в проетной работе совершает незначительные ошибки. **Отлично** Студент знает способы решения проектных задач, умеет ставить задачи, умеет структурировать проектную деятельность, владеет приемами организации проектной задачи.

УК.3

Способен осуществлять коммуникации в рамках академического и профессионального взаимодействия на русском и иностранном языках

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
УК.3.3 Представляет результаты деятельности на публичных мероприятиях в устной и письменной формах	Студент знает правила проведения публичных научных выступлений, умеет оформлять иллюстративный материал для научных докладов, владеет навыками ведения научной дискуссии.	**Неудовлетворител** Студент не знает правила проведения публичных научных выступлений, не умеет оформлять иллюстративный материал для научных докладов, не владеет навыками ведения научной дискуссии. **Удовлетворительн** Студент в основном знает правила проведения публичных научных выступлений, умеет оформлять иллюстративный материал для научных докладов, в соновном владеет навыками

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительн ведения научной дискуссии. **Хорошо** Студент знает правила проведения публичных научных выступлений, умеет оформлять иллюстративный материал для научных докладов, владеет навыками ведения научной дискуссии. **Отлично** Студент знает правила проведения публичных научных выступлений, умеет оформлять иллюстративный материал для научных докладов, владеет навыками ведения научной дискуссии. Владеет приемами защиты научной истины и убеждения оппонентов.
УК.3.4 Устанавливает и поддерживает контакты в академическом и профессиональном взаимодействии с использованием современных коммуникативных технологий	Студент знает правила общения в академическом и профессиональном сообществе, умеет применять современные коммуникационные возможности, владеет методами ведения научной и деловой беседы.	**Неудовлетворител** Студент не знает правила общения в академическом и профессиональном сообществе, не умеет применять современные коммуникационные возможности, не владеет методами ведения научной и деловой беседы. **Удовлетворительн** Студент знает некоторые правила общения в академическом и профессиональном сообществе, в основном умеет применять современные коммуникационные возможности. **Хорошо** Студент знает правила общения в академическом и профессиональном сообществе, умеет применять современные коммуникационные возможности, владеет методами ведения научной и деловой беседы. **Отлично** Студент знает правила общения в академическом и профессиональном сообществе, умеет применять современные коммуникационные возможности, владеет методами ведения научной и деловой беседы. Студент в состоянии наладить отношения с новыми коллективами и

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично отдельными персонами и вовлечь их в свой проект.

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Базовая

Вид мероприятия промежуточной аттестации : Экзамен
Способ проведения мероприятия промежуточной аттестации : Оценка по дисциплине в рамках промежуточной аттестации определяется на основе баллов, набранных обучающимся на контрольных мероприятиях, проводимых в течение учебного периода.
Максимальное количество баллов : 100

Конвертация баллов в отметки

«отлично» - от 81 до 100
«хорошо» - от 61 до 80
«удовлетворительно» - от 44 до 60
«неудовлетворительно» / «незачтено» менее 44 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
Входной контроль	Учечки речевой информации. Виброакустический канал утечки информации. **Входное тестирование**	проверка остаточных знаний по электричеству и магнетизму, радиоэлектронике, методам радиофизических измерений

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
УК.2.1 Формулирует на основе поставленной проблемы проектную задачу и предлагает способы ее решения **ОПСК.3.2** Определяет источники и причины возникновения инцидентов безопасности в автоматизированных системах **ПК.6.1** Проводит специальные исследования на утечку информации по техническим каналам **ПК.6.3** Проводит контроль защищенности информации от несанкционированного доступа и специальных воздействий **ПК.6.2** Подготавливает отчетные материалы по результатам специальных исследований **ОПК.15.1** Анализирует физические явления и процессы, идентифицирует и формулирует проблемы в профессиональной области **ОПК.15.2** Применяет знания физических основ современных информационно-телекоммуникационных технологий для решения профессиональных задач	Досмотровая техника. **Защищаемое контрольное мероприятие**	Проверка знаний техники безопасности.Принцип действия технических средств защиты информации , проверка навыков использования технических средств.для поиска утечек информации.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
УК.1.1 Осуществляет поиск информации, производит критическую оценку надежности ее источников **УК.2.1** Формулирует на основе поставленной проблемы проектную задачу и предлагает способы ее решения **УК.3.4** Устанавливает и поддерживает контакты в академическом и профессиональном взаимодействии с использованием современных коммуникативных технологий **ОПК.7.2** Применяет методы и средства защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки по техническим каналам, сетей и систем передачи информации при решении профессиональных задач, учитывая текущее состояние и тенденции развития методов и средств обеспечения защиты информации **ОПК.15.2** Применяет знания физических основ современных информационно-телекоммуникационных технологий для решения профессиональных задач	Организация защиты информации. **Защищаемое контрольное мероприятие**	Проверка знаний основных принципов работы оборудования, методики проведения экспериментально-исследовательских работ, Умений использования контрольно-измерительное и прочее оборудование, необходимое для проведения аттестационных мероприятий.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
УК.1.1 Осуществляет поиск информации, производит критическую оценку надежности ее источников **УК.2.1** Формулирует на основе поставленной проблемы проектную задачу и предлагает способы ее решения **ПК.6.2** Подготавливает отчетные материалы по результатам специальных исследований **ПК.6.3** Проводит контроль защищенности информации от несанкционированного доступа и специальных воздействий **ОПК.15.1** Анализирует физические явления и процессы, идентифицирует и формулирует проблемы в профессиональной области **ОПК.15.2** Применяет знания физических основ современных информационно-телекоммуникационных технологий для решения профессиональных задач	Защита от утечек информации при транспортировке информации. **Защищаемое контрольное мероприятие**	Проверка знаний в области систем передачи информации, обнаружение утечек информации при её транспорте. Защита информации, обрабатываемой и передаваемой по линиям связи.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
УК.3.3 Представляет результаты деятельности на публичных мероприятиях в устной и письменной формах **УК.3.4** Устанавливает и поддерживает контакты в академическом и профессиональном взаимодействии с использованием современных коммуникативных технологий **ПК.6.1** Проводит специальные исследования на утечку информации по техническим каналам **ОПК.15.2** Применяет знания физических основ современных информационно-телекоммуникационных технологий для решения профессиональных задач	Специальные проверки.Специальные обследования.Специальные исследования. **Итоговое контрольное мероприятие**	Характеристика каналов утечки информации. Организация защиты информации на предприятиях. Комплекс мер по защите информации. Каналы утечки информационных систем. Специальные исследования. Утечки речевой информации. Специальные обследования. Виброакустический канал утечки информации. Утечка информации при передаче по каналам связи. Утечки видовой информации. Закладные устройства. Скрытые радиомикрофоны, микрофоны и диктофоны. Несанкционированный доступ к информации.. Утечка информации по каналам ПЭМИН.. Средства обнаружения каналов утечки информации.. Индикаторы электромагнитного поля. Пассивная защита. активные средства защиты информации. Измерительные радиоприёмные устройства. Исследование спектральных характеристик сигналов.Политика информационной безопасности предприятия. Автоматизированные поисковые системы. Нелинейные локаторы. Металлодетекторы. Принцип корреляционного анализа для идентификации источника утечки Разборчивость речи.

Спецификация мероприятий текущего контроля

Учечки речевой информации. Виброакустический канал утечки информации.

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **0**
Проходной балл: **0**

Показатели оценивания	Баллы
Допущено не более 10% ошибок при тестировании	81
Допущено не более 30% ошибок при тестировании	61

Допущено не более 50% ошибок при тестировании	41
Допущено более 50% ошибок при тестировании	0

Досмотровая техника.

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**
Проходной балл: **9**

Показатели оценивания	Баллы
Выполнение лабораторной работы	5
Обсуждение результатов измерений	5
Ответы на вопросы по теме лабораторной работы.	5
Представление результатов лабораторной работы	5

Организация защиты информации.

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**
Проходной балл: **9**

Показатели оценивания	Баллы
Выполнение заданий лабораторной работы	5
Ответы на вопросы по теме лабораторной работы	5
Объяснение результатов экспериментов	5
Оформление и представление результатов измерений.	5

Защита от утечек информации при транспортировке информации.

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**
Проходной балл: **9**

Показатели оценивания	Баллы
Выполнение заданий лабораторных работ	5
Ответы на вопросы по темам лабораторных работ	5
Объяснение результатов экспериментов	5
Оформление и представление результатов измерений	5

Специальные проверки.Специальные обследования.Специальные исследования.

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**

Проходной балл: **17**

Показатели оценивания	**Баллы**
Ответ на вопрос №2 экзаменационного билета	12
Ответ на вопрос №1 экзаменационного билета	12
Ответ на дополнительный вопрос по теме вопроса №2 экзаменационного билета	8
Ответ на дополнительный вопрос по теме вопроса №1 экзаменационного билета	8