МИНОБРНАУКИ РОССИИ

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

Кафедра информационной безопасности и систем связи

Авторы-составители: **Пенский Олег Геннадьевич**
Лобков Армандо Львович
Мустакимова Яна Романовна
Никитина Елена Юрьевна

Рабочая программа дисциплины

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Код УМК 81395

Утверждено
Протокол №6
от «26» июня 2020 г.

Пермь, 2020

1. Наименование дисциплины

Теоретические основы компьютерной безопасности

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в базовую 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 **Теоретические основы компьютерной безопасности** у обучающегося должны быть сформированы следующие компетенции:

10.05.01 Компьютерная безопасность (специализация : Разработка защищенного программного обеспечения)

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

ОК.6 Способность анализировать социально значимые проблемы и процессы

ОПК.3 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ПК.10 Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах

ПК.11 способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи

ПК.14 способность обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения

ПК.15 Способность оценивать эффективность системы защиты информации в компьютерных системах

ПК.3 Способность к анализу и формализации поставленных задач в области информационной безопасности

ПК.4 способность проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов в области компьютерной безопасности

ПК.5 Способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций

ПК.6 Способность разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем

ПК.7 Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований

ПК.9 Способность проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем

4. Объем и содержание дисциплины

Направления подготовки	10.05.01 Компьютерная безопасность (направленность: Разработка защищенного программного обеспечения)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	9
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	0
Проведение лабораторных работ, занятий по иностранному языку	28
Самостоятельная работа (ак.час.)	88
Формы текущего контроля	Защищаемое контрольное мероприятие (1) Итоговое контрольное мероприятие (1) Письменное контрольное мероприятие (1)
Формы промежуточной аттестации	Экзамен (9 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Теоретические основы компьютерной безопасности. Первый семестр

Студенты должны усвоить то, что компьютерная безопасность является частью информационной безопасности государства, должны понять общие принципы построения СЗИ и формализацию в подходе построения СЗИ, студенты должны научиться применять при построении оценки эффективности СЗИ правила четкой и нечеткой математики, уметь использовать методы экспертных оценок при создании СЗИ, должны создать СЗИ ПК и оценить ее эффективность с помощью всех изученных методов и применении метода экспертного оценивания DELPHI, должны понять общие принципы работы хакеров в сети Интернет и уметь работать в сети с наибольшей вероятностью предохранения от утечек информации, должны усвоить принципы организации работы СЗИ в банковских структурах и узнать современные основные угрозы ИС, должны узнать об основных типах сетей и классификации СЗИ этих сетей.

Безопасность информации в компьютерных системах и ее составляющие

При рассмотрении данной темы необходимо дать характеристики следующим неопределенностям, влияющим на адекватность работы СЗИ:

☐ Неясное представление целей СЗИ;
☐ Неясное представление угроз и ущерба от наступающих угроз;
☐ Отсутствие точных методов оценки эффективности СЗИ.

Построение системы защиты компьютерных систем

При рассмотрении данной темы необходимо сформировать у студентов твердые навыки по использованию матрицы знаний при создании СЗИ. Студент должен разработать программу, позволяющую заполнять элементы матрицы знаний в ходе создания СЗИ. На лекции преподаватель рассказывает о структуре матрицы знаний и контроле создания СЗИ на основе этой матрицы знаний. При рассмотрении данной темы необходимо сформировать у студентов практические навыки построения матрицы знаний, как основном механизме планирования создания СЗИ. Студентам в качестве практического задания предлагается разработать компьютерную программу, формирующую матрицу знаний для ПК. Текущим контролем усвоения материалов темы является защита плана построения СЗИ ПК с помощью матрицы знаний перед аудиторией.

Принципы защиты информации в компьютерных системах

Студент должен понять общие свойства большинства математических моделей и методов оценки эффективности СЗИ. Он должен знать то, все методы носят оценочный и приближенный характер, часто использующий экспертное оценивание и, как нечеткие, так и четкие характеристики. Студенты должны понять, что, исходя из этого, матмодели СЗИ делятся на три типа: основанные на теории четкой математики, нечеткой математики и использующие смешанные основы.

Студент, основываясь на знаниях теории вероятностей и понятиях теории нечетких множеств, должен освоить методы построения функции ущерба СЗИ и вычислять численные значения этой функции для конкретных СЗИ. Студент должени уметь применять расчеты для определения наиболее эффективной СЗИ из заданных СЗИ.

Комплексное применение моделей СЗИ при построении СЗИ

1. Создание СЗИ терминального класса.
2. Применение матрицы знаний при создании СЗИ ТК.
3. Оценка эффективности СЗИ ТК на основе методов проективного ранжирования.
4. Оценка эффективности СЗИ ТК на основе функции устраненного ущерба.
5. Вычисление материальных затрат по созданию СЗИ ТК, как одних из показателей эффективности СЗИ.

Безопасность сети Интернет

Интернет.

Студент должен изучить следующие вопросы:

1. Интернет в структуре информационно-аналитического обеспечения.
2. Основные протоколы Интернет и их использование злоумышленниками.
3. Аутентификация в Интернет.
4. Легкость наблюдения за передаваемыеми данными.
5. Потенциальные проблемы с электронной почтой.

Классификация СЗИ

Студент должен ознакомиться с типами ИС и СЗИ для каждого из этих типов.

Обзор материала курса

Дается обзор основного (главного), прочитанного курса, того, на что стоит обратить особое внимание. В качестве лабораторной работы студенты готовять СЗИ с применением матрицы знаний о СЗИ, математических моделей СЗИ и применения программного обоспечения, решающего задачи компьютерной безопасности.

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. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/87995.html

2. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 c. — ISBN 978-5-4497-0675-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/97562

3. 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

Дополнительная:

1. 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

2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // ЭБС Юрайт [сайт]. https://urait.ru/bcode/449548

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 **Теоретические основы компьютерной безопасности** предполагает использование следующего программного обеспечения и информационных справочных систем:
Ресурсы сети Интернет

- 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

Аппаратура Центра Интернет ПГНИУ, аудиоколнки, видеопроектры и микрофон для чтения лекций в большой аудитории
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 компьютерный класс. Состав оборудования определен в Паспорте компьютерного класса.
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 «Интернет» 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
Теоретические основы компьютерной безопасности

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

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.3 Способность к анализу и формализации поставленных задач в области информационной безопасности	Знать основные задачи в области информационной безопасности. Уметь формализовать поставленные задачи в области информационной безопасности. Владеть методами анализа поставленных задач в области информационной безопасности.	**Неудовлетворител** Не знает задачи ИБ **Удовлетворительн** Знает основные задачи ИБ **Хорошо** Знает основные задачи ИБ и структуру матрицы знания для построения СЗИ **Отлично** Знает основные задачи ИБ и структуру матрицы знания для построения СЗИ. Может применить матрицу знаний при построении простейшей СЗИ.
ПК.14 способность обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения	Знать базовые модели решения профессиональной задачи. Уметь обосновывать правильность выбранной модели решения профессиональной задачи, Владеть навыками обработки результатов экспериментов.	**Неудовлетворител** Не знает модели численной оценки эффективности СЗИ. **Удовлетворительн** Знает модели численной оценки эффективности СЗИ. Знает метод ДЕЛФИ экспертного оценивания эффективности сЗИ. **Хорошо** Знает модели численной оценки эффективности СЗИ. Знает метод ДЕЛФИ экспертного оценивания эффективности СЗИ. Знает метод функции устраненного ущерба для оценки эффективности СЗИ. **Отлично** Знает модели численной оценки эффективности СЗИ. Знает метод ДЕЛФИ экспертного оценивания эффективности СЗИ. Знает метод функции устраненного ущерба для оценки эффективности СЗИ. Может применит модели эффективности оценки СЗИ при посторении простейших СЗИ.
ПК.7 Способность провести обоснование и выбор рационального решения	Знать основы информационной безопасности компьютерных систем. Уметь выбирать рациональное решение по	**Неудовлетворител** Не умеет создавать простейшие СЗИ **Удовлетворительн** Умеет создавать простейшие СЗИ

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований	уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований и обосновывать его. Владеть методами определения уровня обеспечения информационной безопасности компьютерных систем с учетом заданных требований	**Хорошо** Умеет создавать простейшие СЗИ и оценивать их эффективность с помощью математических моделей. **Отлично** Умеет создавать простейшие СЗИ и оценивать их эффективность с помощью математических моделей. Может проектировать СЗИ с упреждением угроз.
ПК.9 Способность проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем	Знать основы информационной безопасности компьютерных систем Уметь проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем. Владеть методами анализа проектных решений по обеспечению информационной безопасности компьютерных систем.	**Неудовлетворител** Не знает основных принципов, обеспечиавющих безопасность сети Интернет **Удовлетворительн** Знает основные принципы, обеспечиавющие безопасность сети Интернет **Хорошо** Знает основные принципы, обеспечиавющие безопасность сети Интернет. Знает основные протоколы Интернет. **Отлично** Знает основные принципы, обеспечиавющие безопасность сети Интернет. Знает основные протоколы Интернет. Знает типы антивирусных программ и принципы их работы.
ПК.5 Способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций	Знать основы обеспечения информационной безопасности компьютерных систем. Уметь осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, Владеть навыками обработки найденной информации, оформления результатов проведенных исследований в виде конкретных рекомендаций.	**Неудовлетворител** Не знает задачи ИБ **Удовлетворительн** Знает основные задачи ИБ **Хорошо** Знает основные задачи ИБ и структуру матрицы знания для построения СЗИ **Отлично** Знает основные задачи ИБ и структуру матрицы знания для построения СЗИ. Может применить матрицу знаний при построении простейшей СЗИ.
ПК.11 способность оценивать степень надежности выбранных механизмов	Знать механизмы обеспечения безопасности. Уметь оценивать степень надежности выбранных механизмов обеспечения	**Неудовлетворител** Не знает задачи ИБ **Удовлетворительн**

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
обеспечения безопасности для решения поставленной задачи	безопасности для решения поставленной задачи. Владеть методами оценки степени надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи.	**Удовлетворительн** Знает основные задачи ИБ **Хорошо** Знает основные задачи ИБ и структуру матрицы знания для построения СЗИ **Отлично** Знает основные задачи ИБ и структуру матрицы знания для построения СЗИ. Может применить матрицу знаний при построении простейшей СЗИ.
ПК.15 Способность оценивать эффективность системы защиты информации в компьютерных системах	Знать составляющие системы защиты информации в компьютерных системах. Уметь оценивать эффективность системы защиты информации в компьютерных системах. Владеть методами оценки эффективности системы защиты информации в компьютерных системах.	**Неудовлетворител** Не знает задачи ИБ **Удовлетворительн** Знает основные задачи ИБ **Хорошо** Знает основные задачи ИБ и структуру матрицы знания для построения СЗИ **Отлично** Знает основные задачи ИБ и структуру матрицы знания для построения СЗИ. Может применить матрицу знаний при построении простейшей СЗИ.
ПК.4 способность проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов в области компьютерной безопасности	Знать отечественные и зарубежные стандарты в области компьютерной безопасности. Уметь проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов в области компьютерной безопасности. Владеть методами анализа безопасности компьютерных систем с использованием отечественных и зарубежных стандартов в области компьютерной безопасности.	**Неудовлетворител** Не умеет создавать простейшие СЗИ **Удовлетворительн** Умеет создавать простейшие СЗИ **Хорошо** Умеет создавать простейшие СЗИ и оценивать их эффективность с помощью математических моделей. **Отлично** Умеет создавать простейшие СЗИ и оценивать их эффективность с помощью математических моделей. Может проектировать СЗИ с упреждением угроз.
ПК.6 Способность разрабатывать математические модели	Знать составляющие системы обеспечения информационной безопасности компьютерных систем. Уметь разрабатывать	**Неудовлетворител** Не знает модели численной оценки эффективности СЗИ. **Удовлетворительн**

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
защищаемых систем и системы обеспечения информационной безопасности компьютерных систем	математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем Владеть математическим аппаратом для разработки математических моделей защищаемых систем и системы обеспечения информационной безопасности компьютерных систем.	**Удовлетворительн** Знает модели численной оценки эффективности СЗИ. Знает метод ДЕЛФИ экспертного оценивания эффективности сЗИ. **Хорошо** Знает модели численной оценки эффективности СЗИ. Знает метод ДЕЛФИ экспертного оценивания эффективности СЗИ. Знает метод функции устраненного ущерба для оценки эффективности СЗИ. **Отлично** Знает модели численной оценки эффективности СЗИ. Знает метод ДЕЛФИ экспертного оценивания эффективности СЗИ. Знает метод функции устраненного ущерба для оценки эффективности СЗИ. Может применит модели эффективности оценки СЗИ при посторении простейших СЗИ.
ПК.10 Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах	Знать компоненты системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах. Уметь принимать участие в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах.	**Неудовлетворител** Не знает модели численной оценки эффективности СЗИ. **Удовлетворительн** Знает модели численной оценки эффективности СЗИ. Знает метод ДЕЛФИ экспертного оценивания эффективности сЗИ. **Хорошо** Знает модели численной оценки эффективности СЗИ. Знает метод ДЕЛФИ экспертного оценивания эффективности СЗИ. Знает метод функции устраненного ущерба для оценки эффективности СЗИ. **Отлично** Знает модели численной оценки эффективности СЗИ. Знает метод ДЕЛФИ экспертного оценивания эффективности СЗИ. Знает метод функции устраненного ущерба для оценки эффективности СЗИ. Может применит модели эффективности оценки СЗИ при посторении простейших СЗИ.
ОК.10 понимать сущность и значение информации в развитии современного	Знать основные требования информационной безопасности. Уметь понимать сущность и значение информации в	**Неудовлетворител** Не знает задачи ИБ **Удовлетворительн** Знает основные задачи ИБ **Хорошо**

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
общества, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны	развитии современного общества, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны	**Хорошо** Знает основные задачи ИБ и структуру матрицы знания для построения СЗИ **Отлично** Знает основные задачи ИБ и структуру матрицы знания для построения СЗИ. Может применить матрицу знаний при построении простейшей СЗИ.
ОК.6 Способность анализировать социально значимые проблемы и процессы	Знать социально значимые проблемы и процессы. Уметь анализировать социально значимые проблемы и процессы. Владеть методами анализа социально значимых проблем и процессов.	**Неудовлетворител** Не знает задачи ИБ **Удовлетворительн** Знает основные задачи ИБ **Хорошо** Знает основные задачи ИБ и структуру матрицы знания для построения СЗИ **Отлично** Знает основные задачи ИБ и структуру матрицы знания для построения СЗИ. Может применить матрицу знаний при построении простейшей СЗИ.
ОПК.3 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Знать основные требования информационной безопасности. Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	**Неудовлетворител** Не знает задачи ИБ **Удовлетворительн** Знает основные задачи ИБ **Хорошо** Знает основные задачи ИБ и структуру матрицы знания для построения СЗИ **Отлично** Знает основные задачи ИБ и структуру матрицы знания для построения СЗИ. Может применить матрицу знаний при построении простейшей СЗИ.

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 47 до 60
«неудовлетворительно» / «незачтено» менее 47 балла

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.3 Способность к анализу и формализации поставленных задач в области информационной безопасности **ОПК.3** способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности **ПК.5** Способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций **ПК.6** Способность разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем **ОК.6** Способность анализировать социально значимые проблемы и процессы **ПК.9** Способность проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем **ОК.10** понимать сущность и значение информации в развитии современного общества,	Построение системы защиты компьютерных систем **Письменное контрольное мероприятие**	Знание основных задач компьютерной безопасности, основ, направлений и этапов создания СЗИ, умение применять матрицу знаний для создания простейших СЗИ.

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны **ПК.11** способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи		
ОПК.3 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности **ПК.5** Способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций **ОК.6** Способность анализировать социально значимые проблемы и процессы **ПК.14** способность обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения **ПК.15** Способность оценивать эффективность системы защиты информации в компьютерных системах	Принципы защиты информации в компьютерных системах **Защищаемое контрольное мероприятие**	Умение применять матрицу знаний при построении простейшей СЗИ. Умение применять функцию устраненного ущерба при оценке эффективности простейших СЗИ.

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.4 способность проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов в области компьютерной безопасности **ПК.7** Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований **ПК.10** Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах	Классификация СЗИ **Итоговое контрольное мероприятие**	Знание классификации СЗИ. Знание физических, аппаратных, программных, организационных, законодательных средств.

Спецификация мероприятий текущего контроля

Построение системы защиты компьютерных систем

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **15**

Показатели оценивания	Баллы
Знание основ, направлений и этапов создания СЗИ	10
Умение применять матрицу знаний для создания простейших СЗИ	10
Знание основных задач компьютерной безопасности	10

Принципы защиты информации в компьютерных системах

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **15**

Показатели оценивания	Баллы
Умение применять матрицу знаний при построении простейшей СЗИ	15
Умение применять функцию устраненного ущерба при оценке эффективности простейших СЗИ.	15

Классификация СЗИ

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **17**

Показатели оценивания	Баллы
Знание физических, аппаратных, программных СЗИ.	15
Знание организационных, законодательных СЗИ.	15
Знание классификации СЗИ.	10