МИНОБРНАУКИ РОССИИ

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

Кафедра радиоэлектроники и защиты информации

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

Рабочая программа дисциплины

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Код УМК 81658

Утверждено
Протокол №4
от «24» июня 2020 г.

Пермь, 2020

1. Наименование дисциплины

Техническая защита информации

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в базовую 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)

ОПК.6 способность применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций

ПК.15 способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации

ПК.16 способность участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты автоматизированных систем

ПК.17 способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных требований по защите информации

ПК.18 способность проводить инструментальный мониторинг защищенности автоматизированных систем

4. Объем и содержание дисциплины

Направления подготовки	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.)	6
Объем дисциплины (ак.час.)	216
Контактная работа с преподавателем (ак.час.), в том числе:	84
Проведение лекционных занятий	42
Проведение практических занятий, семинаров	0
Проведение лабораторных работ, занятий по иностранному языку	42
Самостоятельная работа (ак.час.)	132
Формы текущего контроля	Входное тестирование (1) Защищаемое контрольное мероприятие (2) Итоговое контрольное мероприятие (1)
Формы промежуточной аттестации	Экзамен (11 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Техническая защита информации. Первый семестр

Характеристика каналов утечки информации.

Каналы утечки информационных систем.
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.

Учечки речевой информации. Виброакустический канал утечки информации.
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.

Утечки видовой информации. Несанкционированный доступ к информации.
Защита от утечек информации по видовому каналу. Организационные меры, необходимые для устранения возможности утечек информации по видовому каналу. Потенциальные угрозы: Окна, камеры виденаблюдения охранных систем, Веб-камеры персональных компьютеров. Специальные средства видеонаблюдения, приборы ночного видения.

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. Техничееские 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.

Защита от НСД.

Защита от несанкционированного доступа в помещения предприятия. Защита от .НСД к информационным системам. Защита от НСД в сети.

Мероприятия по выявлению технических каналов утечки информации.

Специальные проверки.

Методика проведения специальных проверок для выявления угроз утечки информации.

Специальные обследования.

Обследования помещений, и средств передачи, обработки и хранения информации, на предмет возможных утечек информации.

Специальные исследования.

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. Технические средства защиты информации : учебное пособие / А. А. Титов. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. — 194 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/13989

2. Башлы, П. Н. Информационная безопасность и защита информации : учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. — Москва : Евразийский открытый институт, 2012. — 311 с. — ISBN 978-5-374-00301-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/10677

3. Гуляев В. П. Анализ демаскирующих признаков объектов информатизации и технических каналов утечки информации:Учебно-методический комплект/Гуляев В. П..-Екатеринбург:Уральский федеральный университет, ЭБС АСВ,2014, ISBN 978-5-7996-1120-0.-164. http://www.iprbookshop.ru/68221.html

Дополнительная:

1. Методические указания и контрольные задания по дисциплине Инженерно-техническая защита информации/сост.: А. С. Большаков, Режеб Бен.-Москва:Московский технический университет связи и информатики,2013.-149. 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

https://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://studfile.net/preview/304025/page:7/ Лекция. Технические каналы утечки.

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

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

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/8_120962_ugrozi-utechki-vidovoy-informatsii.html угрозы утечки видовой информации

https://fstec.ru/component/attachments/download/298 Несанкционированный доступ .Руководящий документ.

https://studopedia.ru/3_37317_sredstva-viyavleniya-i-zashchiti-ot-pemin.html ПЭМИН

http://stsz.ru/info/articles/zashchita-informatsii-ot-utechki-za-schyet-pemin-v-korporativnoy-seti-predpriyatiya/ Защита информации от утечки за счёт ПЭМИН в корпоративной сети предприятия.

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://studfile.net/preview/2713907/page:4/ Защита от утечек по техническим каналам

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 НА ЗАЩИТУ ОТ УТЕЧКИ ИНФОРМАЦИИ В ОРГАНИЗАЦИИ

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

https://pandia.ru/text/77/158/16343.php Организация защиты 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 ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ, ВОЗНИКАЮЩЕЙ ПРИ РАБОТЕ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ, ЗА СЧЕТ ПЭМИН

https://studopedia.ru/19_373718_meri-metodi-i-sredstva-obespecheniya-trebuemogo-urovnya-zashchishchennosti-informatsionnih-resursov.html Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов

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://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

https://studopedia.ru/17_1112_izuchenie-osobennostey-attestatsii-pomeshcheniy-po-trebovaniyam-bezopasnosti-informatsii.html Изучение особенностей аттестации помещений по требованиям безопасности информации

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

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 и критерии их оценивания

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.18 способность проводить инструментальный мониторинг защищенности автоматизированных систем	Знать основные методы оценки защищенности автоматизированных систем уметь выполнять исследования защищенности автоматизированных систем Владеть навыками эксплуатации контрольно-измерительной техники	**Неудовлетворител** ставится в том случае, когда студент обнаруживает незнание большой части программного материала, отвечает, как правило, лишь на наводящие вопросы преподавателя неуверенно. В письменных работах допускает частые и грубые ошибки, а также ставится в том случае, когда студент обнаруживает полное незнание пройденного учебного материала. **Удовлетворительн** ставится в том случае, когда студент обнаруживает знание основного программного учебного материала. При применении знаний на практике испытывает некоторые затруднения и преодолевает их с небольшой помощью преподавателя. В устных ответах допускает ошибки при изложении материала и в построении речи. В письменных работах делает ошибки. **Хорошо** ставится в том случае, когда студент знает весь требуемый программой материал, хорошо понимает и прочно усвоил его. На вопросы (в пределах программы) отвечает без затруднений. Умеет применять полученные знания в практических заданиях. В письменных работах допускает только незначительные ошибки. **Отлично** ставится в том случае, когда студент исчерпывающе знает весь программный материал, отлично понимает и прочно усвоил его. На вопросы (в пределах программы) дает правильные, сознательные и уверенные ответы. В различных

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично практических заданиях умеет самостоятельно пользоваться полученными знаниями.
ПК.15 способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Знать физические принципы действия технических средств защиты информации и особенности их эксплуатации, Знать способы обнаружения и исследования каналов утечки информации Уметь проводить контрольные проверки работоспособности , технических средств защиты информации Владеть навыками борьбы с утечками информации, навыками проведения специальных исследжаваний	**Неудовлетворител** ставится в том случае, когда студент обнаруживает незнание большой части программного материала, отвечает, как правило, лишь на наводящие вопросы преподавателя неуверенно. В письменных работах допускает частые и грубые ошибки, а также ставится в том случае, когда студент обнаруживает полное незнание пройденного учебного материала. **Удовлетворительн** ставится в том случае, когда студент обнаруживает знание основного программного учебного материала. При применении знаний на практике испытывает некоторые затруднения и преодолевает их с небольшой помощью преподавателя. В устных ответах допускает ошибки при изложении материала и в построении речи. В письменных работах делает ошибки. **Хорошо** ставится в том случае, когда студент знает весь требуемый программой материал, хорошо понимает и прочно усвоил его. На вопросы (в пределах программы) отвечает без затруднений. Умеет применять полученные знания в практических заданиях. В письменных работах допускает только незначительные ошибки. **Отлично** ставится в том случае, когда студент исчерпывающе знает весь программный материал, отлично понимает и прочно усвоил его. На вопросы (в пределах программы) дает правильные, сознательные и уверенные ответы. В различных практических заданиях умеет самостоятельно пользоваться полученными знаниями.

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.17 способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных требований по защите информации	Знать нормативные требования по защите информации Уметь проведить экспериментально-исследовательских работ при аттестации автоматизированных систем Владеть навыками специальных технических исследований, проводимых для аттестации автоматизированных систем	**Неудовлетворител** ставится в том случае, когда студент обнаруживает незнание большой части программного материала, отвечает, как правило, лишь на наводящие вопросы преподавателя неуверенно. В письменных работах допускает частые и грубые ошибки, а также ставится в том случае, когда студент обнаруживает полное незнание пройденного учебного материала. **Удовлетворительн** ставится в том случае, когда студент обнаруживает знание основного программного учебного материала. При применении знаний на практике испытывает некоторые затруднения и преодолевает их с небольшой помощью преподавателя. В устных ответах допускает ошибки при изложении материала и в построении речи. В письменных работах делает ошибки. **Хорошо** ставится в том случае, когда студент знает весь требуемый программой материал, хорошо понимает и прочно усвоил его. На вопросы (в пределах программы) отвечает без затруднений. Умеет применять полученные знания в практических заданиях. В письменных работах допускает только незначительные ошибки. **Отлично** ставится в том случае, когда студент исчерпывающе знает весь программный материал, отлично понимает и прочно усвоил его. На вопросы (в пределах программы) дает правильные, сознательные и уверенные ответы. В различных практических заданиях умеет самостоятельно пользоваться полученными знаниями.
ПК.16 способность участвовать в проведении	Знать процедуру сертификации средств защиты автоматизированных систем Уметь измерять технические	**Неудовлетворител** ставится в том случае, когда студент обнаруживает незнание большой части программного материала, отвечает, как

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
экспериментально-исследовательских работ при сертификации средств защиты автоматизированных систем	характеристики средств защиты информации Владеть приёмами специальных технических исследований для проведения экспериментально-исследовательских работ при сертификации средств защиты автоматизированных систем	**Неудовлетворител** правило, лишь на наводящие вопросы преподавателя неуверенно. В письменных работах допускает частые и грубые ошибки, а также ставится в том случае, когда студент обнаруживает полное незнание пройденного учебного материала. **Удовлетворительн** ставится в том случае, когда студент обнаруживает знание основного программного учебного материала. При применении знаний на практике испытывает некоторые затруднения и преодолевает их с небольшой помощью преподавателя. В устных ответах допускает ошибки при изложении материала и в построении речи. В письменных работах делает ошибки. **Хорошо** ставится в том случае, когда студент знает весь требуемый программой материал, хорошо понимает и прочно усвоил его. На вопросы (в пределах программы) отвечает без затруднений. Умеет применять полученные знания в практических заданиях. В письменных работах допускает только незначительные ошибки. **Отлично** ставится в том случае, когда студент исчерпывающе знает весь программный материал, отлично понимает и прочно усвоил его. На вопросы (в пределах программы) дает правильные, сознательные и уверенные ответы. В различных практических заданиях умеет самостоятельно пользоваться полученными знаниями.
ОПК.6 способность применять приемы оказания первой помощи, методы защиты производственного персонала и населения	знать приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций	**Неудовлетворител** не знает приемов оказания первой помощи, методов защиты производственного персонала и населения в условиях чрезвычайных ситуаций **Удовлетворительн** частично сформированные знания приемы

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
в условиях чрезвычайных ситуаций		**Удовлетворительн** оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций **Хорошо** сформированные, но содержащие пробелы знания приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций **Отлично** сформированные знания приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций

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 52 до 60
«неудовлетворительно» / «незачтено» менее 52 балла

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
Входной контроль	Каналы утечки информационных систем. **Входное тестирование**	Проверка остаточных знаний по дисциплинам: электричество и магнетизм, радиоэлектроника, программно-аппаратные средства защиты информации, сети и системы передачи данных

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПК.6 способность применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций **ПК.15** способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации **ПК.17** способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных требований по защите информации	Закладные устройства и защита от них. **Защищаемое контрольное мероприятие**	Средства технического контроля для поиска источников излучения. Определение источника излучения, приводящего к утечке информации. Пеленгация закладных устройств. Активные помехи.
ПК.15 способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации **ПК.16** способность участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты автоматизированных систем	Специальные проверки. **Защищаемое контрольное мероприятие**	Исследования виброакустического канала утечки инфыормации. Разборчивость речи.

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.15 способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации **ПК.16** способность участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты автоматизированных систем **ПК.17** способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных требований по защите информации **ПК.18** способность проводить инструментальный мониторинг защищенности автоматизированных систем	Специальные исследования. **Итоговое контрольное мероприятие**	Характеристика каналов утечки информации.,Средства обнаружения каналов утечки информации,.Организация технической защиты информации.,Методы защиты информации.,Мероприятия по выявлению технических каналов утечки информации.

Спецификация мероприятий текущего контроля

Каналы утечки информационных систем.

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
При тестировании допущено менее 10% ошибок	81
При тестировании допущено менее 30% ошибок	61
При тестировании допущено менее 50% ошибок	41
При тестировании допущено более 50% ошибок	0

Закладные устройства и защита от них.

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **16**

Показатели оценивания	Баллы
Выполнение лабораторных работ	14
Ответы на вопросы по темам лабораторных работ	12
Отчеты по лабораторным работам	4

Специальные проверки.

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **16**

Показатели оценивания	Баллы
Выполнение лабораторных работ	14
Ответы по теме лабораторных работ	10
Отчеты по лабораторным работам	6

Специальные исследования.

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **20**

Показатели оценивания	Баллы
Ответы на 2 теоретический вопрос экзаменационного билета	12
Ответы на 1 теоретический вопрос экзаменационного билета	12
Ответы на дополнительный вопрос к вопросу 2 экзаменационного билета	8
Ответы на дополнительный вопрос к вопросу 1 экзаменационного билета	8