МИНОБРНАУКИ РОССИИ

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

Институт компьютерных наук и технологий

Авторы-составители: **Мустакимова Яна Романовна**
Лобков Армандо Львович

Рабочая программа дисциплины

РАЗРАБОТКА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Код УМК 94460

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

Пермь, 2022

1. Наименование дисциплины

Разработка средств 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 **Разработка средств защиты информации** у обучающегося должны быть сформированы следующие компетенции:

10.05.01 Компьютерная безопасность (специализация : Разработка защищенного программного обеспечения)

ПК.2 Способен принимать участие в проектировании программных (программно-технических) средств защиты информации

Индикаторы

ПК.2.1 Ориентируется в методах проектирования программных (программно-технических) средств защиты информации

ПК.2.2 Применяет на практике методы проектирования программных (программно-технических) средств защиты информации

ОПСК.1 Способен проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей

Индикаторы

ОПСК.1.1 Ориентируется в требованиях нормативных документов по разработке программного кода

4. Объем и содержание дисциплины

Специальность	10.05.01 Компьютерная безопасность (специализация: Разработка защищенного программного обеспечения)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	16
Объем дисциплины (з.е.)	3
Объем дисциплины (ак.час.)	108
Контактная работа с преподавателем (ак.час.), в том числе:	42
Проведение лекционных занятий	28
Проведение лабораторных работ, занятий по иностранному языку	14
Самостоятельная работа (ак.час.)	66
Формы текущего контроля	Защищаемое контрольное мероприятие (3)
Формы промежуточной аттестации	Зачет (16 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Разработка средств защиты информации.Первый семестр

Раздел 1. Законодательная база РФ в области осущсетвления деятельности по разработке средств защиты информации

Законы РФ в области разработки средств защиты информации
- структура законодательства в области разработки и применения средств защиты информации;
- ФЗ "О лицензировании отдельных видов деятельности".

Положение о лицензировании деятельности по разработке срелдств защиты информации
- постановление Правительства РФ "О лицензировании деятельности по технической защите конфиденциальной информации";
- постановление Правительства РФ "О лицензировании деятельности по разработке и (или) производству средств защиты информации".

Раздел 2. Электромагнитные волны и их распространение

Принципы распространения радиоволн
- распространение радиоволн вдоль поверхности Земли;
- состав и строение земной атмосферы, тропосферы и их особенности.

Принципы распространения радиоволн СДВ и СК диапазонов
- сверхдлинные, длинные поверхностные и ионосферные волны, особенности их распространения;
- средние волны, дневное и ночное их распространение.

Принципы распространения радиоволн КВ и УКВ диапазонов
- короткие волны, роль различных слоев ионосферы в формировании ионосферных волн;
- зоны молчан7ия и замирания, возникающие при распространении КВ радиоволн;
- особенности распространения радиоволн УКВ диапазона, влияние тропосферы, ионосферы и не гладкости поверхности Земли.

Раздел 3. Принципы построения антенных устройств как средств защиты информации

Использование антенных устройств для обнаружения каналов утечки информации
- основные параметры и характеристики антенных устройств и их взаимность;
- элементарный электрический излучатель, симметричный и несимметричный вибраторы и их особенности.

Классификация антенных устройств и принципы их построения
- разновидности антенных устройств ДВ, СВ диапазонов длин волн;
- антенные системы КВ диапазонов длин волн;
- антенные устройства УКВ диапазонов длин волн.

Раздел 4. Построение средств защиты объектов информатизации для закрытия каналов утечки информации

Принципы построения генераторов как устройств создания преднамеренных помех радиоэлектронному каналу утечки информации
- трехточечные схемы автогенераторов;
- стабилизация частоты в автогенераторе.

Принципы построения широкополосных генераторов

- функциональные и принципиальные схемы широкополосных генераторов.

Основы передачи информации по радиоканалам

- принципы построения радиопередающих устройств как средств защиты информации;
- структурные и функциональные схемы радиопередающих устройств.

Принципы работы функциональных каскадов радиопередающих устройств

- генерирование радиочастотных колебаний в передающих устройствах;
- резонансные усилители и делители частоты;
- усилители мощности и модуляторы.

Основы приема информации по радиоканалам

- структурные и функциональные схемы радиоприемных устройств;
- принципы построения супергетеродинных приемных устройств.

Принципы работы функциональных каскадов радиоприемных устройств как техническихъ средств защиты информации

- входные цепи, избирательность и помехоустойчивость приема;
- резонансные усилители радиочастоты и преобразователи частоты;
- усилители промежуточной частоты;
- разновидности и принцип действия детекторных устройств;
- усилители низкой частоты.

Принципы построения приемных устройств в оптическом диапазоне длин волн как технических средств защиты информации

- разновидности приемных устройств, работающих в оптическом диапазоне длин волн;
- принципы работы функциональных и принципиальных каскадов приемных устройств в оптическом диапазоне длин волн.

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. Соболев А. Н.,Кириллов В. М. Физические основы технических средств обеспечения информационной безопасности:учебное пособие для студентов вузов/А. Н. Соболев, В. М. Кириллов.-Москва:Гелиос АРВ,2004, ISBN 5-85438-084-6.-224.-Библиогр.: с. 215-218

Дополнительная:

1. Технические средства обеспечения информационной безопасности.учебное пособие/Министерство образования и науки Российской Федерации; сост. А. П. Зайцев.-Томск:Томский межвузовский центр дистанционного образования,2004.Ч. 1.Технические каналы утечки информации/Томский университет автоматизированных систем управления и радиоэлектроники (ТУСУР), Кафедра КИБЭВС.-2004.-199

2. Технические средства обеспечения информационной безопасности.учебное пособие/Министерство образования и науки Российской Федерации; сост. А. П. Зайцев.-Томск:Томский межвузовский центр дистанционного образования,2004.Ч. 2.Средства защиты информации от утечки по техническим каналам/Томский государственный университет систем управления и радиоэлектроники (ТУСУР), Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС).-2004.-279

3. 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

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 **Разработка средств защиты информации** предполагает использование следующего программного обеспечения и информационных справочных систем:
Образовательный процесс по дисциплине "Разработка средств защиты информации" предполагает использование следующего программного обеспечения и информационных справочных 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 лабораторных работ требуется аудитория Лаборатории Информационной безопасности: аппаратные и программные средства определены паспортом лаборатории.
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
Разработка средств защиты информации

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

ОПСК.1

Способен проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПСК.1.1 Ориентируется в требованиях нормативных документов по разработке программного кода	Знать основные требования нормативных документов по разработке защищенного программного кода. Уметь применять требования нормативных документов по разработке защищенного программного кода при решении профессиональных задач. Владеть навыками поиска необходимой информации в нормативных документах по разработке защищенного программного кода.	**Неудовлетворител** Не знает основные требования нормативных документов по разработке защищенного программного кода. Не умеет обосновывать выбор требований нормативных документов по разработке защищенного программного кода при решении профессиональных задач. Не владеет навыками поиска необходимой информации в нормативных документах по разработке защищенного программного кода. **Удовлетворительн** Знает не все основные требования нормативных документов по разработке защищенного программного кода. Плохо умеет обосновывать выбор требований нормативных документов по разработке защищенного программного кода при решении профессиональных задач. Не владеет навыками поиска необходимой информации в нормативных документах по разработке защищенного программного кода. **Хорошо** Знает все основные требования нормативных документов по разработке защищенного программного кода. Хорошо умеет обосновывать выбор требований нормативных документов по разработке защищенного программного кода при решении профессиональных задач. Не в полной мере владеет навыками поиска необходимой информации в нормативных документах по разработке защищенного программного кода.

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично Знает все основные требования нормативных документов по разработке защищенного программного кода. Хорошо умеет обосновывать выбор требований нормативных документов по разработке защищенного программного кода при решении профессиональных задач. В полной мере владеет навыками поиска необходимой информации в нормативных документах по разработке защищенного программного кода.

ПК.2

Способен принимать участие в проектировании программных (программно-технических) средств защиты информации

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.2.1 Ориентируется в методах проектирования программных (программно-технических) средств защиты информации	Знать методы проектирования программных (программно-технических) средств защиты информации. Уметь находить информацию о методах проектирования программных (программно-технических) средств защиты информации. Владеть навыками поиска, анализа и обобщения информации о методах проектирования программных (программно-технических) средств защиты информации.	**Неудовлетворител** Не знает методы проектирования программных (программно-технических) средств защиты информации. Не умеет находить информацию о методах проектирования программных (программно-технических) средств защиты информации. Не владеет навыками поиска, анализа и обобщения информации о методах проектирования программных (программно-технических) средств защиты информации. **Удовлетворительн** Знает основные методы проектирования программных (программно-технических) средств защиты информации. Частично умеет находить информацию о методах проектирования программных (программно-технических) средств защиты информации. Не владеет навыками поиска, анализа и обобщения информации о методах проектирования программных (программно-технических) средств защиты информации. **Хорошо** Знает все методы проектирования программных (программно-технических) средств защиты информации.

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо Умеет в полной мере находить информацию о методах проектирования программных (программно-технических) средств защиты информации. Не владеет в полной мере навыками поиска, анализа и обобщения информации о методах проектирования программных (программно-технических) средств защиты информации. **Отлично** Знает все методы проектирования программных (программно-технических) средств защиты информации. Умеет в полной мере находить информацию о методах проектирования программных (программно-технических) средств защиты информации. Владеет в полной мере навыками поиска, анализа и обобщения информации о методах проектирования программных (программно-технических) средств защиты информации.
ПК.2.2 Применяет на практике методы проектирования программных (программно-технических) средств защиты информации	Знать методы проектирования программных (программно-технических) средств защиты информации. Уметь применять на практике методы проектирования программных (программно-технических) средств защиты информации. Владеть навыками применения методов проектирования программных (программно-технических) средств защиты информации в соответствии с профессиональными задачами.	**Неудовлетворител** Не знает методы проектирования программных (программно-технических) средств защиты информации. Не умеет применять на практике методы проектирования программных (программно-технических) средств защиты информации. Не владеет навыками применения методов проектирования программных (программно-технических) средств защиты информации в соответствии с профессиональными задачами. **Удовлетворительн** Знает методы проектирования программных (программно-технических) средств защиты информации. Умеет с ошибками применять на практике методы проектирования программных (программно-технических) средств защиты информации. Не владеет навыками применения методов проектирования программных (программно-технических) средств защиты информации в соответствии с профессиональными

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительн задачами. **Хорошо** Знает методы проектирования программных (программно-технических) средств защиты информации. Умеет без ошибок применять на практике методы проектирования программных (программно-технических) средств защиты информации. Не владеет в полной мере навыками применения методов проектирования программных (программно-технических) средств защиты информации в соответствии с профессиональными задачами. **Отлично** Знает методы проектирования программных (программно-технических) средств защиты информации. Умеет без ошибок применять на практике методы проектирования программных (программно-технических) средств защиты информации. Владеет в полной мере навыками применения методов проектирования программных (программно-технических) средств защиты информации в соответствии с профессиональными задачами.

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Базовая

Вид мероприятия промежуточной аттестации : Зачет
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 42 до 60
«неудовлетворительно» / «незачтено» менее 42 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПСК.1.1 Ориентируется в требованиях нормативных документов по разработке программного кода **ПК.2.2** Применяет на практике методы проектирования программных (программно-технических) средств защиты информации **ПК.2.1** Ориентируется в методах проектирования программных (программно-технических) средств защиты информации	Принципы распространения радиоволн КВ и УКВ диапазонов **Защищаемое контрольное мероприятие**	Знание принципов распространения радиоволн различных диапазонов
ОПСК.1.1 Ориентируется в требованиях нормативных документов по разработке программного кода **ПК.2.2** Применяет на практике методы проектирования программных (программно-технических) средств защиты информации **ПК.2.1** Ориентируется в методах проектирования программных (программно-технических) средств защиты информации	Принципы построения широкополосных генераторов **Защищаемое контрольное мероприятие**	Умение проводить расчеты по построению электрических схем средств защиты информации

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПСК.1.1 Ориентируется в требованиях нормативных документов по разработке программного кода **ПК.2.2** Применяет на практике методы проектирования программных (программно-технических) средств защиты информации **ПК.2.1** Ориентируется в методах проектирования программных (программно-технических) средств защиты информации	Принципы построения приемных устройств в оптическом диапазоне длин волн как технических средств защиты информации **Защищаемое контрольное мероприятие**	Знать математический аппарат расчета электрических схем устройств защиты информации

Спецификация мероприятий текущего контроля

Принципы распространения радиоволн КВ и УКВ диапазонов

Продолжительность проведения мероприятия промежуточной аттестации: **.5 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **12.6**

Показатели оценивания	Баллы
Умение проводить расчеты по распространению радиоволн	30

Принципы построения широкополосных генераторов

Продолжительность проведения мероприятия промежуточной аттестации: **.5 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **12.6**

Показатели оценивания	Баллы
Знание принципов построения электрических схем устройств защиты информации	30

Принципы построения приемных устройств в оптическом диапазоне длин волн как технических средств защиты 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: **16.8**

Показатели оценивания	Баллы
Умение проводить расчеты параметров электрических схем устройств защиты информации	40