**МИНОБРНАУКИ РОССИИ**

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

**Кафедра радиоэлектроники и защиты информации**

Авторы-составители: **Лунегов Игорь Владимирович**
**Черепанов Иван Николаевич**

Рабочая программа дисциплины

# ОТКРЫТЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Код УМК 94117

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

Пермь, 2021

## 1. Наименование дисциплины

Открытые информационные системы

## 2. Место дисциплины в структуре образовательной программы

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

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

## 3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Открытые информационные системы** у обучающегося должны быть сформированы следующие компетенции:

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

**ОПК.12** Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем

**Индикаторы**

**ОПК.12.1** Организует диагностику и тестирование систем защиты информации автоматизированных систем

**ОПК.12.2** Проводит анализ уязвимостей систем защиты информации автоматизированных систем

**ПК.1** Способен использовать языки, системы, инструментальные, программные и аппаратные средства для моделирования информационных систем и испытаний систем защиты

**Индикаторы**

**ПК.1.1** Проводит моделирование безопасности информационных систем

**ПК.1.3** Анализирует эффективность решений по обеспечению информационной безопасности автоматизированных систем

**ПК.5** Способен анализировать уязвимости внедряемой системы защиты информации

**Индикаторы**

**ПК.5.1** Проводит анализ уязвимости программных и программно-аппаратных средств системы защиты информации автоматизированной системы

## 4. Объем и содержание дисциплины

| | |
|---|---|
| **Специальность** | 10.05.03 Информационная безопасность автоматизированных систем (направленность: Безопасность открытых информационных систем) |
| **форма обучения** | очная |
| **№№ триместров, выделенных для изучения дисциплины** | 10 |
| **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 лабораторных работ, занятий по иностранному языку** | 28 |
| **Самостоятельная работа (ак.час.)** | 88 |
| **Формы текущего контроля** | Входное тестирование (1)<br>Итоговое контрольное мероприятие (1)<br>Письменное контрольное мероприятие (2) |
| **Формы промежуточной аттестации** | Экзамен (10 триместр) |

## 5. Аннотированное описание содержания разделов и тем дисциплины

**«Открытые информационные системы»**

Курс посвящен изучению понятия открытых систем и методов стандартизации ИТ. На примере web технологий рассматриваются сосновые проблемы взаимодействия гетерогенных систем и пути их решения. Рассматриваются основных источники угроз информационной безопасности и способы борьбы с ними.

**Технологии открытых систем**

**Понятие открытых систем**

Рассматривается история вопроса. Приводятся предпосылки появления открытых систем, а также причины введения стандартов. Вводятся основные термины и понятия открытых систем

**Методологический базис открытых систем .**

Рассматривается международная структура в области стандартизации открытых систем. Приводятся организации по стандартизации различных уровней: Международные, промышленные, отраслевые. Так же рассматривается методологический базис открытых систем, основанный на системе стандартов

**Эталонная модель среды и взаимодействия открытых систем**

Вводится понятие эталонной модели открытых систем (OSE). Рассматривается структура данной модели. Обсуждаются состовные части эталонной модели, а также интерфейсы взаимодействия.

**Понятие профиля открытрытых систем**

Вводится понятие профиля открытых систем, а также обоснование необходимости применений профилей при разработке открытых систем. Вводится классификация профилей. Рассматривается типичная структура профиля на базе профиля ISP. Так же приводятся требования к содержанию профиля

**Сетевые технологии обработки данных. Основны компьютерной телекомуникации**

Рассматриваются история появления сетевых технологий, появление сети internet. Приводятся основые сэлементы технологии WWW: HTML, HTTP, URI, URL, DNS, CGI. Производится краткий обзор структуры вычислительных сетей, а также адресация сетей (IP-адреса). Также рассматривается клиет-серверная архитектура

**Сетевые сервиси и сетевые стандарты**

Распространение глобальных сетей позволило каждому пользователю иметь постоянное подключение к сети для общения с близкими или поиску нужной информации. За видимой простотой использования глобальных сетей сокрыты сложный стек технологий. В теме рассматриваются основные понятия глобальных сетей, а история развития сети internet, а также базовые концепции всемирной паутины и web технологии HTML, CSS, JavaScript.

**Понятие сетевых протоколов глобальных сетей**

Подробно рассматривается стек протокола TCP/IP. Приводятся основные протоколы обмена данными в сетях TCP/IP: Telnet, SSH, FTP, SMTP, DNS, RIP, SNMP, TCP, UDP,

**Информационные сервисы Internet,Адресация в компьютерных сетях .**

Рассматриваются основные сервисы Internet: электронная почта, поисковые системы, электронные библиотеки, форумы и тд. Подробно рассматривается структура адресации IP сетей, структура IP адреса, а также стандарты распределения адресов в сетях

**Язык гипертекстовой разметки HTML**

Рассматривается язык разметки HTML. Приводятся структура документа и основыне теги разметки. Также рассматривыются стандарты относящиеся к стуктурк веб-страниц

**Стандарты WWW**

Рассматриваются основные стандарты действующие в WWW. На базе исторических примеров рассматривается необходимость соблюдения как разработанных стандартов, так и стандартов дефакто.

## Концепции и аспекты обеспечения информационной безопасности

**Понятия экономической информационной безопасности**

Рассматривается история информационной безопасности. Приводятся основные понятия, а также основые нормативные документы по информационной безопасности в открытых системах

**Виды угроз информационной безопасности и класификация источников угроз**

Рассматриваются основные источники угроз информационной безопасности, вводится классификация данных угроз. Приовдятся основыне критиерии экономической безопасности

**Основные виды защиты информации**

Рассматриваются основные виды защиты информации, приводится классификация информации: Общедоступная, Для служебного пользования, Конфиденциальная, Персональная. Приводятся требования по информационной безопасности соответствующие различным типам информации

**Правовое обеспечение информационной безопасности**

Рассматривается законодательство различных стран в области информационной безопасности. Приводятся основные законы и нормативные акты по информационной безопасности.

**Основные аспекты построения систем информационной безопасности**

Рассматриваются вопросы ответственности и организационные меры в области обеспечения информационной безопасности, приводится программы информационной безопасности предприятий различного размера. Также рассматриваются основные этапы реализации программ информационной безопасности

**Определение защищенной информационной системы**

Рассматриваются способы определения защищенности информации. Приводятся основные критерии для определения надежности защиты информации

**Методология анализа защищенности информационной системы**

Рассматриваются основные подходы к анализу защищенности открытых систем. Приводятся различные модели и критерии анализа защищенности информационно системы

**Требования к архитектуре информационных систем для обеспечения безопасности ее функционирования**

Формируются основные требования к архитектуре информационных систем для обеспечения безопасности: гибкость, надежности, аргономичности и тд. Особенно важно показать необходимость поддержания документации в актуальном состоянии, так как это оказывает большое влияние на работу и безопасность системы. Также приводится ряд требований которые необходимо соблюдать как при разработке, так и при работе системы: непрерывность защиты в пространстве и времени, Усиление самого слабого звена, эшелонирование обороны и тд.

**Стандартизация подходов к обеспечению информационной безопасности**

Рассматривается структура стандартов в области информационной безопасности. Приводиться

основные нормативные документы, стандарты и требования в международной практике

**Технологии и инструменты обеспечения безопасности информации в системах и сетях**
Технологии и инструменты обеспечения безопасности информации в системах и сетях: технологии криптографической защиты информации,технологии нижнего уровня защиты информации в локальных сетях: межсетевые экраны, концепция защищенных виртуальных частных сетей, обеспечение интегральной безопасности информационных систем и сетей,Антивирусная защита

**Технологическая модель подсистемы информационной безопасности**
Ввиду большой сложной структуры современных информационных систем, включающих не только сложность в организационном плане, но и большой перечень гетерогенных систем, работающих в едино пространстве данных. Поэтому была создана технологическая модуль, которая позволяет разделить сложную систему на более просты части, объединяя наиболее общие ее части в единый уровень.

**Технологии криптографической защиты информации**
На примере базовых потребностей информационного обмена рассматриваются основные криптографические алгоритмы с прикладной точки зрения. Показывается способы аутентификации сторон при помощи асимметричных методов шифрования, и проверки подлинности документов. Рассматриваются основные способы атаки на шифрованные сообщения.

**Технологии нижнего уровня защиты информации в локальных сетях: межсетевые экраны**
Рассматривает нижний уровень защиты информационных сетей. На примере межсетевых экранов рассматриваются основные угрозы ИБ и способы разграничения сегментов сети.

**Концепция защищенных виртуальных частных сетей**
Рассматривается концепция виртуальных частных сетей. На примере исторических событий приводится рассматривается важность своевременной доставки защищенной информации. Сравнивается технология VPN с другими способами защищенной передачи информации. Приводится пример наиболее распространенных реализаций концентрации защищенных сетей.

**Антивирусная защита**
рассматриваются виды и классификация вредоносного ПО. Приводятся в пример основные классические вредоносный,  а также рассматриваются наиболее распространенные и опасные возможности современных вирусов. Так же приводятся основные способы обнаружения вирусов: эвристический анализ и базы вирусных сигнатур.

**Современные средства биометрической идентификации**
Приводится описание основных средств биометрической идентификации. Средства биометрической модификации основы на физиологических отличиях людей. При этом существуют как статические (отпечаток плаца, сетчатка глаза и пр.) так и динамические (голос, почерк ) признаки. Каждый их них имеет множество достоин и недостатков, которые не очевидны с первого взгляда.

**Обеспечение интегральной безопасности информационных систем и сетей**
На основании всего пройденного материала подводится итог о том, что подсистема информационной безопасности является много уровненной системой со множеством объектов. При этом обеспечение информационной безопасности предприятия на должном уровненные можно доиться только при интегральном подходе к данному вопроса. Необходимо не только привлекать к данному вопросы как высшее руководство предприятия, так и людей на местах, но так же проводить работу с персоналом для разъяснения положений информационной безопасности и периодически проводить аудит политики информационной 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. Антонов А. С. Технологии параллельного программирования MPI и OpenMP:[учебное пособие для вузов по направлениям 010400 "Прикладная математика и информатика", 010300 "Фундаментальная информатика и информационные технологии"]/А. С. Антонов.-Москва:Издательство Московского государственного университета,2012, ISBN 978-5-211-06343-3.-339.-Библиогр.: с. 333-334

2. Ясницкий Л. Н. Интеллектуальные информационные технологии и системы:учебно-методическое пособие/Л. Н. Ясницкий.-Пермь,2007, ISBN 5-7944-0997-5.-271.-Библиогр.: с. 260-267

3. Вальке, А. А. Электронные средства сбора и обработки информации : учебное пособие / А. А. Вальке, В. А. Захаренко. — Омск : Омский государственный технический университет, 2017. — 112 c. — ISBN 978-5-8149-2519-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/78495.html

**Дополнительная:**

1. Тузовский, А. Ф. Проектирование и разработка web-приложений : учебное пособие / А. Ф. Тузовский. — Томск : Томский политехнический университет, 2014. — 219 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/34702

2. Хаулет, Т. Защитные средства с открытыми исходными текстами. Практическое руководство по защитным приложениям : учебное пособие / Т. Хаулет ; перевод В. Галатенко, О. Труфанова ; под редакцией В. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 607 c. — ISBN 978-5-4497-0658-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/97544.html

3. Якубайтис Э. А. Открытые информационные сети/Э. А. Якубайтис.-Москва:Радио и связь,1991, ISBN 5-256-00823-4.-208.-Библиогр.: с. 193-197. - Предм. указ.: с. 204-206

## 9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

**https://falcongaze.ru/** Компания Falcongaze

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

Образовательный процесс по дисциплине **Открытые информационные системы** предполагает использование следующего программного обеспечения и информационных справочных систем:
Образовательный процесс по дисциплине предполагает использование следующего информационных технологий, программного обеспечения и информационных справочных систем:
- презентационные материалы (слайды по темам лекционных и практических занятий);
- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательной среду университета (ЕТИС ПГНИУ);
- интернет-сервисы и электронные ресурсы (поисковые системы, электронная почта, профессиональные тематические чаты и форумы, системы аудио и видео конференций, онлайн энциклопедии и т.д.).
Перечень используемого программного обеспечения:
- открытая система "ALT Linux"
- офисный пакет приложений "Libre office";
- приложение позволяющее просматривать и воспроизводить медиа контент PDF-файлов "Adobe Acrobat Reader DC";
- программы демонстрации видео материалов (проигрыватель) "Windows Media Plaer";
- программа просмотра интернет контента (браузер) "Google Chrome
- технологии реляционных баз данных (SQLite),
-веб-технологии (html, css, javascript),
-сетевой обмен данными по средствам стека протоколов TCP/IP

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

Для проведения лекционных и лабораторных занятий требуется наличие компьютерного класса с доступом к сети интернет, и предустановленным программным обеспечением, включающим в себя интерпретатор языка Python, среду разработки, а также пакетный менеджер pip

Аудитория для самостоятельной работы: компьютерный класс кафедры, помещения Научной библиотеки ПГНИУ, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет», обеспеченные 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**
**Открытые информационные системы**

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

**ОПК.12**

**Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем**

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|---|---|
| **ОПК.12.1** Организует диагностику и тестирование систем защиты информации автоматизированных систем | Организует диагностику и тестирование систем защиты информации автоматизированных систем | **Неудовлетворител** Отсутствие знаний по проектированию, эксплуатации и совершенствования системы управления информационной безопасностью открытой информационной системы. **Удовлетворительн** Общие, но не структурированные знания по проектированию, эксплуатации и совершенствования системы управления информационной безопасностью открытой информационной системы. **Хорошо** Сформированные, но содержащие отдельные пробелы знания по проектированию, эксплуатации и совершенствования системы управления информационной безопасностью открытой информационной системы. **Отлично** Сформированные систематические знания по проектированию, эксплуатации и совершенствования системы управления информационной безопасностью открытой информационной системы. |
| **ОПК.12.2** Проводит анализ уязвимостей систем защиты информации автоматизированных систем | Проводит анализ уязвимостей систем защиты информации автоматизированных систем | **Неудовлетворител** Отсутствие знаний и навыков по организации и проведению контроля обеспечения информационной безопасности открытой информационной системы. **Удовлетворительн** Общие, но не структурированные знания и навыки по организации и проведению контроля обеспечения информационной безопасности открытой информационной системы. **Хорошо** |

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|---|---|
| | | **Хорошо**<br>Сформированные, но содержащие отдельные пробелы знания и навыки по организации и проведению контроля обеспечения информационной безопасности открытой информационной систе<br>**Отлично**<br>Сформированные систематические знания и навыки по организации и проведению контроля обеспечения информационной безопасности открытой информационной системы. |

**ПК.1**

**Способен использовать языки, системы, инструментальные, программные и аппаратные средства для моделирования информационных систем и испытаний систем защиты**

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|---|---|
| **ПК.1.1**<br>Проводит моделирование безопасности информационных систем | Проводит моделирование безопасности информационных систем | **Неудовлетворител**<br>Отсутствие знаний и навыков по организации и проведению аудита обеспечения информационной безопасности открытой информационной системы.<br>**Удовлетворительн**<br>Общие, но не структурированные знаний и навыков по организации и проведению аудита обеспечения информационной безопасности открытой информационной системы.<br>**Хорошо**<br>Сформированные, но содержащие отдельные пробелы знания и навыки по организации и проведению аудита обеспечения информационной безопасности открытой информационной системы.<br>**Отлично**<br>Сформированные систематические знания и навыки по организации и проведению аудита обеспечения информационной безопасности открытой информационной системы. |
| **ПК.1.3**<br>Анализирует эффективность решений по обеспечению | Анализирует эффективность решений по обеспечению информационной безопасности автоматизированных систем | **Неудовлетворител**<br>Отсутствие знаний базовых моделей открытых систем ( модели OSE/RM OSI) и современных стандартов по обеспечению информационной безопасности |

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|---|---|
| информационной безопасности автоматизированных систем | | **Удовлетворительн**<br>Общие, но не структурированные знания базовых моделей открытых систем ( модели OSE/RM OSI) и современных стандартов по обеспечению информационной безопасности<br>**Хорошо**<br>Сформированные, но содержащие отдельные пробелы знания базовых моделей открытых систем ( модели OSE/RM OSI) и современных стандартов по обеспечению информационной безопасности<br>**Отлично**<br>Сформированные систематические знания базовых моделей открытых систем ( модели OSE/RM OSI) и современных стандартов по обеспечению информационной безопасности |

**ПК.5**

**Способен анализировать уязвимости внедряемой системы защиты информации**

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|---|---|
| **ПК.5.1**<br>Проводит анализ уязвимости программных и программно-аппаратных средств системы защиты информации автоматизированной системы | Проводит анализ уязвимости программных и программно-аппаратных средств системы защиты информации автоматизированной системы | **Неудовлетворител**<br>Отсутствие знаний и навыков по стандартным моделям построения защищённых информационных систем.<br>**Удовлетворительн**<br>Общие, но не структурированные знания по стандартным моделям построения защищённых информационных систем.<br>**Хорошо**<br>Сформированные, но содержащие отдельные пробелы знания по стандартным моделям построения защищённых информационных систем.<br>**Отлично**<br>Сформированные систематические знания по стандартным моделям построения защищённых информационных систем. |

## 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 (индикатор) | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|---|---|---|
| **Входной контроль** | Понятие открытых систем<br>**Входное тестирование** | проверяются базовые знания архитектуры современных ЭВМ, а также навыки программирования. |
| **ПК.1.3**<br>Анализирует эффективность решений по обеспечению информационной безопасности автоматизированных систем<br>**ОПК.12.1**<br>Организует диагностику и тестирование систем защиты информации автоматизированных систем | контрольная работа<br>**Письменное контрольное мероприятие** | Знание методов разработки компонентов открытых информационных систем, структуры стандартизации в области информационных технологий. А также знание базовых моделей среды открытых систем и взаимосвязи открытых систем |
| **ПК.5.1**<br>Проводит анализ уязвимости программных и программно-аппаратных средств системы защиты информации автоматизированной системы<br>**ОПК.12.2**<br>Проводит анализ уязвимостей систем защиты информации автоматизированных систем | Современные средства биометрической идентификации<br>**Письменное контрольное мероприятие** | Умение проводить оценку защищенности информационной системы. Знание основных типов защищаемой информации и источников угроз информационной безопасности |

| Компетенция (индикатор) | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|---|---|---|
| **ПК.1.1** Проводит моделирование безопасности информационных систем | Обеспечение интегральной безопасности информационных систем и сетей **Итоговое контрольное мероприятие** | Знание основной идеи открытых систем, а также структуры стандартизации в области ИТ. Владение базовыми эталонными моделями среды и взаимосвязи открытых систем. Понимание основных принципов формирования политик безопасности в система построенных по открытом принципу |

## Спецификация мероприятий текущего контроля

### Понятие открытых систем

Продолжительность проведения мероприятия промежуточной аттестации: **.5 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **0**
Проходной балл: **0**

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

### контрольная работа

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 сетевых стандартов | 10 |
| знание сетевые технологии обработки данных | 10 |
| знание понятие профиля открытых систем | 5 |
| знание методологического базис открытых систем | 5 |

### Современные средства биометрической идентификации

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 видов угроз информационной безопасности | 10 |
| знание методологии анализа защищенности информационной системы | 10 |
| умение применять технологии и инструменты обеспечения безопасности информации в системах и сетях | 5 |
| знание основ экономической информационной безопасности | 5 |

**Обеспечение интегральной безопасности информационных систем и сетей**

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **17**

| Показатели оценивания | Баллы |
|---|---|
| знание методов обеспечение интегральной безопасности информационных систем и сетей | 10 |
| обладание навыком оценки рисков | 10 |
| обладание навыком классификации угроз | 10 |
| Знание структуры международной стандартизации | 10 |