МИНОБРНАУКИ РОССИИ

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

Институт компьютерных наук и технологий

Авторы-составители: **Черников Арсений Викторович**
Политов Александр Владимирович

Рабочая программа дисциплины

ЗАЩИТА СИСТЕМ СВЯЗИ

Код УМК 93288

Утверждено
Протокол №1
от «28» июня 2024 г.

Пермь, 2024

1. Наименование дисциплины

Защита систем связи

2. Место дисциплины в структуре образовательной программы

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

Специальность: **10.05.04** Информационно-аналитические системы безопасности
направленность Информационная безопасность финансовых и экономических структур

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Защита систем связи** у обучающегося должны быть сформированы следующие компетенции:

10.05.04 Информационно-аналитические системы безопасности (направленность : Информационная безопасность финансовых и экономических структур)

ОПК.11 Способен осуществлять синтез технологий и основных компонентов функциональной и обеспечивающей частей создаваемых информационно-аналитических систем, в том числе выбор мероприятий по защите информации

Индикаторы

ОПК.11.1 Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем

ОПК.11.2 Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации

4. Объем и содержание дисциплины

Специальность	10.05.04 Информационно-аналитические системы безопасности (направленность: Информационная безопасность финансовых и экономических структур)
форма обучения	очная
№№ семестров, выделенных для изучения дисциплины	9
Объем дисциплины (з.е.)	4
Объем дисциплины (ак.час.)	144
Контактная работа с преподавателем (ак.час.), в том числе:	108
Проведение лекционных занятий	18
Проведение практических занятий, семинаров	36
Проведение лабораторных работ, занятий по иностранному языку	54
Самостоятельная работа (ак.час.)	36
Формы текущего контроля	Защищаемое контрольное мероприятие (4)
Формы промежуточной аттестации	Экзамен (9 семестр)

5. Аннотированное описание содержания разделов и тем дисциплины

1 семестр

Понятие модели безопасности. Концептуальная модель информационной безопасности в системах связи.
В разделе курса рассматриваются вопросы посвященные общим вопросам защиты данных, понятия модели безопасности. Рассматриваются основные подходы к построению систем защиты в системах связи. Основные программные и аппаратные элементы.

Программные средства защиты информации в системах связи.
В разделе курса рассматриваются вопросы посвященные вопросам защиты данных в системах связи с помощью программных средств. Программные бранмауэры, программные антивирусы, программный VPN.

Аппаратные средства защиты информации в системах связи.
В разделе курса рассматриваются вопросы посвященные вопросам защиты данных в системах связи с помощью аппаратных средств. АКПШ Континет, аппаратно-программные VPN, сетевые брандмауэры.

Тестирование на проникновение и защита.
В разделе курса рассматриваются вопросы посвященные вопросам защиты данных в системах связи с помощью аппаратных средств. В разделе рассматривается документация, программное и аппаратное обеспечения для тестирования систем защиты.

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. Галицкий А. В.,Рябко С. Д.,Шаньгин В. Ф. Защита информации в сети - анализ технологий и синтез решений/А. В. Галицкий, С. Д. Рябко, В. Ф. Шаньгин.-М.:ДМК Пресс,2004, ISBN 5-94074-244-0.-616.-Библиогр.: с. 599-608

2. Винокуров, В. М. Сети связи и системы коммутации : учебное пособие / В. М. Винокуров. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2012. — 304 c. — ISBN 5-86889-215-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/13972

3. Голиков, А. М. Сети и системы радиосвязи и средства их информационной защиты : учебное пособие / А. М. Голиков. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2007. — 392 c. — ISBN 978-5-86889-393-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/13971

Дополнительная:

1. Тестирование радиооборудования систем связи : учебное пособие / составители С. И. Дингес. — Москва : Московский технический университет связи и информатики, 2016. — 48 c. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. http://www.iprbookshop.ru/61768.html

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

https://intuit.ru/studies/courses/13845/1242/info Безопасность информационных систем
https://intuit.ru/studies/courses/57/57/info Основы локальных сетей

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

Образовательный процесс по дисциплине **Защита систем связи** предполагает использование следующего программного обеспечения и информационных справочных систем:
Образовательный процесс по дисциплине предполагает использование следующих 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:
- операционная система "ALT Linux"
- офисный пакет приложений "Libre office";
- программа просмотра интернет контента (браузер)
Специализированное программное обеспечение Лаборатории радиотехнических средств защиты информации.

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

Аудитория для лекционных занятий - Специализированный учебный кабинет «Лекционный кабинет» (защищённое помещение по конфиденциальной информации), оборудованный: специализированная мебель, телевизор, маркерная доска.

Аудитория для семинарских (практических) занятий, групповых (индивидуальных) консультаций, текущего контроля и промежуточной аттестации оборудованная: специализированная мебель, компьютер/ноутбук, проектор, экран/телевизор, меловая или маркерная доска.

Аудитория для лабораторных занятий - Лаборатория радиотехнических средств защиты информации, оборудованная: специализированная мебель, лабораторное оборудование, проектор, экран, персональные компьютеры, маркерная доска, специализированное оборудование и программное обеспечение.

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
Защита систем связи

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

ОПК.11

Способен осуществлять синтез технологий и основных компонентов функциональной и обеспечивающей частей создаваемых информационно-аналитических систем, в том числе выбор мероприятий по защите информации

Индикатор	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.11.1 Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем	Студенты демонстрируют знание принципов защиты информации, способность анализировать угрозы и уязвимости, разрабатывать и внедрять политики безопасности, оценивать эффективность мер безопасности, применять стандарты и регуляторные требования, а также использовать методики контроля, представлять результаты анализа и работать в команде, что приведет к формированию навыков эффективного контроля и оценки политики безопасности информации в автоматизированных системах.	**Неудовлетворител** не знает основные понятия и принципы защиты информации; проводит поверхностный анализ угроз; многие уязвимости не учитывает; демонстрирует ограниченные способности к разработке политик безопасности; проводит поверхностную оценку эффективности мер безопасности; показывает ограниченные знания стандартов безопасности; демонстрирует ограниченное применение методик контроля **Удовлетворительн** демонстрирует основное понимание принципов защиты безопасности; проводит поверхностный анализ угроз и уязвимостей безопасности; разработанные политики безопасности частично отвечают требованиям; требует доработки; проводится базовая оценка эффективности мер безопасности, но не все меры учитываются; показывает не полные знания стандартов безопасности; демонстрирует ограниченное применение методик контроля. **Хорошо** показывает точное понимание понятий безопасности; может объяснять и применять их в различных контекстах; проводит хороший анализ угроз безопасности с незначительными упущениями; определяет основные уязвимости; разрабатывает политики безопасности, но с небольшими недостатками или ограничениями; проводит хорошую оценку эффективности мер безопасности с небольшими недочетами;

Индикатор	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо соблюдает стандарты и требования безопасности. **Отлично** показывает полное и точное понимание понятий и принципов защиты информации; может объяснять и применять их в различных контекстах; проводит глубокий и всесторонний анализ угроз; умело определяет уязвимости систем; предлагает эффективные и практичные политики; правильно применяет теорию на практике; проводит глубокую оценку эффективности мер безопасности; соблюдает стандарты и требования; способен интегрировать их в практику.
ОПК.11.2 Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации	Студенты анализируют программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем для выявления потенциальных уязвимостей, разрабатывают рекомендации по повышению безопасности систем связи и проводят тестирование на проникновение с целью улучшения защищенности информации	**Неудовлетворител** Демонстрирует ограниченное понимание архитектурных и программных решений, нечеткие рекомендации, ограниченное применение инструментов, примитивные и неэффективные рекомендации **Удовлетворительн** Выявляет уязвимости, но недостаточно детализирует и обосновывает решения, ориентируется в основных инструментах, дает обоснованные рекомендации, но недостаточно практичные. **Хорошо** Проводит полный анализ с четким выявлением уязвимостей и разумными рекомендациями, эффективно использует инструменты с убедительными результатами. **Отлично** Проводит глубокий анализ с комплексной оценкой уязвимостей и детально обоснованными решениями. Применяет инструменты с глубоким анализом полученных данных. Предлагает эффективные рекомендации, способствующие значительному повышению безопасности

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : для ИАСБ

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 41 до 60
«неудовлетворительно» / «незачтено» менее 41 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПК.11.2 Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации **ОПК.11.1** Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем	Понятие модели безопасности. Концептуальная модель информационной безопасности в системах связи. **Защищаемое контрольное мероприятие**	Теоретические знания по основам моделей безопасности в системах связи. Умение применять полученные теоретические знания на практике, в построении конкретных систем. Владение навыками разработки актуальной модели безопасности в системах связи.
ОПК.11.2 Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации	Программные средства защиты информации в системах связи. **Защищаемое контрольное мероприятие**	Теоретические знания по основным программным средствам безопасности в системах связи. Умение применять полученные теоретические знания на практике, в построении конкретных систем. Владение навыками организации и настройки защищенной программной системы в системах связи.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПК.11.2 Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации **ОПК.11.1** Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем	Аппаратные средства защиты информации в системах связи. **Защищаемое контрольное мероприятие**	Теоретические знания по основным аппаратным средствам безопасности в системах связи. Умение применять полученные теоретические знания на практике, в построении конкретных систем. Владение навыками организации и настройки защищенной аппаратной системы в системах связи.
ОПК.11.2 Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации **ОПК.11.1** Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем	Тестирование на проникновение и защита. **Защищаемое контрольное мероприятие**	Теоретические знания по основным программным и аппаратными средствам тестирования безопасности в системах связи. Умение применять полученные теоретические знания на практике, в построении конкретных систем. Владение навыками организации и настройки защищенной программной системы в системах связи.

Спецификация мероприятий текущего контроля

Понятие модели безопасности. Концептуальная модель информационной безопасности в системах связи.

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **25**
Проходной балл: **10.3**

Показатели оценивания	Баллы
Отчет в электронной форме.	25

Программные средства защиты информации в системах связи.

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **25**
Проходной балл: **10.3**

Показатели оценивания	Баллы
Отчет в электронной форме.	25

Аппаратные средства защиты информации в системах связи.

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **25**
Проходной балл: **10.3**

Показатели оценивания	Баллы
Установка и настройка системы защиты информации с использованием аппаратных средств	13
Описание процедуры настройки реализованной студентом системы защиты информации согласно ГОСТ	12

Тестирование на проникновение и защита.

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **25**
Проходной балл: **10.3**

Показатели оценивания	Баллы
Отчет в электронной форме.	25