МИНОБРНАУКИ РОССИИ

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

Колледж профессионального образования

Авторы-составители: **Серебрякова Наталия Александровна**

Рабочая программа дисциплины

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Код УМК 99266

Утверждено
Протокол №10
от «25» мая 2022 г.

Пермь, 2022

1. Наименование дисциплины

Информационная безопасность

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в Блок « ПРОФ » образовательной программы по направлениям подготовки (специальностям):

Направление подготовки: **09.02.07** Информационные системы и программирование
направленность не предусмотрена

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Информационная безопасность** у обучающегося должны быть сформированы следующие компетенции:

09.02.07 Информационные системы и программирование (направленность : не предусмотрена)

ОК.1 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам

ОК.2 Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности

ОК.4 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами

ОК.7 Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях

ПК.4.4 Обеспечивать защиту программного обеспечения компьютерных систем программными средствами

4. Объем и содержание дисциплины

Направление подготовки	09.02.07 Информационные системы и программирование (направленность: не предусмотрена) на базе основного общего
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	11
Объем дисциплины (з.е.)	4.3
Объем дисциплины (ак.час.)	156
Контактная работа с преподавателем (ак.час.), в том числе:	104
Проведение лекционных занятий	48
Проведение практических занятий, семинаров	56
Самостоятельная работа (ак.час.)	52
Формы текущего контроля	Входное тестирование (1) Защищаемое контрольное мероприятие (2) Итоговое контрольное мероприятие (1)
Формы промежуточной аттестации	Экзамен (11 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Основы информационной безопасности

В разделе рассматриваются основные понятия информационной безопасности и защиты информации.

Основные понятия и определения, эволюция подходов к обеспечению информационной безопасности. аспекты информационной безопасности

Общие проблемы безопасности. Роль и место информационной безопасности.
Основные предметные направления защиты информации
Информационные, программно-математические, физические и организационные угрозы системы
- Понятие угрозы защиты информации, источники угроз.
- Угрозы информации в ЭВМ.
- Классификация угроз и их характеристики.
- Функции и задачи защиты информации.
- Угроза безопасности информации в компьютерных системах.

Функции и задачи защиты информации. Методы и системы защиты информации

Защита от несанкционированного доступа, модели, и основные принципы защиты информации.
Функции и задачи защиты информации. Методы и системы защиты информации.
Основные свойства защищаемой информации.
Методы и средства защиты информации от традиционных шпионажи и диверсий.
Методы и средства защиты информации от электромагнитных излучений и наводок

Организационное обеспечение информационной безопасности. Модели угроз и нарушителей информационной безопасности организации.

Определение понятия «конфиденциальное делопроизводство». Сущность и задачи конфиденциального делопроизводства, его организационно-технические особенности.
Организация конфиденциального делопроизводства. Задачи и функции подразделения по работе с конфиденциальными документами. Нормативно-правовая регламентация деятельности подразделения по работе с конфиденциальными документами. Угрозы документам в процессе работы с ними руководителей, специалистов и технических сотрудников. Разрешительная система доступа к бумажным и электронным документам, ее назначение, содержание и организация. Деятельность постоянно действующей экспертной комиссии.

Политика ИБ организации

Правомерные методы получения предпринимательской информации, их состав. Понятие разведки в бизнесе как одной из форм маркетингового исследования. Промышленный и экономический шпионаж, его сущность и сфера распространения. Легальные способы получения ценной и конфиденциальной информации. Нелегальные способы получения ценной и конфиденциальной информации, их состав. Методы нелегального получения информации. Агентурный канал. Технические средства промышленного шпионажа.

Организация безопасности в автоматизированных информационных системах АИС

В разделе рассматриваются основные способы и методы программной защиты информации в автоматизированных информационных системах

Угрозы безопасности АИС. Угрозы доступности, конфиденциальности, целостности информации

Понятие клиента прав доступа, групп, паролей, политики безопасности в современных АИС
Элементы и объекты защиты информации в АИС. Угрозы безопасности информации. Методы подтверждения подлинности пользователей и разграничение доступа к компьютерным ресурсам. Цели

защиты информации в АИС.
Информационные, программно-математические, физические и организационные угрозы.
Обеспечение и поддержка целостности и согласованности данных в АИС. Основные цели политики безопасности современных АИС. Методы и приемы обеспечения безопасности информации в АИС.
Политика безопасности АИС.
Принципы организации разноуровнего доступа в АИС. Способы защиты. Разграничение и управление доступом к элементам защищаемой информации.

Методы защиты от угроз в АИС

Цели и задачи системы защиты конфиденциальной информации. Комплексность системы защиты и принципы ее построения. Методика разработки системы защиты информации предприятия. Правовая, организационная, инженерно-техническая система защиты конфиденциальной информации. Криптографическая система защиты информации. Компьютерные вирусы и способы воздействия на информацию. Методы и средства обеспечения компьютерной безопасности.

Криптографические методы защиты информации

В разделе изучаются специальные методы шифрования, кодирования или иного преобразования информации, в результате которого ее содержание становится недоступным без предъявления ключа криптограммы и обратного преобразования

Шифрование. Шифры. Стандарты шифрования.

Основные понятия: криптология, криптография, ключ, криптографическая система. Требования к криптографическим методам преобразования информации. Этапы развития криптологии как науки.

Криптосистемы.

Методы криптографии. Средства криптографической защиты информации (СКЗИ). Криптографические преобразования. Шифрование и дешифрование информации. Причины нарушения безопасности информации при ее обработке СКЗИ (утечки информации по техническому каналу, неисправности в элементах СКЗИ, работа совместно с другими программами). Использование криптографических средств для решения задач идентификация и аутентификация. Электронная цифровая подпись (ЭЦП), принципы ее формирования и использования. Подтверждение подлинности объектов и субъектов информационной системы. Контроль за целостностью информации. Хэш-функции, принципы использования хэш-функций для обеспечения целостности данных.

Идентификация и аутентификация. Хэш-функции

Классификация криптосистем. Алгоритмы шифрования. Шифры замены. Шифры перестановки. Ассиметричное шифрование: метод гаммирования и аналитического преобразования данных.

Асимметричное шифрование. Электронно-цифровая подпись.

Зашифровывание и расшифровывание. Криптостойкость шифра. Алгоритмы шифрования.
Симметричное шифрование
Асимметричное шифрование (с открытым ключом). Хеш-функции. ЭЦП

Безопасность операционных систем

В разделе изучаются основные вопросы организации безопасности ОС Unix и Windows.

Основные механизмы безопасности в ОС Windows, Linux. Администрирование ОС

Программы-детекторы, программы-доктора, программы-ревизоры, программы-фильтры. Профилактика заражения вирусом. Зашита информации в сетях. Компьютерный вирус: понятие, пути распространения, проявление действия вируса. Структура современных вирусов: модели поведения вирусов;

деструктивные действия вируса; разрушение программы защиты, схем контроля или изменение состояния программной среды; воздействия на программно-аппаратные средства защиты информации. Программы-шпионы. Взлом парольной защиты. Защита от воздействия вирусов.

Программно-аппаратные средства защиты информации

В разделе изучаются программы и комплексы, предназначенные для решения задач, связанных с обеспечением информационной безопасности.

Программно-аппаратные средства защиты компьютерной информации от НСД

Проблема вирусного заражения программ
Классификация вирусов. Вред наносимый информации компьютерными вирусами
Структура современных антивирусных программ и перспективные методы антивирусной защиты.
Методы борьбы с компьютерными вирусами

Правовое обеспечение информационной безопасности

В разделе рассмотрены вопросы правовой сферы информационной защит, совокупность официальных взглядов на цели, задачи, направления развития политики в сфере информационной безопасности РФ. Понятие, виды норм и условия применения юридической ответственности за нарушение правовых норм в области защиты
информации. Уголовная ответственность за нарушение правовых норм в сфере защищаемой информации. Административная
ответственность за нарушения правовых норм в сфере защищаемой информации. Особенности юридической ответственности за
нарушение норм информационной безопасности в области трудовых и гражданско-правовых отношений

Системы защиты государственной тайны и конфиденциальной информации.

Правовые основы защиты информации
Правовые и законодательные меры по защите информации
Административные и организационные мероприятия информационной безопасности
Построение политики безопасности организации.

Модели информационной безопасности; международные и отечественные стандарты информационной безопасности, политика безопасности

Безопасность компьютерных сетей
Элементы сети. Возможности угрозы целостности информации сети.
Защита информации в компьютерных сетях.
Политика безопасности работы в Интернете.
Требования к защищенности КС от несанкционированного изменения структур.
Система разграничения доступа к информации в КС.
Меры технологической безопасности информации в вычислительных сетях.
Программные и технические средства защиты информации в сети.
Сетевые экраны/

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. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2021. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. https://urait.ru/bcode/470351

2. Рыбальченко, М. В. Архитектура информационных систем : учебное пособие для среднего профессионального образования / М. В. Рыбальченко. — Москва : Издательство Юрайт, 2020. — 91 с. — (Профессиональное образование). — ISBN 978-5-534-01252-1. — Текст : электронный // ЭБС Юрайт [сайт]. https://urait.ru/bcode/452922

3. 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

Дополнительная:

1. Информационные технологии в 2 т. Том 1 : учебник для среднего профессионального образования / В. В. Трофимов, О. П. Ильина, В. И. КИЯЕВ, Е. В. Трофимова ; под редакцией В. В. Трофимова. — Москва : Издательство Юрайт, 2021. — 238 с. — (Профессиональное образование). — ISBN 978-5-534-03964-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. https://urait.ru/bcode/469957

2. Петров, А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. — 2-е изд. — Саратов : Профобразование, 2019. — 446 с. — ISBN 978-5-4488-0091-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/87998.html

3. Информационные технологии в 2 т. Том 2 : учебник для среднего профессионального образования / В. В. Трофимов, О. П. Ильина, В. И. КИЯЕВ, Е. В. Трофимова ; под редакцией В. В. Трофимова. — Москва : Издательство Юрайт, 2021. — 390 с. — (Профессиональное образование). — ISBN 978-5-534-03966-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. https://urait.ru/bcode/469958

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

При освоении дисциплины использование ресурсов сети Интернет не предусмотрено.

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

Образовательный процесс по дисциплине **Информационная безопасность** предполагает использование следующего программного обеспечения и информационных справочных систем:
Windows 10
Microsoft Office
Microsoft Access 2016 (в составе пакета Ofiice)
1С Предприятие
Windows Server 2008
Microsoft SQL Server Express
My SQL Server
WPS Office
Dev C++
ABC Pascal
Android Studio
Симулятор сети передачи данных Cisco Packet Tracer
СДО Колледжа профессионального образования

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

Лекционная аудитория: проектор, экран, компьютер/ноутбук, меловая (и) или маркерная доска.
Аудитория для практических занятий и текущего контроля: лаборатория информационных ресурсов/ лаборатория вычислительной техники, архитектуры персонального компьютера и периферийных устройств. Оснащение согласно паспорту кабинета/ лаборатории.
Групповые (индивидуальные) консультации: меловая (и) или маркерная доска.
Аудитория для самостоятельной работы - помещения Научной библиотеки ПГНИУ: компьютерная техника с возможностью подключения к сети «Интернет», обеспеченная доступом в электронную информационно-образовательную среду университета.

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
Информационная безопасность

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

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОК.1 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	Знать и использовать способы решения задач защиты информации в профессиональной деятельности, применительно к различным контекстам	**Неудовлетворител** не знает основные средства и методы защиты компьютерных систем программными и аппаратными средствами; не умеет использовать методы защиты программного обеспечения компьютерных систем; не умеет анализировать риски и характеристики качества программного обеспечения; не умеет выбирать и использовать методы и средства защиты компьютерных систем программными и аппаратными средствами **Удовлетворительн** фрагментарно знает основные средства и методы защиты компьютерных систем программными и аппаратными средствами; частично умеет использовать методы защиты программного обеспечения компьютерных систем; допускает грубые ошибки в анализе рисков и характеристиках качества программного обеспечения. **Хорошо** в целом успешно, но с пробелами знает основные средства и методы защиты компьютерных систем программными и аппаратными средствами; с незначительными ошибками умеет использовать методы защиты программного обеспечения компьютерных систем; анализировать риски и характеристики качества программного обеспечения; выбирать и использовать методы и средства защиты компьютерных систем программными и аппаратными средствами **Отлично** знать основные средства и методы защиты компьютерных систем программными и

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично аппаратными средствами; уметь использовать методы защиты программного обеспечения компьютерных систем; анализировать риски и характеристики качества программного обеспечения; выбирать и использовать методы и средства защиты компьютерных систем программными и аппаратными средствами
ПК.4.4 Обеспечивать защиту программного обеспечения компьютерных систем программными средствами	Уметь защищать программное обеспечение компьютерных систем программными средствами	**Неудовлетворител** не знает основные средства и методы защиты компьютерных систем программными и аппаратными средствами; не умеет использовать методы защиты программного обеспечения компьютерных систем; не умеет анализировать риски и характеристики качества программного обеспечения; не умеет выбирать и использовать методы и средства защиты компьютерных систем программными и аппаратными средствами **Удовлетворительн** фрагментарно знает основные средства и методы защиты компьютерных систем программными и аппаратными средствами; частично умеет использовать методы защиты программного обеспечения компьютерных систем; допускает грубые ошибки в анализе рисков и характеристиках качества программного обеспечения. **Хорошо** в целом успешно, но с пробелами знает основные средства и методы защиты компьютерных систем программными и аппаратными средствами; с незначительными ошибками умеет использовать методы защиты программного обеспечения компьютерных систем; анализировать риски и характеристики качества программного обеспечения; выбирать и использовать методы и средства защиты компьютерных систем программными и аппаратными средствами **Отлично** знать основные средства и методы защиты

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично компьютерных систем программными и аппаратными средствами; уметь использовать методы защиты программного обеспечения компьютерных систем; анализировать риски и характеристики качества программного обеспечения; выбирать и использовать методы и средства защиты компьютерных систем программными и аппаратными средствами
ОК.2 Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	**Неудовлетворител** не знает анализ производительности и надежности, управление безопасностью; проблемы обеспечения технологической безопасности информационных систем; требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных; основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем методы устранения неисправностей в технических средствах; не умеет описывать концепции сетевой безопасности; описывать современные технологии и архитектуры безопасности **Удовлетворительн** фрагментарно знает анализ производительности и надежности, управление безопасностью; проблемы обеспечения технологической безопасности информационных систем; требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных; основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем методы устранения неисправностей в технических средствах; не

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительн умеет описывать концепции сетевой безопасности; описывать современные технологии и архитектуры безопасности **Хорошо** в целом знает анализ производительности и надежности, управление безопасностью; проблемы обеспечения технологической безопасности информационных систем; требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных; основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем методы устранения неисправностей в технических средствах, но допускает отдельные пробелы в знаниях; частично умеет описывать концепции сетевой безопасности; описывать современные технологии и архитектуры безопасности **Отлично** знать анализ производительности и надежности, управление безопасностью; проблемы обеспечения технологической безопасности информационных систем; требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных; основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем методы устранения неисправностей в технических средствах; уметь описывать концепции сетевой безопасности; описывать современные технологии и архитектуры безопасности
ОК.4	Работать в коллективе и	**Неудовлетворител**

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	команде, эффективно взаимодействовать с коллегами, руководством, клиентами	**Неудовлетворител** не знает требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных; не умеет описывать концепции сетевой безопасности; описывать современные технологии и архитектуры безопасности; не владеет навыками защиты сетевых устройств; внедрения механизмов сетевой безопасности на втором уровне модели OSI; внедрения механизмов сетевой безопасности с помощью межсетевых экранов **Удовлетворительн** фрагментарно знает требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных; частично умеет описывать концепции сетевой безопасности; описывать современные технологии и архитектуры безопасности; не владеет навыками защиты сетевых устройств; механизмов сетевой безопасности на втором уровне модели OSI; механизмов сетевой безопасности с помощью межсетевых экранов **Хорошо** сформированные, но содержащие отдельные пробелы знания требований к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативных методов повышения безопасности функционирования программных средств и баз данных; достаточно хорошо уметь описывать концепции сетевой безопасности; описывать современные технологии и архитектуры безопасности; владеть навыками защиты сетевых устройств; внедрять механизмы сетевой безопасности на втором уровне модели OSI; внедрять механизмы сетевой

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо безопасности с помощью межсетевых экранов **Отлично** знать требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных; уметь описывать концепции сетевой безопасности; описывать современные технологии и архитектуры безопасности; владеть навыками защиты сетевых устройств; внедрять механизмы сетевой безопасности на втором уровне модели OSI; внедрять механизмы сетевой безопасности с помощью межсетевых экранов
ОК.7 Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях, знать задачи управления безопасностью; основные проблемы обеспечения технологической безопасности информационных систем; основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем; оперативные методы повышения безопасности	**Неудовлетворител** не знает задачи управления безопасностью; основные проблемы обеспечения технологической безопасности информационных систем; основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем; оперативные методы повышения безопасности **Удовлетворительн** фрагментарно формулирует задачи управления безопасностью; основные проблемы обеспечения технологической безопасности информационных систем; основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем; не знает оперативные методы повышения безопасности **Хорошо** в целом успешное знание задач управления безопасностью; основных проблем обеспечения технологической безопасности информационных систем; основных требований к средствам и видам

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо тестирования для определения технологической безопасности информационных систем; оперативных методов повышения безопасности **Отлично** знает задачи управления безопасностью; основные проблемы обеспечения технологической безопасности информационных систем; основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем; оперативные методы повышения безопасности

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 44 до 60
«неудовлетворительно» / «незачтено» менее 44 балла

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
Входной контроль	Основные понятия и определения, эволюция подходов к обеспечению информационной безопасности. аспекты информационной безопасности **Входное тестирование**	Знания основных понятий

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОК.1 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам **ОК.2** Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	Угрозы безопасности АИС. Угрозы доступности, конфиденциальности, целостности информации **Защищаемое контрольное мероприятие**	знать:- назначение и место использования идентификации и аутентификации;- необходимость использования разграничения доступа;- особенности протоколирования информации и ее анализа. уметь: - управлять доступом к информации; - использовать стандартные средства безопасности ОС Windows; - использовать способы защиты информации от копирования.Основные защитные механизмы: идентификация и аутентификация, протоколирование и аудит. Разграничение доступа. Контроль целостности. Обнаружение и противодействие атакам. Защита от копирования информации.
ОК.1 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам **ОК.2** Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	Асимметричное шифрование. Электронно-цифровая подпись. **Защищаемое контрольное мероприятие**	знать:- группы криптосистем;- классификацию методов криптографического преобразования;- способы применения алгоритмов шифрования.уметь:- применять симметричные методы преобразования информации.- создавать программные продукты по защите информации.

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОК.1 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам **ОК.2** Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности **ОК.4** Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами **ПК.4.4** Обеспечивать защиту программного обеспечения компьютерных систем программными средствами **ОК.7** Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях	Модели информационной безопасности; международные и отечественные стандарты информационной безопасности, политика безопасности **Итоговое контрольное мероприятие**	Основы информационной безопасности Криптографические методы защиты информацииБезопасность операционных системПрограммно-аппаратные средства защиты информацииПравовое обеспечение информационной безопасности

Спецификация мероприятий текущего контроля

Основные понятия и определения, эволюция подходов к обеспечению информационной безопасности. аспекты информационной безопасности

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
Понятия информации, защиты данных, свойств информации, методы зашиты	10

Угрозы безопасности АИС. Угрозы доступности, конфиденциальности, целостности 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
классификация основных объектов защиты информации	8
определение этапов эволюции подходов к обеспечению информационной безопасности	8
полные формулировки основных понятий и определений информационной безопасности	8
определение целей и задач защиты информации	6

Асимметричное шифрование. Электронно-цифровая подпись.

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
Шифры. Виды шифрования. Использование шифров в шифровании	8
Криптография и криптосистемы.	8
Идентификация а аутентификация. Методы идентификации и аутентификации.. Хэш-функции	8
ЭЦП	6

Модели информационной безопасности; международные и отечественные стандарты информационной безопасности, политика безопасности

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **18**

Показатели оценивания	Баллы
Системы защиты государственной тайны и конфиденциальной информации.	10
Программно-аппаратные средства защиты информации	10
Криптографические методы защиты информации	10
Модели информационной безопасности	10