МИНОБРНАУКИ РОССИИ

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

Кафедра радиоэлектроники и защиты информации

Авторы-составители: **Лунегов Игорь Владимирович**
Балтаев Родион Хамзаевич

Рабочая программа дисциплины

ДОПОЛНИТЕЛЬНЫЕ ГЛАВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Код УМК 97497

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

Пермь, 2021

1. Наименование дисциплины

Дополнительные главы информационной безопасности

2. Место дисциплины в структуре образовательной программы

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

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

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Дополнительные главы информационной безопасности** у обучающегося должны быть сформированы следующие компетенции:

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

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

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

Индикаторы

ПК.6.2 Подготавливает отчетные материалы по результатам специальных исследований

4. Объем и содержание дисциплины

Специальность	10.05.03 Информационная безопасность автоматизированных систем (направленность: Безопасность открытых информационных систем)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	16
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	Входное тестирование (1) Защищаемое контрольное мероприятие (2) Итоговое контрольное мероприятие (1)
Формы промежуточной аттестации	Экзамен (16 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Дополнительные главы информационной безопасности

Объекты информационной системы. Поиск каналов утечки информации. Поиск радио закладок с помощью носимых многофункциональных поисковых приборов. Общая методология поиска радио закладок. Защита речевой информации. Организация проверки объектов информационной системы на наличие "жучков". Общие технические требования к средствам вычислительной техники для защиты от несанкционированного доступа к информации. Обеспечение информационной безопасности в организации. Испытание технических средств обработки информации на соответствие требованиям защищенности. Концепции и модели менеджмента безопасности информационных и телекоммуникационных технологий. Угрозы и каналы утечки информации. Оценка уязвимости и рисков. Требования к средствам защиты информации. Выбор средств защиты информации. Внедрение и использование мер и средств защиты информации. Математические основы шифрования. Симметричные / ассиметричные шифры. Элементарные функции шифрования. Сеть Фей стеля. Блочные шифры. поточные шифры. ЭЦП. Хеш-функции. Другие криптографические примитивы. Вопросы коллизии. Построение систем, использующих криптографические примитивы. Криптографические стандарты. DES/ AES. Стандарт RC4. Стандарты ЭЦП. Стандарты хеш-функций. Основные модели управления доступом. Разработка модели управления доступом. Защита процедур управления доступом. Цели и задачи разработки системы защиты информации. Стадии и этапы разработки системы защиты информации. Изучение исходных данных по информационной системе. Оценка рисков, связанных с осуществлением угроз безопасности в отношении ресурсов информационной системы. Анализ механизмов безопасности.

Технические средства защиты информации

Объекты информационной системы. Поиск каналов утечки информации. Поиск радио закладок с помощью носимых многофункциональных поисковых приборов. Общая методология поиска радио закладок. Защита речевой информации. Организация проверки объектов информационной системы на наличие "жучков".

Стандарты и спецификации в области информационной безопасности

Общие технические требования к средствам вычислительной техники для защиты от несанкционированного доступа к информации. Обеспечение информационной безопасности в организации. Испытание технических средств обработки информации на соответствие требованиям защищенности. Концепции и модели менеджмента безопасности информационных и телекоммуникационных технологий.

Управление системой защиты

Угрозы и каналы утечки информации. Оценка уязвимости и рисков. Требования к средствам защиты ифнормации. Выбор средств защиты информации. Внедрение и использование мер и средств защиты информации.

Криптографические методы защиты информации

Математические основы шифрования. Симметричные / ассиметричные шифры. Элементарные функции шифрования. Сеть Фейстеля. Блочные шифры. поточные шифры. ЭЦП. Хеш-функции. Другие криптографические примитивы. Вопросы коллизии. Построение систем, использующих криптографические примитивы. Криптографические стандарты. DES/ AES. Стандарт RC4. Стандарты ЭЦП. Стандарты хеш-функций.

Идентификация и аутентификация, управление доступом

Основные модели управления доступом. Разработка модели управления доступом. Защита процедур управления доступом.

Организация разработки системы защиты информации

Цели и задачи разработки системы защиты информации. Стадии и этапы разработки системы защиты информации.

Анализ уровня защищенности корпоративной информационной системы

Изучение исходных данных по информационной системе. Оценка рисков, связанных с осуществлением угроз безопасности в отношении русурсов информационной системы. Анализ механизмов безопасности

Итоговое контрольное мероприятие

Вопросы к итоговому мероприятию (экзамену).

1. Понятие технического канала утечки информации
2. Виды технических каналов утечки информации
3. Понятие технического средства приема, обработки, хранения и передачи информации (ТСПИ)
4. Понятие и примеры основных технических средств и систем (ОТСС)
5. Понятие и примеры вспомогательных технических средств и систем (ВТСС)
6. Понятие опасной зоны R1
7. Понятие опасной зоны R2
8. Понятие контролируемой зоны
9. Понятие специального исследования
10. Понятие специальной проверки
11. Принцип работы нелинейного локатора
12. Понятие высокочастотного навязывания
13. Понятие симметричных алгоритмов шифрования и их недостатки
14. Понятие асимметричных алгоритмов шифрования и их недостатки
15. Понятие электронной цифровой подписи.
16. Виды электронной подписи и их отличие.
17. Понятие хэш-функции
18. Параметры (длина ключа, длина блока шифрования, количество раундов) алгоритмов шифрования «Кузнечик» и «Магма»
19. Параметры (длина ключа, длина блока шифрования, количество раундов) алгоритма шифрования AES
20. Режимы работы алгоритмов блочного шифрования

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. Федин, Ф. О. Информационная безопасность : учебное пособие / Ф. О. Федин, В. П. Офицеров, Ф. Ф. Федин. — Москва : Московский городской педагогический университет, 2011. — 260 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/26486

2. Петров, С. В. Информационная безопасность : учебное пособие / С. В. Петров, П. А. Кисляков. — Саратов : Ай Пи Ар Букс, 2015. — 326 c. — ISBN 978-5-906-17271-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/33857

Дополнительная:

1. Спицын, В. Г. Информационная безопасность вычислительной техники : учебное пособие / В. Г. Спицын. — Томск : Томский государственный университет систем управления и радиоэлектроники, Эль Контент, 2011. — 148 c. — ISBN 978-5-4332-0020-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/13936

2. Горюхина, Е. Ю. Информационная безопасность : учебное пособие / Е. Ю. Горюхина, Л. И. Литвинова, Н. В. Ткачева. — Воронеж : Воронежский Государственный Аграрный Университет им. Императора Петра Первого, 2015. — 221 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/72672.html

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

https://www.intuit.ru/studies/courses/2291/591/lecture/12677 Лекции ИНТУИТ
s://studref.cohttpm/ Студенческие реферативные статьи и материалы
https://www.intuit.ru/studies/courses/2291/591/lecture/12677 Лекции ИНТУИТ
https://www.intuit.ru/studies/courses/10/10/lecture/304 Лекции ИНТУИТ
https://www.intuit.ru/studies/courses/531/387/lecture/8994 Лекции ИНТУИТ
https://www.lektorium.tv/course/22759 Криптографические протоколы. Николенко
https://www.intuit.ru/studies/courses/10/10/lecture/314 Лекции ИНТУИТ .
https://www.intuit.ru/studies/courses/3649/891/lecture/32341?page=3 Лекции ИНТУИТ
https://www.intuit.ru/studies/courses/600/456/lecture/10220?page=3 Лекции ИНТУИТ
https://www.intuit.ru/studies/courses/2291/591/lecture/12677 Лекции ИНТУИТ
https://www.intuit.ru/studies/courses/10/10/lecture/304 Лекции ИНТУИТ

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

Образовательный процесс по дисциплине **Дополнительные главы информационной безопасности** 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 "Libre office";
- приложение позволяющее просматривать и воспроизводить медиа контент PDF-файлов "Adobe Acrobat Reader DC";
- программы демонстрации видео материалов (проигрыватель) "Windows Media Plaer";
- программа просмотра интернет контента (браузер) "Google Chrome"

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.

Практические занятия проводятся в компьютерном классе кафедры радиоэлектроники и защиты информации с техническим оснащением, указанным в паспорте

Аудитория для самостоятельной работы: Компьютерный класс кафедры радиоэлектроники и защиты информации и помещения библиотеки с персональными компьютерами с доступом к локальной и глобальной сетям

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
Дополнительные главы информационной безопасности

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	Знания принципов, методов и средств 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** Отсутствие каких либо знаний методов и средств 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** Частично сформированы общие знания методов и средств 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. Не полностью сформировано умение свободно осуществлять мыслительную деятельность, ставить цели, и успешно достигать их в процессе профессиональной деятельности. Затрудненное владение терминологией. **Хорошо** Сформированные систематические знания методов и средств 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, не влияющие на общий уровень профессиональной подготовки. В

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо целом успешно сформировано умение свободно осуществлять мыслительную деятельность, ставить цели, и успешно достигать их в процессе профессиональной деятельности. Свободное владение терминологией за некоторым исключением. **Отлично** Полностью сформированные знания методов и средств 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. Сформировано умение свободно осуществлять мыслительную деятельность, ставить цели, и успешно достигать их в процессе профессиональной деятельности. Свободное владение терминологией.

ПК.6

Способен проводить контроль защищенности информации от утечки по техническим каналам

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.6.2 Подготавливает отчетные материалы по результатам специальных исследований	Умеет обеспечивать сбор научно-технической (научной) информации, необходимой для постановки и решения задач исследования	**Неудовлетворител** Не знает тенденции развития современных инфраструктурных решений, основные риски информационной безопасности; не умеет осуществлять сбор, анализ, структурирование научно-технической информации, необходимой для постановки и решения задач исследования; не владеет практическими навыками сбора, анализа и систематизации научно-технической информации **Удовлетворительн** Не совсем знает тенденции развития современных инфраструктурных решений, основные риски информационной

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительн безопасности; не совсем умеет осуществлять сбор, анализ, структурирование научно-технической информации, необходимой для постановки и решения задач исследования; слабое владение практическими навыками сбора, анализа и систематизации научно-технической информации **Хорошо** хорошо знает тенденции развития современных инфраструктурных решений, основные риски информационной безопасности; Умеет осуществлять сбор, анализ, структурирование научно-технической информации, необходимой для постановки и решения задач исследования; владеет практическими навыками сбора, анализа и систематизации научно-технической информации **Отлично** Отлично знает тенденции развития современных инфраструктурных решений, основные риски информационной безопасности; Умеет осуществлять сбор, анализ, структурирование научно-технической информации, необходимой для постановки и решения задач исследования; в совершенстве владеет практическими навыками сбора, анализа и систематизации научно-технической 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 46 до 60
«неудовлетворительно» / «незачтено» менее 46 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
Входной контроль	Технические средства защиты информации **Входное тестирование**	Проверяются базовые знания в области информационной безопасности и защиты информации.
ПК.6.2 Подготавливает отчетные материалы по результатам специальных исследований **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	Управление системой защиты **Защищаемое контрольное мероприятие**	Знание принципов организации и контроля системы защиты, умение разрабатывать политики безопасности
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	Организация разработки системы защиты информации **Защищаемое контрольное мероприятие**	Знание основных подсистем защиты информации и основных требований к ним

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.6.2 Подготавливает отчетные материалы по результатам специальных исследований **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	Итоговое контрольное мероприятие **Итоговое контрольное мероприятие**	Знание принципов организации и контроля системы защиты, умение разрабатывать политики безопасности. Знание основных подсистем защиты информации и основных требований к ним

Спецификация мероприятий текущего контроля

Технические средства защиты информации

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **0**
Проходной балл: **0**

Показатели оценивания	Баллы
Отсутствие ошибок при входном контроле	100
Одна ошибка при входном контроле	81
Две ошибки при входном контроле	61
Три ошибки при входном контроле	41

Управление системой защиты

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **13**

Показатели оценивания	Баллы
Знание угроз и каналов утечки информации	15
Знание методик оценки рисков и уязвимостей информационной системы	15

Организация разработки системы защиты информации

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **13**

Показатели оценивания	Баллы
Знание требований к применению способов, методов и средств защиты информации	15
Знание основных функциональных задач, решаемых системой защиты информации	15

Итоговое контрольное мероприятие

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы самостоятельной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **20**

Показатели оценивания	Баллы
Знание методик оценки качества системы защиты информации	10
Знание правил осуществления организационных мер защиты информации	10
Знание правил организации технических мер защиты информации	10
Знание порядка проведения работ по защите информации	10