МИНОБРНАУКИ РОССИИ

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

Институт компьютерных наук и технологий

Авторы-составители: **Лобков Армандо Львович**
Черников Арсений Викторович

Рабочая программа дисциплины

ТЕХНИЧЕСКИЕ СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Код УМК 69463

Утверждено
Протокол №6
от «06» мая 2022 г.

Пермь, 2022

1. Наименование дисциплины

Технические средства и методы защиты информации

2. Место дисциплины в структуре образовательной программы

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

Специальность: **10.05.01** Компьютерная безопасность

специализация Разработка защищенного программного обеспечения

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Технические средства и методы защиты информации** у обучающегося должны быть сформированы следующие компетенции:

10.05.01 Компьютерная безопасность (специализация : Разработка защищенного программного обеспечения)

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.7.1 Ориентируется в методах и средствах защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методах и средствах защиты информации от утечки по техническим каналам, сетей и систем передачи информации

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

4. Объем и содержание дисциплины

Специальность	10.05.01 Компьютерная безопасность (специализация: Разработка защищенного программного обеспечения)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	10
Объем дисциплины (з.е.)	4
Объем дисциплины (ак.час.)	144
Контактная работа с преподавателем (ак.час.), в том числе:	56
Проведение лекционных занятий	28
Проведение практических занятий, семинаров	28
Самостоятельная работа (ак.час.)	88
Формы текущего контроля	Защищаемое контрольное мероприятие (1) Итоговое контрольное мероприятие (1) Письменное контрольное мероприятие (1)
Формы промежуточной аттестации	Экзамен (10 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Технические средства и методы защиты информации.Первый семестр

Раздел 1. Объекты защиты

Объекты защиты информации

- виды защищаемой информации, защита информации от утечки, непреднамеренного и несанкционированного воздействия;
- объекты защиты, информация ограниченного доступа, носитель информации, информационные процессы.

Демаскирующие признаки объектов защиты

- классификация демаскирующих признаков. Опознавательные признаки и признаки деятельности объектов;
- демаскирующие признаки объектов. Информативность признаков;
- особенности демаскирующих признаков в видимом, инфракрасном и радиолокационном диапазоне длин волн.

Источники и носители информации ограниченного доступа

- разновидности источников и носителей информации ограниченного доступа;
- способы записи на различные виды носителей и принципы съема информации.

Раздел 2. Технические каналы утечки информации

Общие сведения о каналах утечки информации

- общие сведения, классификация и структура каналов утечки информации.

Разновидности каналов утечки информации

- оптические каналы утечки информации ограниченного доступа, влияние на них среды распространения;
- акустические и виброакустические каналы утечки информации ограниченного доступа;
- вещественные каналы утечки информации ограниченного доступа.

Условия возникновения каналов утечки информации за счет побочных электромагнитных излучений и наводок

- построение каналов утечки конфиденциальной информации в радиоэлектронном диапазоне длин волн;
- технические средства информации применяемые в радиоэлектронном диапазоне длин волн.

Моделирование объектов защиты информации и каналов утечки информации

- моделирование утечки информации за счет акустических и виброакустических каналов утечки информации;
- моделирование утечки информации за счет радиоэлектронного канала утечки информации.

Раздел 3. Способы добывания информации

Роль разведывательной деятельности государтсвенных и коммерческих структур, структура органов разведки и ее виды

- виды угроз безопасности информации, принципы добывания и обработки информации;
- органы добывания информации, структура органов разведки и ее виды.

Способы доступа к источникам информации ограниченного доступа, обнаружение и

распознавания объектов защиты
- способы доступа к источникам информации ограниченного доступа;
- добывание и обработка информации, наблюдение, перехват, подслушивание.

Раздел 4. Концепция и методы инженерно-технической защиты информации

Скрытие объектов наблюдения, скрытие речевой информации в каналах связи
- способы и средства противодействия наблюдению в оптическом диапазоне длин волн;
- способы и средства противодействия наблюдению в радиолокационном диапазоне длин волн;
- акустическая защита выделенного (защищаемого) помещения;
- пассивные и активные способы (средства) защиты акустической (речевой) информации.

Обнаружение и локализация устройств негласного съема информации, подавление их сигналов
- противодействия техническим средствам негласного съема информации в акустическом диапазоне длин волн.

Подавление опасных сигналов акустических преобразователей
- технические средства защиты информации, применяемые для закрытия акустоэлектрических каналов утечки информации.

Подавление информационных ситналов в цепях заземления и электропитания
- пассивные способы противодействия утечки информации за счет ПЭМИН;
- способы подавления опасных побочных электромагнитных импульсов и наводок в цепях заземления и электропитания с использованием искусственных преднамеренных помех.

Раздел 5. Нормативные документы по противодействию технической разведке

Виды контроля эффективности защиты информации
- методы контроля эффективности защиты информации на объектах информатизации;
- предварительный, периодический и постоянный контроль защиты информации на объектах информатизации.

Основные положения методологии инженерно-технической защиты информации
- общие положения об инженерно-технической защите информации в организации;
- организационные и технические меры инженерно-технической защиты информации.

Методы расчета и инструментального контроля показателей защищенности информации
- расчет защищенности защищаемого помещения по акустическому каналу утечки информации;
- расчет защищенности автоматизированного рабочего места по радиоэлектронному каналу 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. Торокин А. А. Инженерно-техническая защита информации:учебное пособие для студентов вузов, обучающихся по специальностям в области информационной безопасности/А. А. Торокин.-Москва:Гелиос АРВ,2005, ISBN 5-85438-140-0.-960.-Библиогр.: с. 934-949

Дополнительная:

1. Технические средства и методы защиты информации:учебное пособие для студентов вузов, обучающихся по специальностям 090102 "Компьютерная безопасность",090105 "Комплексное обеспечение информационной безопасности автоматизированных систем", 090106 "Информационная безопасность телекоммуникационных систем"/А. П. Зайцев [и др.] ; ред.: А. П. Зайцев, А. А. Шелупанов.-4-е изд., испр. и доп..-Москва:Горячая линия - Телеком,2012, ISBN 978-5-9912-0084-4.-616.-Библиогр.: с. 608-609

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

http://www.psu.ru/elektronnye-resursy-dlya-psu Электронные ресурсы для ПГНИУ
http://www.mathnet.ru/ Общероссийский математический портал
http://window.edu.ru/ Единое окно доступа к образовательным ресурсам

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

Образовательный процесс по дисциплине **Технические средства и методы защиты информации** предполагает использование следующего программного обеспечения и информационных справочных систем:
Образовательный процесс по дисциплине "Технические средства и методы защиты информации" предполагает
использование следующего программного обеспечения и информационных систем:
- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательную среду университета.
Необходимое лицензионное и (или) свободно распространяемое программное обеспечение:
- приложение позволяющее просматривать и воспроизводить медиаконтент PDF-файлов "Adobe Acrobat Reader DC";
- офисный пакет приложений "LibreOffice";
- MS Word; MS Excel; Multisim; MathCAD.
При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ (student.psu.ru).

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

Для лекционных занятий требуется аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.
Для проведения практических занятий - аудитория, аудитория оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.
Для групповых (индивидуальных) консультаций - аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.
Для проведения текущего контроля - аудитория, оснащенная меловой (и) или маркерной доской.
Самостоятельная работа студентов: аудитория, оснащенная компьютерной техникой с возможностью

подключения к сети "Интерне, с обеспеченным доступом в электронную информационно-образовательную среду университета, помещения Научной библиотеки ПГНИУ,"

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
Технические средства и методы защиты информации

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

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.7.1 Ориентируется в методах и средствах защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методах и средствах защиты информации от утечки по техническим каналам, сетей и систем передачи информации	Знает методы и средства защиты информации в операционных системах, компьютерных сетях и системах управления базами данных. Умеет ориентироваться в методах и средствах защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методах и средствах защиты информации от утечки по техническим каналам, сетей и систем передачи информации.	**Неудовлетворител** Не знает методы и средства защиты информации в операционных системах, компьютерных сетях и системах управления базами данных. Не умеет ориентироваться в методах и средствах защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методах и средствах защиты информации от утечки по техническим каналам, сетей и систем передачи информации. **Удовлетворительн** Знает часть методов и средств защиты информации в операционных системах, компьютерных сетях и системах управления базами данных. Не умеет ориентироваться в методах и средствах защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методах и средствах защиты информации от утечки по техническим каналам, сетей и систем передачи информации. **Хорошо** Знает методы и средства защиты информации в операционных системах, компьютерных сетях и системах управления базами данных. Умеет частично ориентироваться в методах и средствах защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методах

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо и средствах защиты информации от утечки по техническим каналам, сетей и систем передачи информации. **Отлично** Знает методы и средства защиты информации в операционных системах, компьютерных сетях и системах управления базами данных. Умеет ориентироваться в методах и средствах защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методах и средствах защиты информации от утечки по техническим каналам, сетей и систем передачи информации.
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	Знает методы и средства защиты информации в операционных системах, компьютерных сетях и системах управления базами данных. Умеет применять 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.	**Неудовлетворител** Не знает методы и средства защиты информации в операционных системах, компьютерных сетях и системах управления базами данных. Не умеет применять 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. **Удовлетворительн** Знает часть методов и средств защиты информации в операционных системах, компьютерных сетях и системах управления базами данных. Не умеет применять 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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительн средств обеспечения защиты информации. **Хорошо** Знает методы и средства защиты информации в операционных системах, компьютерных сетях и системах управления базами данных. Частично умеет применять 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. **Отлично** Знает методы и средства защиты информации в операционных системах, компьютерных сетях и системах управления базами данных. Умеет применять 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.

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 43 до 60
«неудовлетворительно» / «незачтено» менее 43 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
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.7.1** Ориентируется в методах и средствах защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методах и средствах защиты информации от утечки по техническим каналам, сетей и систем передачи информации	Источники и носители информации ограниченного доступа **Письменное контрольное мероприятие**	Письменная контрольная работа

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
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.7.1** Ориентируется в методах и средствах защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методах и средствах защиты информации от утечки по техническим каналам, сетей и систем передачи информации	Способы доступа к источникам информации ограниченного доступа, обнаружение и распознавания объектов защиты **Защищаемое контрольное мероприятие**	Письменная контрольная работа

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
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.7.1** Ориентируется в методах и средствах защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методах и средствах защиты информации от утечки по техническим каналам, сетей и систем передачи информации	Методы расчета и инструментального контроля показателей защищенности информации **Итоговое контрольное мероприятие**	Письменная контрольная работа

Спецификация мероприятий текущего контроля

Источники и носители информации ограниченного доступа

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **13**

Показатели оценивания	Баллы
Письменная контрольная работа	30

Способы доступа к источникам информации ограниченного доступа, обнаружение и распознавания объектов защиты

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **12**

Показатели оценивания	Баллы

Проведение контрольной работы	30

Методы расчета и инструментального контроля показателей защищенности информации

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **18**

Показатели оценивания	Баллы
Проведение контрольной работы	40