

МИНОБРНАУКИ РОССИИ

**Федеральное государственное бюджетное 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 2020 г.

Пермь, 2020

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
специализация 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 (специализация : Безопасность открытых информационных систем)

ПК.10 способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности

ПК.11 способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности

ПК.12 способность разрабатывать политики информационной безопасности автоматизированных систем

ПК.13 способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы

ПК.14 способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы

ПК.15 способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации

ПК.18 способность проводить инструментальный мониторинг защищенности автоматизированных систем

ПК.23 способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности

ПК.30 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы

ПК.31 способность управлять информационной безопасностью автоматизированной системы

ПК.32 способность обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций

ПК.5 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы

ПК.6 способность проводить анализ рисков информационной безопасности автоматизированной системы

ПК.7 способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем

ПК.9 способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем

ПСК.1.1 способность на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем

ПСК.1.2 способность разрабатывать и реализовывать политики информационной безопасности открытых информационных систем

ПСК.1.3 способность участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы

ПСК.1.4 способность участвовать в организации и проведении контроля обеспечения информационной безопасности открытой информационной системы

ПСК.1.5 способность формировать и эффективно применять комплекс мер (правила, процедуры,

практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем

4. Объем и содержание дисциплины

| | |
|---|--|
| Направления подготовки | 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 (1) Итоговое контрольное мероприятие (1) Письменное 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 главные 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-поток 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-поток или другие данные, которые необходимы клиенту. В ответ веб-сервер передаёт клиенту запрошенные данные. Этот обмен происходит по протоколу HTTP.

Настройка виртуальной машины

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 blsbox -- 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. Первичный анализ является довольно творческим процессом. Каждая цель анализируется с чистого листа.

Основные методы атаки серверов

Атака на веб приложение направлена на выявление нештатного поведения системы. В идеале выполнение действий необходимых атакующему. Атака может производиться

POST/ GET Параметры. Необходимо проводить 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 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 файл, 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 направлена 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 с. — 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.-М.: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://psu.bibliotech.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-образовательную среду университета (ЕТИС ПГНИУ);
- интернет-сервисы и электронные ресурсы (поисковые системы, электронная почта, профессиональные тематические чаты и форумы, системы аудио и видео конференций, онлайн энциклопедии и т.д.).

Перечень используемого программного обеспечения:

- открытая система "ALT Linux"
- офисный пакет приложений "Libre office";
- приложение позволяющее просматривать и воспроизводить медиа контент PDF-файлов "Adobe Acrobat Reader DC";
- программы демонстрации видео материалов (проигрыватель) "Windows Media Player";
- 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 в 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**

ПК.30

способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|--|---|
| ПК.30 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы | Знать политик информационной безопасности автоматизированной системы Уметь осуществлять мониторинг безопасности автоматизированной системы Владеть навыками работы со специальным программным обеспечением | Неудовлетворител Отсутствие знаний политик информационной безопасности автоматизированной системы Отсутствие умений работы с политикой безопасности Удовлетворительн Общие, но не структурированные знания основ информационной безопасности, знает основные понятия и терминологию, Хорошо Сформированные, но содержащие отдельные пробелы знания основ информационной безопасности, определение основных угроз информационной системе, терминологию и основные понятия. Отлично Сформированные систематические знания методов анализа и мониторинга безопасности автоматизированной системы, знает терминологию и основные понятия используемые в теории и практике информационной безопасности |

ПК.32

способность обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|---|--|
| ПК.32 способность обеспечить восстановление работоспособности | Знать методы мониторинга систем информационной безопасности Уметь обеспечить | Неудовлетворител Отсутствие знаний функционирования открытых систем Отсутствие умений восстановления |

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|--|---|
| систем защиты информации при возникновении нештатных ситуаций | восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций Владеть навыками анализа причин сбоя | <p>Неудовлетворител работоспособности систем при возникновении нештатных ситуаций Отсутствие навыков определение неполадок и возникновения нештатных ситуаций</p> <p>Удовлетворительн Общие, но не структурированные знания основ функционирования и взаимодействия открытых систем. Частично сформированное умение по восстановлению работоспособности систем защиты информации при возникновении нештатных ситуаций.</p> <p>Хорошо Сформированные, но содержащие отдельные пробелы знания основ функционирования и взаимодействия открытых систем, В целом успешные, но содержащие отдельные пробелы умение по восстановлению работоспособности систем защиты информации при возникновении нештатных ситуаций.</p> <p>Отлично Сформированные систематические знания основ функционирования и взаимодействия открытых систем. Сформированное умение по восстановлению работоспособности систем защиты информации при возникновении нештатных ситуаций.</p> |

ПК.7

способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|--|---|
| ПК.7 способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности | Знать критерии оценки и классификации уязвимостей информационных систем Уметь проводить анализ уровня эффективности применения автоматизированных систем Владеть навыками работы с соответствующим | <p>Неудовлетворител Отсутствие знаний политик информационной безопасности автоматизированной системы Отсутствие умений проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения</p> |

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|--|--|---|
| применения автоматизированных систем | программным обеспечением | <p>Неудовлетворител автоматизированных систем</p> <p>Удовлетворительн Общие, но не структурированные знания способов проведения анализ и выбора решений по обеспечению требуемого уровня эффективности применения автоматизированных систем</p> <p>Хорошо Сформированные, но содержащие отдельные пробелы знания способов проведения анализ и выбора решений по обеспечению требуемого уровня эффективности применения автоматизированных систем</p> <p>Отлично Сформированные систематические знания способов проведения анализ и выбора решений по обеспечению требуемого уровня эффективности применения автоматизированных систем</p> |

ПК.6

способность проводить анализ рисков информационной безопасности автоматизированной системы

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|--|--|--|
| ПК.6 способность проводить анализ рисков информационной безопасности автоматизированной системы | Знать критерии оценки рисков информационной безопасности Уметь проводить анализ рисков информационной безопасности автоматизированной системы Владеть методами анализа информационной безопасности | <p>Неудовлетворител Отсутствие знаний политик информационной безопасности автоматизированной системы Отсутствие умений проводить анализ рисков информационной безопасности автоматизированной системы</p> <p>Удовлетворительн Общие, но не структурированные знания основ информационной безопасности, способность проводить анализ рисков информационной безопасности автоматизированной системы</p> <p>Хорошо Сформированные, но содержащие отдельные пробелы знания способов анализа рисков информационной безопасности автоматизированной системы</p> |

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|----------------------------|------------------------------------|--|
| | | Отлично Сформированные систематические знания способов анализа рисков информационной безопасности автоматизированной системы |

ПК.18

способность проводить инструментальный мониторинг защищенности автоматизированных систем

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|---|---|
| ПК.18 способность проводить инструментальный мониторинг защищенности автоматизированных систем | Знать способы мониторинга защищенности автоматизированных систем Уметь проводить инструментальный мониторинг защищенности автоматизированных систем Владеть специализированным ПО для проведения мониторинга защищенности автоматизированных систем | Неудовлетворител Отсутствие знаний инструментов мониторинга защищенности автоматизированных систем Удовлетворительн Общие, но не структурированные знания инструментов мониторинга защищенности автоматизированных систем Хорошо Сформированные, но содержащие отдельные пробелы знания инструментов мониторинга защищенности автоматизированных систем Отлично Сформированные систематические знания методов анализа и мониторинга безопасности автоматизированной системы, знает терминологию и основные понятия используемые в теории и практике информационной безопасности |

ПК.15

способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|--|--|---|
| ПК.15 способность проводить контрольные проверки работоспособности и эффективности применяемых программно- аппаратных, | Знать криптографические и технические средств защиты информации Уметь проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и | Неудовлетворител Отсутствие знаний методов контрольных проверок работоспособности и эффективности применяемых программно- аппаратных, криптографических и технических средств защиты информации Удовлетворительн Общие, но не структурированные знания |

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|--|--|
| криптографических и технических средств защиты информации | технических средств защиты информации Владеть методами автоматического тестирования | <p>Удовлетворительн методов контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации</p> <p>Хорошо Сформированные, но содержащие отдельные пробелы знания методов контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации</p> <p>Отлично Сформированные систематические знания методов контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации</p> |

ПК.9

способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|--|--|--|
| ПК.9 способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем | Знать методы анализа проектных решений Уметь проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем Владеть навыками проектирования | <p>Неудовлетворител Отсутствие умений проведения синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем</p> <p>Удовлетворительн Общие, но не структурированные умения синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем</p> <p>Хорошо Сформированные, но содержащие отдельные умения синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем</p> <p>Отлично Сформированные систематические умения синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем</p> |

ПК.5

способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|---|---|
| ПК.5 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы | Знать классификацию угроз информационной безопасности Уметь разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы Владеть современными средствами анализа информационной безопасности автоматизированной системы | Неудовлетворител Отсутствие способности разрабатывать политики информационной безопасности автоматизированных систем Удовлетворительн Общие, но не структурированные знания методов разработки политики информационной безопасности автоматизированных систем Хорошо Сформированные, но содержащие отдельные пробелы знания методов разработки политики информационной безопасности автоматизированных систем Отлично Сформированные систематические умение разрабатывать политики информационной безопасности автоматизированных систем |

ПК.12

способность разрабатывать политики информационной безопасности автоматизированных систем

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|--|---|--|
| ПК.12 способность разрабатывать политики информационной безопасности автоматизированных систем | Знать нормативные документы для создания политики информационной безопасности Уметь разрабатывать политики информационной безопасности автоматизированных систем Владеть навыками формирования политики информационной безопасности | Неудовлетворител Отсутствие умений разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы Удовлетворительн Общие, но не структурированные умения разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы Хорошо Сформированные, но содержащие отдельные пробелы умения разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы Отлично Сформированные систематические умения разрабатывать модели угроз и модели |

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|----------------------------|------------------------------------|--|
| | | Отлично нарушителя информационной безопасности автоматизированной системы |

ПК.23

способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|--|---|--|
| ПК.23 способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно- распорядительных документов в сфере профессиональной деятельности | Знать методологическую базу создания проектов и регламентирующих документов Уметь разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, Владеть навыками работы с международными стандартами и спецификациями | Неудовлетворител Отсутствие знаний методологической базы создания проектов и регламентирующих документов Отсутствие умений разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, Не владение навыками работы с международными стандартами и спецификациями Удовлетворительн Общие, но не структурированные знания методологической базы создания проектов и регламентирующих документов Частично сформированное умение разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, Частичное владение навыками работы с международными стандартами и спецификациями Хорошо Сформированные, но содержащие отдельные пробелы знания методологической базы создания проектов и регламентирующих документов В целом успешные, но содержащие отдельные пробелы умения разрабатывать |

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|----------------------------|------------------------------------|---|
| | | <p>Хорошо проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, В целом успешные, но содержащие отдельные пробелы владения навыками работы с международными стандартами и спецификациями</p> <p>Отлично Сформированные систематические знания методологической базы создания проектов и регламентирующих документов Сформированное умение разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, Сформированное владение навыками работы с международными стандартами и спецификациями</p> |

ПК.31

способность управлять информационной безопасностью автоматизированной системы

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|---|--|
| ПК.31 способность управлять информационной безопасностью автоматизированной системы | Знать архитектуру и функциональные особенности автоматизированной системы Уметь управлять информационной безопасностью автоматизированной системы Владеть навыками администрирования сложной автоматизированной системы | <p>Неудовлетворител Отсутствие знаний архитектур и функциональных особенностей автоматизированной системы Отсутствие умений управлять информационной безопасностью автоматизированной системы Не владение навыками администрирования сложной автоматизированной системы</p> <p>Удовлетворительн Общие, но не структурированные знания архитектур и функциональных особенностей автоматизированной системы Частично сформированное умение управлять информационной безопасностью автоматизированной системы Частичное владение навыками администрирования сложной</p> |

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|----------------------------|------------------------------------|---|
| | | <p>Удовлетворительн автоматизированной системы</p> <p>Хорошо Сформированные, но содержащие отдельные пробелы знания архитектур и функциональных особенностей автоматизированной системы В целом успешные, но содержащие отдельные пробелы умения управлять информационной безопасностью автоматизированной системы В целом успешные, но содержащие отдельные пробелы владения навыками администрирования сложной автоматизированной системы</p> <p>Отлично Сформированные систематические знания архитектур и функциональных особенностей автоматизированной системы Сформированное умение управлять информационной безопасностью автоматизированной системы Сформированное владение навыками администрирования сложной автоматизированной системы</p> |

ПК.13

способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|---|--|
| ПК.13 способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы | Знать современные паттерны проектирования. Уметь проектировать системы управления информационной безопасностью автоматизированной системы. Владеть оснoвом управления проектами и системами контроля версий . | <p>Неудовлетворител Отсутствие знаний современных паттернов проектирования. Отсутствие умений проектировать системы управления информационной безопасностью автоматизированной системы. Не владение оснoвом управления проектами и системами контроля версий.</p> <p>Удовлетворительн Общие, но не структурированные знания современных паттернов проектирования. Частично сформированное умение проектировать системы управления информационной безопасностью</p> |

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|----------------------------|------------------------------------|---|
| | | <p>Удовлетворительн автоматизированной системы. Частичное владение осиновом управления проектов и системами контроля версий.</p> <p>Хорошо Сформированные, но содержащие отдельные пробелы знания современных паттернов проектирования. Вцелом успешные, но содержащие отдельные пробелы умения проектировать системы управления информационной безопасностью автоматизированной системы. Вцелом успешные, но содержащие отдельные пробелы владения осиновом управления проектов и системами контроля версий .</p> <p>Отлично Сформированные систематические знания современных паттернов проектирования. Сформированное умение проектировать системы управления информационной безопасностью автоматизированной системы. Сформированное владение осиновом управления проектов и системами контроля версий .</p> |

ПК.14

способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|--|--|---|
| ПК.14 способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы | Знать современные паттерны проектирования Уметь проектировать средств защиты информации и средств контроля защищенности автоматизированной системы Владеть программным обеспечением по контролю защищенности автоматизированных систем | <p>Неудовлетворител Отсутствие знаний современных паттернов проектирования Отсутствие умений проектировать средств защиты информации и средств контроля защищенности автоматизированной системы Не владение программным обеспечением по контролю защищенности автоматизированных систем</p> <p>Удовлетворительн</p> |

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|----------------------------|------------------------------------|--|
| | | <p>Удовлетворительн Общие, но не структурированные знания современных паттерны проектирования Частично сформированное умение проектировать средств защиты информации и средств контроля защищенности автоматизированной системы Частичное владение программным обеспечением по контролю защищенности автоматизированных систем</p> <p>Хорошо Сформированные, но содержащие отдельные пробелы знания современных паттерны проектирования В целом успешные, но содержащие отдельные пробелы умения проектировать средств защиты информации и средств контроля защищенности автоматизированной системы В целом успешные, но содержащие отдельные пробелы владения программным обеспечением по контролю защищенности автоматизированных систем</p> <p>Отлично Сформированные систематические знания современных паттерны проектирования Сформированное умение проектировать средств защиты информации и средств контроля защищенности автоматизированной системы Сформированное владение программным обеспечением по контролю защищенности автоматизированных систем</p> |

ПК.10

способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|--|---|---|
| ПК.10 способность участвовать в разработке защищенных автоматизированных | Знать методы разработки защищенных автоматизированных систем Уметь разрабатывать защищенных автоматизированных систем по | <p>Неудовлетворител Отсутствие знаний методов разработки защищенных автоматизированных систем Отсутствие умений разрабатывать защищенных автоматизированных систем по профилю своей профессиональной</p> |

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|--|--|--|
| систем по профилю своей профессиональной деятельности | профилю своей профессиональной деятельности Владеть навыками управления проектами, и системами управления версий программ | <p>Неудовлетворител деятельности Не владение навыками управления проектами, и системами управления версий программ</p> <p>Удовлетворительн Общие, но не структурированные знания методов разработки защищенных автоматизированных систем Частично сформированное умение разрабатывать защищенных автоматизированных систем по профилю своей профессиональной деятельности Частичное владение навыками управления проектами, и системами управления версий программ</p> <p>Хорошо Сформированные, но содержащие отдельные пробелы знания методов разработки защищенных автоматизированных систем В целом успешные, но содержащие отдельные пробелы умения разрабатывать защищенных автоматизированных систем по профилю своей профессиональной деятельности В целом успешные, но содержащие отдельные пробелы владения навыками управления проектами, и системами управления версий программ</p> <p>Отлично Сформированные систематические знания методов разработки защищенных автоматизированных систем Сформированное умение разрабатывать защищенных автоматизированных систем по профилю своей профессиональной деятельности Сформированное владение навыками управления проектами, и системами управления версий программ</p> |

ПК.11

способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|--|---|
| ПК.11 способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности | Знать основы проектирования автоматизированных систем Уметь разрабатывать компоненты автоматизированных систем в сфере профессиональной деятельности Владеть навыками управления проектами | <p>Неудовлетворител</p> Отсутствие знания основы проектирования автоматизированных систем Не уметь разрабатывать компоненты автоматизированных систем в сфере профессиональной деятельности отсутствие навыками управления проектами <p>Удовлетворительн</p> Общее но не структурированное знание основы проектирования автоматизированных систем Частично сформированное умение разрабатывать компоненты автоматизированных систем в сфере профессиональной деятельности навыками управления проектами, имеют существенные недостатки <p>Хорошо</p> Сформированные, но содержащие отдельные пробелы знание основы проектирования автоматизированных систем В целом успешные, но содержащие отдельные пробелы умение разрабатывать компоненты автоматизированных систем в сфере профессиональной деятельности В целом успешные, но содержащие отдельные пробелы владение навыками управления проектами <p>Отлично</p> Сформированные систематические знание основ проектирования автоматизированных систем Сформированное умение разрабатывать компоненты автоматизированных систем в сфере профессиональной деятельности Уверенное владение навыками управления проектами |

ПСК.1.1

способность на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|--|---|--|
| ПСК.1.1 способность на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем | знать нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем; уметь применять нормативные документы на практике | <p>Неудовлетворител</p> <p>Отсутствие знаний нормативных документов, относящиеся к обеспечению информационной безопасности открытых информационных систем</p> <p>Отсутствие умений по применению нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем</p> <p>Удовлетворительн</p> <p>Общие, но не структурированные знания нормативных документов, относящиеся к обеспечению информационной безопасности открытых информационных систем</p> <p>Частично сформированное умение применения нормативные документы на практике</p> <p>Хорошо</p> <p>Сформированные, но содержащие отдельные пробелы знания нормативных документов, относящиеся к обеспечению информационной безопасности открытых информационных систем</p> <p>В целом успешные, но содержащие отдельные пробелы умение применения нормативные документы на практике.</p> <p>Отлично</p> <p>Сформированные систематические знания знания нормативных документов, относящиеся к обеспечению информационной безопасности открытых информационных систем</p> <p>Сформированное умение применения нормативные документы на практике</p> |

ПСК.1.2

способность разрабатывать и реализовывать политики информационной безопасности открытых информационных систем

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|--|---|--|
| ПСК.1.2 способность разрабатывать и реализовывать политики информационной безопасности открытых информационных систем | знать требования по разработке и реализации политики информационной безопасности открытых информационных систем; уметь разрабатывать по разработке и реализации политики информационной безопасности открытых информационных систем; владеть навыками по разработке и реализации политики информационной безопасности открытых информационных систем. | Неудовлетворител Отсутствие знаний по разработке и реализации политики информационной безопасности открытых информационных систем Отсутствие умений по разработке и реализации политики информационной безопасности открытых информационных систем Не владение навыками по разработке и реализации политики информационной безопасности открытых информационных систем Удовлетворительн Общие, но не структурированные знания по разработке и реализации политики информационной безопасности открытых информационных систем Частично сформированное умение по разработке и реализации политики информационной безопасности открытых информационных систем Частичное владение навыками по разработке и реализации политики информационной безопасности открытых информационных систем Хорошо Сформированные, но содержащие отдельные пробелы по разработке и реализации политики информационной безопасности открытых информационных систем В целом успешные, но содержащие отдельные пробелы по разработке и реализации политики информационной безопасности открытых информационных систем В целом успешные, но содержащие отдельные пробелы по разработке и реализации политики информационной безопасности открытых информационных систем |

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|----------------------------|------------------------------------|--|
| | | <p>Отлично</p> <p>Сформированные систематические знания по разработке и реализации политики информационной безопасности открытых информационных систем</p> <p>Сформированное умение разрабатывать по разработке и реализации политики информационной безопасности открытых информационных систем</p> <p>Сформированное владение навыками по разработке и реализации политики информационной безопасности открытых информационных систем</p> |

ПСК.1.3

способность участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|---|---|
| <p>ПСК.1.3</p> <p>способность участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы</p> | <p>знать требования по организации и проведении контроля обеспечения информационной безопасности открытой информационной системы;</p> <p>уметь разрабатывать требования по организации и проведении контроля обеспечения информационной безопасности открытой информационной системы;</p> <p>владеть навыками по организации и проведении контроля обеспечения информационной безопасности открытой информационной системы.</p> | <p>Неудовлетворител</p> <p>Отсутствие знаний по организации и проведении контроля обеспечения информационной безопасности открытой информационной системы</p> <p>Отсутствие умений по организации и проведении контроля обеспечения информационной безопасности открытой информационной системы</p> <p>Не владение навыками по организации и проведении контроля обеспечения информационной безопасности открытой информационной системы</p> <p>Удовлетворительн</p> <p>Общие, но не структурированные знания по организации и проведении контроля обеспечения информационной безопасности открытой информационной системы</p> <p>Частично сформированное умение по организации и проведении контроля обеспечения информационной безопасности открытой информационной системы</p> <p>Частичное владение навыками по организации и проведении контроля обеспечения информационной безопасности</p> |

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|----------------------------|------------------------------------|--|
| | | <p>Удовлетворительн открытой информационной системы</p> <p>Хорошо Сформированные, но содержащие отдельные пробелы по организации и проведении контроля обеспечения информационной безопасности открытой информационной системы В целом успешные, но содержащие отдельные пробелы по организации и проведении контроля обеспечения информационной безопасности открытой информационной системы В целом успешные, но содержащие отдельные пробелы по организации и проведении контроля обеспечения информационной безопасности открытой информационной системы</p> <p>Отлично Сформированные систематические знания по организации и проведении контроля обеспечения информационной безопасности открытой информационной системы Сформированное умение разрабатывать по организации и проведении контроля обеспечения информационной безопасности открытой информационной системы Сформированное владение навыками по организации и проведении контроля обеспечения информационной безопасности открытой информационной системы</p> |

ПСК.1.4

способность участвовать в организации и проведении контроля обеспечения информационной безопасности открытой информационной системы

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|--|--|
| ПСК.1.4 способность участвовать в организации и проведении контроля обеспечения информационной | знать требования по проектированию, эксплуатации и совершенствованию системы управления информационной безопасностью открытой информационной системы; уметь разрабатывать | <p>Неудовлетворител Отсутствие знаний по проектированию, эксплуатации и совершенствованию системы управления информационной безопасностью открытой информационной системы Отсутствие умений по проектированию, эксплуатации и совершенствованию системы</p> |

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|--|--|--|
| безопасности открытой информационной системы | требования по проектированию, эксплуатации и совершенствованию системы управления информационной безопасностью открытой информационной системы; владеть навыками по проектированию, эксплуатации и совершенствованию системы управления информационной безопасностью открытой информационной системы. | <p>Неудовлетворител управления информационной безопасностью открытой информационной системы Не владение навыками по проектированию, эксплуатации и совершенствованию системы управления информационной безопасностью открытой информационной системы</p> <p>Удовлетворительн Общие, но не структурированные знания по проектированию, эксплуатации и совершенствованию системы управления информационной безопасностью открытой информационной системы Частично сформированное умение по проектированию, эксплуатации и совершенствованию системы управления информационной безопасностью открытой информационной системы Частичное владение навыками по проектированию, эксплуатации и совершенствованию системы управления информационной безопасностью открытой информационной системы</p> <p>Хорошо Сформированные, но содержащие отдельные пробелы по проектированию, эксплуатации и совершенствованию системы управления информационной безопасностью открытой информационной системы В целом успешные, но содержащие отдельные пробелы по проектированию, эксплуатации и совершенствованию системы управления информационной безопасностью открытой информационной системы В целом успешные, но содержащие отдельные пробелы по проектированию, эксплуатации и совершенствованию системы управления информационной безопасностью открытой информационной системы</p> <p>Отлично Сформированные систематические знания по проектированию, эксплуатации и совершенствованию системы управления информационной безопасностью открытой информационной системы</p> |

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|----------------------------|------------------------------------|--|
| | | <p>Отлично</p> <p>Сформированное умение разрабатывать по проектированию, эксплуатации и совершенствованию системы управления информационной безопасностью открытой информационной системы</p> <p>Сформированное владение навыками по проектированию, эксплуатации и совершенствованию системы управления информационной безопасностью открытой информационной системы</p> |

ПСК.1.5

способность формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|---|--|
| <p>ПСК.1.5</p> <p>способность формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем</p> | <p>знать правила, процедуры, практические приемы, руководящие принципы, методы и средства для обеспечения информационной безопасности открытых информационных систем;</p> <p>уметь разрабатывать правила, процедуры, практические приемы, руководящие принципы, методы и средства для обеспечения информационной безопасности открытых информационных систем</p> <p>владеть навыками разработки правил, процедур, практических приемов, руководящих принципов, методов и средств для обеспечения информационной безопасности открытых информационных систем</p> | <p>Неудовлетворител</p> <p>Отсутствие знаний правил, процедур, практических приемов, руководящих принципов, методов и средств для обеспечения информационной безопасности открытых информационных систем</p> <p>Отсутствие умений правил, процедур, практических приемов, руководящих принципов, методов и средств для обеспечения информационной безопасности открытых информационных систем</p> <p>Не владение навыками правил, процедур, практических приемов, руководящих принципов, методов и средств для обеспечения информационной безопасности открытых информационных систем</p> <p>Удовлетворительн</p> <p>Общие, но не структурированные знания правил, процедур, практических приемов, руководящих принципов, методов и средств для обеспечения информационной безопасности открытых информационных систем</p> <p>Частично сформированное умение правил, процедур, практических приемов,</p> |

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|----------------------------|------------------------------------|---|
| | | <p style="text-align: center;">Удовлетворительн</p> <p>руководящих принципов, методов и средств для обеспечения информационной безопасности открытых информационных систем</p> <p>Частичное владение навыками правил, процедур, практических приемов, руководящих принципов, методов и средств для обеспечения информационной безопасности открытых информационных систем</p> <p style="text-align: center;">Хорошо</p> <p>Сформированные, но содержащие отдельные пробелы знания правил, процедур, практических приемов, руководящих принципов, методов и средств для обеспечения информационной безопасности открытых информационных систем</p> <p>В целом успешные, но содержащие отдельные пробелы знания правил, процедур, практических приемов, руководящих принципов, методов и средств для обеспечения информационной безопасности открытых информационных систем</p> <p>В целом успешные, но содержащие отдельные пробелы знания правил, процедур, практических приемов, руководящих принципов, методов и средств для обеспечения информационной безопасности открытых информационных систем</p> <p style="text-align: center;">Отлично</p> <p>Сформированные систематические знания правил, процедур, практических приемов, руководящих принципов, методов и средств для обеспечения информационной безопасности открытых информационных систем</p> <p>Сформированное умение разрабатывать правил, процедур, практических приемов, руководящих принципов, методов и средств для обеспечения информационной безопасности открытых информационных систем</p> |

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|----------------------------|------------------------------------|---|
| | | Отлично систем Сформированное владение навыками правил, процедур, практических приемов, руководящих принципов, методов и средств для обеспечения информационной безопасности открытых 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 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 |

| Компетенция (индикатор) | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|--|--|---|
| <p>ПСК.1.3 способность участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы</p> <p>ПСК.1.5 способность формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем</p> <p>ПК.5 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы</p> <p>ПК.9 способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем</p> <p>ПК.10 способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности</p> <p>ПК.23 способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-</p> | <p>Контрольная работа</p> <p>Защищаемое контрольное мероприятие</p> | <p>Знание основных угроз и уязвимостей в современных открытых системах.</p> <p>Понимание принципов работы протокола HTTP и веб приложений.</p> <p>Знание базовых понятий web-технологий</p> |

| Компетенция (индикатор) | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|---|----------------------------------|---|
| <p>распорядительных документов в сфере профессиональной деятельности</p> <p>ПК.30</p> <p>способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы</p> <p>ПК.31</p> <p>способность управлять информационной безопасностью автоматизированной системы</p> <p>ПК.32</p> <p>способность обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций</p> | | |

| Компетенция (индикатор) | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|---|--|--|
| <p>ПСК.1.1 способность на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем</p> <p>ПК.5 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы</p> <p>ПК.6 способность проводить анализ рисков информационной безопасности автоматизированной системы</p> <p>ПК.7 способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем</p> <p>ПК.9 способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем</p> <p>ПК.11 способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности</p> <p>ПК.12 способность разрабатывать политики информационной безопасности автоматизированных систем</p> <p>ПК.13 способность участвовать в проектировании системы управления информационной</p> | <p>Контрольная работа</p> <p>Письменное контрольное мероприятие</p> | <p>Знание способов проведения аудита безопасности открытых систем. Умение проводит анализ защищенности система, и проверку системы на наличие уязвимостей. Знание принципов построения атаки на сервер, и способов пост эксплуатации уязвимостей</p> |

| Компетенция (индикатор) | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|---|----------------------------------|---|
| <p>безопасностью автоматизированной системы ПК.14 способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы ПК.15 способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации ПК.18 способность проводить инструментальный мониторинг защищенности автоматизированных систем ПК.30 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы ПК.32 способность обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций</p> | | |

| Компетенция (индикатор) | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|--|--|--|
| <p>ПСК.1.2 способность разрабатывать и реализовывать политики информационной безопасности открытых информационных систем</p> <p>ПСК.1.4 способность участвовать в организации и проведении контроля обеспечения информационной безопасности открытой информационной системы</p> <p>ПК.5 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы</p> <p>ПК.6 способность проводить анализ рисков информационной безопасности автоматизированной системы</p> <p>ПК.7 способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем</p> <p>ПК.11 способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности</p> <p>ПК.12 способность разрабатывать политики информационной безопасности автоматизированных систем</p> <p>ПК.13 способность участвовать в проектировании системы</p> | <p>Итоговое контрольное мероприятие</p> <p>Итоговое контрольное мероприятие</p> | <p>способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы,</p> <p>способность проводить анализ рисков информационной безопасности автоматизированной системы</p> <p>способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем,</p> <p>способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности, способность разрабатывать политики информационной безопасности автоматизированных систем</p> <p>способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы,</p> <p>способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы</p> |

| Компетенция (индикатор) | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|--|----------------------------------|---|
| <p>управления информационной безопасностью автоматизированной системы ПК.14 способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы ПК.15 способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации ПК.18 способность проводить инструментальный мониторинг защищенности автоматизированных систем ПК.23 способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности ПК.30 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы</p> | | |

| Компетенция (индикатор) | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|---|----------------------------------|---|
| ПК.31 способность управлять информационной безопасностью автоматизированной системы ПК.32 способность обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций | | |

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 эталонными 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 аудиторной 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 проводить 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, выставяемый 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 |