

МИНОБРНАУКИ РОССИИ

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

Кафедра радиоэлектроники и защиты информации

Авторы-составители: **Лунегов Игорь Владимирович**

Рабочая программа дисциплины
ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ
Код УМК 80768

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

Пермь, 2020

1. Наименование дисциплины

Основы защиты информации

2. Место дисциплины в структуре образовательной программы

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

Направление: **03.03.01** Прикладные математика и физика
направленность Программа широкого профиля

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Основы защиты информации** у обучающегося должны быть сформированы следующие компетенции:

03.03.01 Прикладные математика и физика (направленность : Программа широкого профиля)

ОК.10 понимать сущность и значение информации в развитии современного общества, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны

4. Объем и содержание дисциплины

Направления подготовки	03.03.01 Прикладные математика и физика (направленность: Программа широкого профиля)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	4
Объем дисциплины (з.е.)	3
Объем дисциплины (ак.час.)	108
Контактная работа с преподавателем (ак.час.), в том числе:	42
Проведение лекционных занятий	14
Проведение практических занятий, семинаров	28
Проведение лабораторных работ, занятий по иностранному языку	0
Самостоятельная работа (ак.час.)	66
Формы текущего контроля	Входное тестирование (1) Защищаемое контрольное мероприятие (3) Итоговое контрольное мероприятие (1)
Формы промежуточной аттестации	Зачет (4 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Основы защиты информации. Первый семестр

Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ. Органы, обеспечивающие национальную безопасность РФ, цели, задачи. Национальные интересы РФ в информационной сфере. Приоритетные направления в области защиты информации в РФ. Тенденции развития информационной политики государств и ведомств. Государственная тайна. Правовое обеспечение защиты информации

Терминологические основы защиты информации. Основные понятия и определения. Понятие информации, информатизации, информационных систем и смежных с ними: информационная безопасность, инфор-мационная война, информационная агрессия, информационное оружие, информационные процессы, информационная система, информационная сфера. Понятия автора и собственника инфор-мации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации, уг-розы - определения, сопоставление.

Общеметодологические принципы теории защиты информации.
Этапы развития информационной безопасности:

1. Системы безопасности ресурса.
2. Этап развитой защиты (постепенное осознание необходимости комплексирования целей защиты, расширение арсенала используемых средств защиты, стали объединяться в функциональные самостоятельные системы защиты).
3. Этап комплексной защиты.
Требования к системе защиты информации.
Показатели информации: важность, полнота, адекватность, релевантность, толерантность.
Комплексность: целевая, инструментальная, структурная, функциональная, временная

Угрозы. Классификация и анализ угроз информационной безопасности.
Понятие угрозы. Виды угроз. Три наиболее выраженные уг-розы:

- 1) подверженность физическому искажению или унич-тожению;
 - 2) возможность несанкционированной (случайной или злоумышленной) модификации;
 - 3) опасность несанкцио-нированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена.
- Характер происхождения угроз: умышленные факторы, есте-ственные факторы.
Источники угроз. Предпосылки появле-ния угроз: объективные, субъективные.

Способы нарушения конфиденциальности, целостности и доступности информации.
Классы каналов несанкционированного получения инфор-мации:

- 1) непосредственно с объекта;
- 2) с каналов отображения информации;
- 3) получение по внешним каналам;
- 4) подклю-чение к каналам получения информации.

Причины нарушения целостности информации: субъективные преднамеренные, субъективные

непреднамеренные,

объективные непреднамеренные.

Потенциально возможные злоумышленные действия в автоматизированных системах обработки данных.

Основные функции защиты информации.

Стратегии защиты информации: оборонительная стратегия,

наступательная стратегия, упреждающая стратегия.

Архитектура систем защиты информации.

Семирубежная модель защиты информации.

Причины, виды, каналы утечки и искажения информации.

Три методологических подхода к оценке уязвимости информации: эмпирический, теоретический и теоретико-эмпирический.

Модель затрат, разработанная специалистами американской фирмы IBM. Модель защиты - модель системы с полным перекрытием. Последовательность решения задачи защиты информации.

Фундаментальные требования, которым должны удовлетворять те вычислительные системы, которые используются для обработки конфиденциальной информации. Требования разделены на три группы: стратегия, подотчетность, гарантии. Классификация автоматизированных систем и требований по защите информации. Факторы, влияющие на требуемый уровень защиты информации.

Функции и задачи защиты информации.

Методы формирования функций защиты. Соккрытие информации о средствах, комплексах, объектах и системах обработки информации.

Дезинформация противника. Легендирование. Введение избыточности элементов системы.

Резервирование элементов системы. Регулирование доступа к элементам системы и защищаемой информации. Регулирование использования элементов системы и защищаемой информации.

Маскировка информации. Регистрация сведений. Уничтожение информации. Обеспечение сигнализации.

Обеспечение реагирования. Управление системой защиты информации. Обеспечение требуемого уровня готовности

обслуживающего персонала к решению задач информационной безопасности. Защита от информационного воздействия

на технические средства обработки. Защита от информационного воздействия на общество. Защита от информационного воздействия на психику человека. Применение криптографии. Региональные компоненты защиты информации. Защита информации предприятия. Проведение анализа защищенности локального объекта.

Итоговое контрольное мероприятие

Проверка уровня усвоения дисциплины.

Знания теории защиты информации, основных направлений. Обеспечение информационной безопасности и направления защиты.

Комплексность (целевая, инструментальная, структурная, функциональная, временная). Требования к системе защиты информации. Угрозы информации. Виды угроз. Основные нарушения. Характер происхождения угроз. Источники угроз. Предпосылки появления угроз.

Система защиты информации. Классы каналов несанкционированного получения информации.

Причины нарушения целостности информации. Методы и модели оценки уязвимости информации.

Общая модель воздействия на информацию.

Общая модель процесса нарушения физической целостности информации. Структурированная схема

потенциально возможных злоумышленных действий в автоматизированных системах обработки данных. Методологические подходы к оценке уязвимости информации. Модель защиты системы с полным перекрытием. Рекомендации по использованию моделей оценки уязвимости информации. Допущения в моделях оценки уязвимости информации. Методы определения требований к защите 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 аудиторские 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. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2020. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. <https://www.urait.ru/bcode/449285>
2. Сычев Ю. Н. Основы информационной безопасности: Учебно-методический комплекс/Сычев Ю. Н..- Москва:Евразийский открытый институт,2012, ISBN 978-5-374-00602-5.-342. <http://www.iprbookshop.ru/14642>

Дополнительная:

1. Мельников В. П.,Клейменов С. А.,Петраков А. М. Информационная безопасность и защита информации:учеб. пособие для вузов/В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова.-М.:Академия,2008, ISBN 978-5-7695-4884-0.-336.-Библиогр.: с. 327-328
2. Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : учебно-методическое пособие / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 218 с. — ISBN 978-5-4487-0297-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/77317.html>
3. Современные радиоэлектронные средства и технологии информационной безопасности : монография / В. А. Майстренко, А. А. Соловьев, М. Ю. Пляскин, А. И. Тихонов. — Омск : Омский государственный технический университет, 2017. — 356 с. — ISBN 978-5-8149-2554-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/78508.html>

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

<https://www.securitycode.ru/> Сайт компании "Код безопасности"

www.infoguard.ru/ сайт НТИЦ "Информационная безопасность"

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

Образовательный процесс по дисциплине **Основы защиты информации** предполагает использование следующего программного обеспечения и информационных справочных систем: Образовательный процесс по дисциплине предполагает использование следующего информационных технологий, программного обеспечения и информационных справочных систем:

- презентационные материалы (слайды по темам лекционных и практических занятий);
- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательную 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

Аудитория для проведения занятий лекционного и практического типа оснащена презентационной техникой:

- 1) персональный компьютер или ноутбук с соответствующим программным обеспечением;
- 2) мультимедийное оборудование (проектор, экран);
- 3) маркерная доска и маркеры (или меловая доска и мел)

Аудитория для текущего контроля:

- 1) персональный компьютер или ноутбук с соответствующим программным обеспечением;
- 2) мультимедийное оборудование (проектор, экран);
- 3) маркерная доска и маркеры (или меловая доска и мел)

Аудитория для индивидуальных (групповых) консультаций:

- 1) персональный компьютер или ноутбук с соответствующим программным обеспечением;
- 2) мультимедийное оборудование (проектор, экран);
- 3) маркерная доска и маркеры (или меловая доска и мел)

Аудитория для самостоятельной работы:

- 1) компьютерная техника с возможностью подключения к сети «Интернет», с доступом в электронную информационно-образовательную среду ПГНИУ;
- 2) помещения Научной библиотеки ПГНИУ

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:

1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютерами 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
Основы защиты информации**

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

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ОК.10 понимать сущность и значение информации в развитии современного общества, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны</p>	<p>- знать нормативную базу по вопросам защиты информации, угрозы информационной безопасности, каналы утечки информации, технические средства по защите информации;</p> <p>- уметь определить состояние защищенности предприятия, выявлять потенциальные внешние и внутренние угрозы;</p> <p>- владеть методами по защите информации при передаче данных по открытым каналам связи.</p>	<p align="center">Неудовлетворител</p> <p>Не знает основ дисциплины, необходимых при формировании компетенции Отсутствие умений Отсутствие навыков</p> <p align="center">Удовлетворительн</p> <p>Общие, но не структурированные знания нормативной базы в области защиты информации, каналов утечки информации и технических средств по ее защите. Частично сформированные умения определить состояние защищенности предприятия, выявлять потенциальные внешние и внутренние угрозы. Фрагментарное применение навыков владения методами по защите информации при передаче данных по открытым каналам связи.</p> <p align="center">Хорошо</p> <p>Сформированные но содержащие отдельные пробелы знания нормативной базы в области защиты информации, каналов утечки информации и технических средств по ее защите. В целом успешные, но содержащие отдельные пробелы умения определить состояние защищенности предприятия, выявлять потенциальные внешние и внутренние угрозы. В целом успешное, но содержащее отдельные пробелы применение навыков владения методами по защите информации при передаче данных по открытым каналам связи.</p> <p align="center">Отлично</p> <p>Сформированные систематические знания</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p style="text-align: center;">Отлично</p> <p>нормативной базы в области защиты информации, каналов утечки информации и технических средств по ее защите. Сформированное умение определить состояние защищенности предприятия, выявлять потенциальные внешние и внутренние угрозы. Успешное и систематическое применение навыков владения методами по защите информации при передаче данных по открытым каналам связи.</p>

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 50 до 60

«неудовлетворительно» / «незачтено» менее 50 балла

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
Входной контроль	Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ. Входное тестирование	проверка остаточных знаний по курсу общая физика и представлений о распространении звуковых и электромагнитных волн
ОК.10 понимать сущность и значение информации в развитии современного общества, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны	Угрозы. Классификация и анализ угроз информационной безопасности. Защищаемое контрольное мероприятие	Знания нормативной базы в области защиты информации. Умения классифицировать угрозы безопасности информации
ОК.10 понимать сущность и значение информации в развитии современного общества, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны	Способы нарушения конфиденциальности, целостности и доступности информации. Защищаемое контрольное мероприятие	знание способов нарушения конфиденциальности, целостности, полноты и доступности

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОК.10 понимать сущность и значение информации в развитии современного общества, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны	Функции и задачи защиты информации. Защищаемое контрольное мероприятие	Знание каналов утечки информации, видов инженерно-технической защиты и организационных мероприятий по защите информации.
ОК.10 понимать сущность и значение информации в развитии современного общества, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны	Итоговое контрольное мероприятие Итоговое контрольное мероприятие	знание нормативной базы в области защиты информации, каналов утечки информации, технических средств защиты.

Спецификация мероприятий текущего контроля

Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ.

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **0**

Проходной балл: **0**

Показатели оценивания	Баллы
Допущено менее 10% ошибок при тестировании	81
Допущено менее 30% ошибок при тестировании	61
Допущено менее 50% ошибок при тестировании	41
Допущено более 50% ошибок при тестировании	0

Угрозы. Классификация и анализ угроз информационной безопасности.

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

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**

Проходной балл: **10**

Показатели оценивания	Баллы
представить доклад по теме дисциплины	10
знать типы угроз и уметь их классифицировать	5
уметь определять вероятность реализации угроз	5

Способы нарушения конфиденциальности, целостности и доступности информации.

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
 Условия проведения мероприятия: **в часы аудиторной работы**
 Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**
 Проходной балл: **10**

Показатели оценивания	Баллы
представление доклада по теме дисциплины	10
знать за счет чего происходит нарушение конфиденциальности, целостности, полноты и доступности	5
уметь определять причину несанкционированного доступа к информации	5

Функции и задачи защиты информации.

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
 Условия проведения мероприятия: **в часы аудиторной работы**
 Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**
 Проходной балл: **10**

Показатели оценивания	Баллы
Представить доклад по теме дисциплины	10
Знание каналов утечки информации. Умение выявлять причину и источники технических каналов утечки информации	5
Знание видов защиты информации, способов их применения и реализации.	5

Итоговое контрольное мероприятие

Продолжительность проведения мероприятия промежуточной аттестации: **10 часа**
 Условия проведения мероприятия: **в часы самостоятельной работы**
 Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
 Проходной балл: **20**

Показатели оценивания	Баллы
Знать: Угрозы информации. Виды угроз. Основные нарушения. Характер происхождения угроз. Источники угроз. Предпосылки появления угроз.	10
Знать основы нормативно-правовой базы в области защиты информации, иерархию законодательных актов в области защиты информации	10
Знать: Модель защиты системы с полным перекрытием. Рекомендации по использованию моделей оценки уязвимости информации. Допущения в моделях оценки уязвимости информации. Методы определения требований к защите информации. Факторы, обуславливающие конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации. Классификация требований к средствам защиты информации. Требования к защите, определяемые структурой автоматизированной системы обработки данных. Требования к защите, обуславливаемые видом защищаемой информации. Требования, обуславливаемые взаимодействием пользователя с комплексом средств автоматизации. Анализ существующих методик определения требований к защите информации.	10
Знать: Классы каналов несанкционированного получения информации. Причины нарушения целостности информации. Методы и модели оценки уязвимости информации.	10

	<p>Общая модель воздействия на информацию. Общая модель процесса нарушения физической целостности информации. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных. Методологические подходы к оценке уязвимости информации.</p>
--	--