МИНОБРНАУКИ РОССИИ

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

Кафедра радиоэлектроники и защиты информации

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

Рабочая программа дисциплины

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОТКРЫТЫХ СИСТЕМ

Код УМК 81659

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

Пермь, 2021

1. Наименование дисциплины

Информационная безопасность открытых систем

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 **Информационная безопасность открытых систем** у обучающегося должны быть сформированы следующие компетенции:

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

ОПК.7 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации

Индикаторы

ОПК.7.2 Применяет методы и средства защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки по техническим каналам, сетей и систем передачи информации при решении профессиональных задач, учитывая текущее состояние и тенденции развития методов и средств обеспечения защиты информации

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.1.3 Анализирует эффективность решений по обеспечению информационной безопасности автоматизированных систем

ОПСК.3 Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах

Индикаторы

ОПСК.3.1 Обнаруживает и устраняет нарушения правил разграничения доступа в автоматизированных системах

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	13
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	Входное тестирование (1) Защищаемое контрольное мероприятие (2) Итоговое контрольное мероприятие (1)
Формы промежуточной аттестации	Экзамен (13 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Информационная безопасность открытых систем. Первый семестр

часть1

Основные элементы открытых систем

Рассматриваются основные принципы открытых систем. На примере истории развития вычислительных технологий обосновываются главыне положения концепции открытых систем

Основные модели открытых систем

Изучаются базовые модели концепции открытых систем. Рассматривается базовая модель взаимодействия OSE/RM и базовая модель OSI/RM

Угрозы ресурсам и причины их реализации

совокупность условий и факторов, создающих опасность нарушения информационной безопасности.[1]

Под угрозой (в общем) понимается потенциально возможное событие, действие (воздействие), процесс или явление, которые могут привести к нанесению ущерба чьим-либо интересам.

Под угрозой интересам субъектов информационных отношений понимают потенциально возможное событие, процесс или явление которое посредством воздействия на информацию или другие компоненты информационной системы может прямо или косвенно привести к нанесению ущерба интересам данных субъектов. [2]

Уязвимости архитектуры клиент-сервер

Клиент-сервер (англ. Client-server) — вычислительная или сетевая архитектура, в которой задания или сетевая нагрузка распределены между поставщиками услуг, называемыми серверами, и заказчиками услуг, называемыми клиентами. Фактически клиент и сервер — это программное обеспечение. Обычно эти программы расположены на разных вычислительных машинах и взаимодействуют между собой через компьютерную сеть посредством сетевых протоколов, но их можно расположить также и на одной машине. Программы — сервера, ожидают от клиентских программ запросы и предоставляют им свои ресурсы в виде данных (например, загрузка файлов посредством HTTP, FTP, BitTorrent, потоковое мультимедиа или работа с базами данных) или сервисных функций (например, работа с электронной почтой, общение посредством систем мгновенного обмена сообщениями, просмотр web-страниц во всемирной паутине). Поскольку одна программа-сервер может выполнять запросы от множества программ-клиентов, ей может потребоваться высокопроизводительная вычислительная машина. Из-за особой роли этой машины в сети, специфики её оборудования и программного обеспечения её так же называют сервером.

Социальная инженерия

Социальная инженерия – метод получения необходимого доступа к информации, основанный на особенностях психологии людей. Основной целью социальной инженерии является получение доступа к конфиденциальной информации, паролям, банковским данным и другим защищенным системам.

Интернет как открытая система

Интернет всемирная система объединённых компьютерных сетей для хранения и передачи информации. Часто упоминается как Всемирная сеть и Глобальная сеть, а также просто Сеть. Построена на базе стека протоколов TCP/IP. На основе Интернета работает Всемирная паутина (World Wide Web, WWW) и множество других систем передачи данных.

Протокол HTTP

HTTP (англ. HyperText Transfer Protocol — «протокол передачи гипертекста») — протокол прикладного уровня передачи данных (изначально — в виде гипертекстовых документов в формате «HTML», в настоящий момент используется для передачи произвольных данных). Основой HTTP является технология «клиент-сервер»,

web-серверы

Веб-сервер — сервер, принимающий HTTP-запросы от клиентов, обычно веб-браузеров, и выдающий им HTTP-ответы, как правило, вместе с HTML-страницей, изображением, файлом, медиа-потоком или другими данными.

Веб-сервером называют как программное обеспечение, выполняющее функции веб-сервера, так и непосредственно компьютер (см.: Сервер (аппаратное обеспечение)), на котором это программное обеспечение работает.

Клиент, которым обычно является веб-браузер, передаёт веб-серверу запросы на получение ресурсов, обозначенных URL-адресами. Ресурсы — это HTML-страницы, изображения, файлы, медиа-потоки или другие данные, которые необходимы клиенту. В ответ веб-сервер передаёт клиенту запрошенные данные. Этот обмен происходит по протоколу HTTP.

Настройка виртуальной машиныы

Настройка виртуальной машины и программного обеспечения для проведения практических занятий

Часть 2

Аудит открытых систем

При планировании атаки на сервер производится анализ объекта атаки. Методика blacbox -- подразумевает проведение атаки с нулевой начальной информацией о цели, то есть без доступа к настройке структуре и исходных кодов. Первично производится сбор данных о цели. как правило для атаки есть точка входа. Например сайт, сервер, IP в сети. при этом на самой цели уязвимость может и не быть, однако уязвимыми могут оказаться соседние объекты, через которые можно провести атаку. Первичны анализ является довольно творческим процессом. Каждая цель анализируется с чистого листа.

Основные методы атаки серверов

Атака на веб приложение направлена на вяление нештатного поведения системы. В идеален выполнение действий необходимых атакующему Атака может производится

POST/ GET Параметры. Необходим проводит проверку данных присылаемых пользователем. Кроме того разработчики иногда игнорируют проверку скрытых полей, считая что пользователь не может изменить их значения Однако необходимо помнить, что злоумышленник может пользоваться дополнительными средствами, а не только просматривать нашу в страницу в браузере.

Загружаемые файлы. Злоумышленник может воспользоваться данной функцией для достижения своих целей. Существует несколько векторов атаки.

Тип файла,
имя файла,
атака обработчика.

Атака типом файла может быть реализована следующим образом. Например у нас есть форум написанный на PHP который позволяет заливать фотографии пользователям. Если не проводится ни

какой проверки файла, то злоумышленник может загрузить на форму PHP фаил, который при отображении исполнится на стороне сервера

На имя файла также можно поместить некоторые данные. Например в имя файла можно поместить спец символы, которые повлияют на работу целевой системы

Атак на обработчик. Данные на стороне сервера как то разбираются и злоумышленник должен построить архитектуру серверного обработчик для проведение атаки.

Уязвимости на стороне пользователя

Рассмотрим уязвимости серверной части. С появлением языков выполняемых на стороне пользователя появились пользовательские уязвимости. Они как правило направлены на кражу данных со стороны клиента В данном случае злоумышленник использует факты работы серверной системы атакует пользователя. целью атаки является

Браузер
Местоположения пользователя.
открытые сессии. Использование открыт сессий с авторизованных сайтов
Пользователь. Попытаться заставить пользователя выполнить какие либо действия

Атаки на протоколы

Атакам может подвергаться не только сам сервер или клиентская сторона но и протоколы передачи данных. Атаки могут быть на направленны на протокол HTTP и DNS

Архитектурные уязвимости

Архитектурные уязвимости как правило закладываются на этапе проектирования и разработки технического задания. То есть фактически это не уязвимость а логика работы системы.

Уязвимости сетевого уровня

Рассмотрим, что доступно злоумышленнику находясь на сетевом уровне.

Передача данных в сети происходит по протоколу IP. Злоумышленник может влиять на заголовки пакета для провокации той или иной уязвимости.

Для анализа трафика можно использовать утилиту Wiresharp.

Аудит кода

Аудит кода представляет собой проверку программного кода по различным критериям в зависимости от нужд конкретного заказчика. Данная процедура направленна на выявление программных закладок, ошибок, уязвимых мест, на предмет безопасности, оптимизированности, соответствия законодательным актам, исходному техническому заданию.

Пост эксплуатация уязвимостей

Рассмотрим какие действия выполняются после получения доступа к системе.

как правило после получения доступа злоумышленник предпринимает следующие действия:
получение расширенного доступа
кража данных данные
получение перманентный доступ

Во первых это получение расширенного доступа к системе. Возможно создание более удобного интереса управление сервера.
Далее происходит изучение данных которых хранятся на системе, а так же анализ окружения.
Последним но не менее важным является получение скрытого перманентного доступа к системе. что позволит совершать дальнейшую эксплуатацию сервера.

Итоговое контрольное мероприятие

Проведение итогового контрольного мероприятия по всему курсу. Экзамен проводится в письменной форме. Билет содержит 2 вопроса. Проверяется глубина знаний вопросам билета, а также задаются дополнительные вопросы на общее понимание аспектов компьютерной безопасности, и умение проводить аудит открытых системы.

Вопросы к экзамену:

Основные модели открытых системам
Угрозы ресурсам и причины их реализации
Уязвимость архитектуры клиент-сервер
Социальная инженерия
Интернет/ Интранет
Протокол HTTP
web- серверы
Анализ системы(blackbox - аудит)
Методы атаки
Уязвимости на стороне пользователя
уязвимости на стороне сервера
Концепция AAA
Парольные политики
Уязвимости сетевого уровня
CMS
Пост-эксплуатация уязвимостей

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. Голиков, А. М. Основы проектирования защищенных телекоммуникационных систем : учебное пособие для специалитета: 10.05.02 Информационная безопасность телекоммуникационных систем. Курс лекций, компьютерный практикум, компьютерные лабораторные работы и задание на самостоятельную работу / А. М. Голиков. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2016. — 396 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/72158.html

2. Журавлева, Т. Ю. Информационные технологии : учебное пособие / Т. Ю. Журавлева. — Саратов : Вузовское образование, 2018. — 72 c. — ISBN 978-5-4487-0218-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/74552.html

3. Технология открытых систем/под общ. ред. А. Я. Олейникова.-М.:Янус-К,2004, ISBN 5-8037-0203-X.-288.-Библиогр. в конце глав

4. Безопасность ИТ:[Криптографические основы безопасности. Основы информационной безопасности. Протоколы безопасного сетевого взаимодействия. Стандарты информационной безопасности]/Интернет-Университет информационных технологий.-Москва:Новый диск,2006.-1.

Дополнительная:

1. Лещев Д. В. Создание интерактивного web-сайта:Учеб. курс/Д. В. Лещев.-СПб.:Питер,2003, ISBN 5-314-00033-4.-544.

2. 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

3. Якубайтис Э. А. Архитектура открытых систем/Э. А. Якубайтис.-Рига,1979.-59.-Библиогр.: с. 58

4. Сычев Ю. Н. Основы информационной безопасности: учебно-практическое пособие / Ю. Н. Сычев. — М.: Изд. цент ЕАОИ, 2010. — 328 с. — ISBN 978-5-374-00381-9. — Текст : электронный // Электронно-библиотечная система БиблиоТех : [сайт]. https://bibliotech.psu.ru/Reader/Book/7723

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 **Информационная безопасность открытых систем** 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
Дополнительно в рамках курса будут применяться 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

Лекционные занятия, групповые (индивидуальные) консультации, мероприятия текущего контроля и промежуточной аттестации проводятся в аудитории, оснащенной презентационной техникой (проектор, экран для проектора, компьютер/ноутбук), а также меловой (и) или маркерной доской

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

Аудитория для самостоятельной работы: компьютерный класс кафедры радиоэлектроники и защиты информации с возможностью запуска виртуальной машины с операционной системой GNU/Linux и помещения библиотеки с персональными компьютерами с доступом к локальной и глобальной сетям ,

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:

1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютера с доступом к локальной и глобальной компьютерным сетям.
2. Читальный зал гуманитарной литературы, корп. 2, ауд. 418. Оборудован 7 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
3. Читальный зал естественной литературы, корп.6, ауд. 107а. Оборудован 5 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
4. Отдел иностранной литературы, корп.2 ауд. 207. Оборудован 1 персональным компьютером с доступом к локальной и глобальной компьютерным сетям.
5. Библиотека юридического факультета, корп.9, ауд. 4. Оборудована 11 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
6. Читальный зал географического факультета, корп.8, ауд. 419. Оборудован 6 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

Все компьютеры, установленные в помещениях научной библиотеки, оснащены следующим программным обеспечением:

Операционная система ALT Linux;

Офисный пакет Libreoffice.

Справочно-правовая система «КонсультантПлюс»

Фонды оценочных средств для аттестации по дисциплине
Информационная безопасность открытых систем

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	Знать методики по тестированию и диагностике защищенных автоматизированных систем	**Неудовлетворител** Отсутствие знаний по тестированию и диагностике защищенных автоматизированных систем **Удовлетворительн** Общие, но не структурированные знания по тестированию и диагностике защищенных автоматизированных систем **Хорошо** Сформированные, но содержащие отдельные пробелы знания по тестированию и диагностике защищенных автоматизированных систем **Отлично** Сформированные систематические знания по тестированию и диагностике защищенных автоматизированных систем
ОПК.12.2 Проводит анализ уязвимостей систем защиты информации автоматизированных систем	Знать критерии оценки и классификации уязвимостей информационных систем Уметь проводить анализ уровня эффективности применения автоматизированных систем Владеть навыками работы с соответствующим программным обеспечением	**Неудовлетворител** Не знает критерии оценки и классификации уязвимостей информационных систем Не умеет проводить анализ уровня эффективности применения автоматизированных систем Не владеет навыками работы с соответствующим программным обеспечением **Удовлетворительн** Частично сформированные знание критерии оценки и классификации уязвимостей информационных систем. Частично сформированные умение проводить анализ уровня эффективности применения автоматизированных систем. Посредственное владение навыками работы

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительн с соответствующим программным обеспечением **Хорошо** Сформированные, но содержащие пробелы знание критерии оценки и классификации уязвимостей информационных систем. Сформированные, но содержащие пробелы умение проводить анализ уровня эффективности применения автоматизированных систем. Неуверенное владение навыками работы с соответствующим программным обеспечением **Отлично** Сформированные знание критерии оценки и классификации уязвимостей информационных систем. Сформированные умение проводить анализ уровня эффективности применения автоматизированных систем. Уверенное владение навыками работы с соответствующим программным обеспечением

ОПК.7

Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.7.2 Применяет методы и средства защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки по техническим	Знать средства защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки	**Неудовлетворител** Отсутствие знаний средства защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки **Удовлетворительн** Общие, но не структурированные знания в области средств защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
каналам, сетей и систем передачи информации при решении профессиональных задач, учитывая текущее состояние и тенденции развития методов и средств обеспечения защиты информации		**Удовлетворительн** информации от утечки **Хорошо** Сформированные, но содержащие отдельные пробелы в области средств защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки **Отлично** Сформированные систематические знания средств защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки

ОПСК.3

Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПСК.3.1 Обнаруживает и устраняет нарушения правил разграничения доступа в автоматизированных системах	Знать правила составления политик безопасности и разграничения прав доступа	**Неудовлетворител** Отсутствие знаний правил составления политик безопасности и разграничения прав доступа **Удовлетворительн** Общие, не структурированные знания правил составления политик безопасности и разграничения прав доступа, Отсутствие знаний по методикам выявления нарушений **Хорошо** Сформированные, но содержащие отдельные пробелы знания правил составления политик безопасности и разграничения прав доступа, и методик выявления нарушений **Отлично** Сформированные систематические знания правил составления политик безопасности и разграничения прав доступа, и методик выявления нарушений

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.1.3 Анализирует эффективность решений по обеспечению информационной безопасности автоматизированных систем	Знание методик анализа эффективность решений по обеспечению информационной безопасности автоматизированных систем	**Неудовлетворител** Отсутствие знаний по методикам анализа эффективность решений по обеспечению информационной безопасности автоматизированных систем **Удовлетворительн** Общие, но не структурированные знания методик анализа эффективность решений по обеспечению информационной безопасности автоматизированных систем **Хорошо** Сформированные, но содержащие отдельные пробелы знания методик анализа эффективность решений по обеспечению информационной безопасности автоматизированных систем **Отлично** Сформированные систематические знания методик анализа эффективность решений по обеспечению информационной безопасности автоматизированных 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 50 до 60
«неудовлетворительно» / «незачтено» менее 50 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
Входной контроль	Основные элементы открытых систем **Входное тестирование**	Входной уровень знаний
ОПСК.3.1 Обнаруживает и устраняет нарушения правил разграничения доступа в автоматизированных системах **ОПК.12.1** Организует диагностику и тестирование систем защиты информации автоматизированных систем	Контрольная работа **Защищаемое контрольное мероприятие**	Знание основных угроз и уязвимостей в современных открытх системах. Понимание принципов работы протокола HTTP и веб приложений. Знание базовых понятий web-технологий
ОПК.12.1 Организует диагностику и тестирование систем защиты информации автоматизированных систем	Контрольная работа **Защищаемое контрольное мероприятие**	Знание способов проведения аудита безопастности открытых систем. Умение проводит анализ защищенности система, и проверку системы на наличие уязвимостей. Знание принципов построения атаки на сервер, и способов пост эксплуетации уязвимостей

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.1.3 Анализирует эффективность решений по обеспечению информационной безопасности автоматизированных систем **ОПК.7.2** Применяет методы и средства защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки по техническим каналам, сетей и систем передачи информации при решении профессиональных задач, учитывая текущее состояние и тенденции развития методов и средств обеспечения защиты информации **ОПК.12.2** Проводит анализ уязвимостей систем защиты информации автоматизированных систем	Итоговое контрольное мероприятие **Итоговое контрольное мероприятие**	способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы, способность проводить анализ рисков информационной безопасности автоматизированной системы способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем, способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности, способность разрабатывать политики информационной безопасности автоматизированных систем способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы, способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы

Спецификация мероприятий текущего контроля

Основные элементы открытых систем

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **0**
Проходной балл: **0**

Показатели оценивания	Баллы
Владение базовыми этолонными моделями среды открытых систем и взаимосвязи открытых систем	34
Знание основных положений открытых системы, а также структуры международной стандартизации	33
Знание основных протоколов передачи данных.	33

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 протокола HTTP и web-технологий	10
Знание структуры международной стандартизации	10
умение работать с виртуальной машиной Linux	5
знание основных угроз информационным ресурсам	5

Контрольная работа

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

Показатели оценивания	Баллы
Умение выявлять архитектурные уязвимости	10
Знание методов аудита открытых систем	10
Умение проводит аудит кода	5
Знание основных атак на архитектуру клиент сервер	5

Итоговое контрольное мероприятие

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **20**

Показатели оценивания	Баллы
Знание основных элементов открытых систем	10
знание методов пост эксплуатации уязвимость	10
умение проводить аудит кода	10
умение определять угрозы информационной безопасности	10