ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Иркутский государственный университет путей сообщения»
(ФГБОУ ВО ИрГУПС)

УТВЕРЖДЕНА
приказом ректора
от «08» мая 2020 г. № 266-1

—

Б1.В.ДВ.06.01 Информационная безопасность открытых систем

рабочая программа дисциплины

Направление подготовки – 10.03.01 Информационная безопасность
Профиль подготовки – Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)
Программа подготовки – академический бакалавриат
Квалификация выпускника – бакалавр
Форма обучения – очная
Нормативный срок обучения – 4 года
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 3
Часов по учебному плану – 108

Формы промежуточной аттестации в семестрах:
зачет 8

Распределение часов дисциплины по семестрам

Семестр	8	**Итого**
Число недель в семестре	12	
Вид занятий	Часов по учебному плану	**Часов по учебному плану**
Аудиторная контактная работа по видам учебных занятий	**48**	**48**
– лекции	24	**24**
– практические (семинарские)	12	**12**
– лабораторные	12	**12**
Самостоятельная работа	**60**	**60**
Итого	**108**	**108**

ИРКУТСК

1 ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1 Цели освоения дисциплины	
1	Изучение обучающимися технологий, методов и средств обеспечения информационной безопасности открытых информационных систем.
2	Научить обучающихся формировать и эффективно применять комплекс мер с целью обеспечения информационной безопасности открытых информационных систем (ОИС).
1.2 Задачи освоения дисциплины	
1	Привитие учащимся основ культуры обеспечения информационной безопасности (ИБ) в открытых информационных системах (ОИС).
2	Ознакомить учащихся с основами построения защищенных ОИС.
3	Познакомить учащихся с основными уязвимостями и угрозами информационной безопасности ОИС.
4	Обучение учащихся различным подходам и методам обеспечения информационной безопасности.
1.3 Задачи освоения дисциплины	
Профессионально-трудовое воспитание обучающихся	
Цель профессионально-трудового воспитания – формирование у обучающихся осознанной профессиональной ориентации, понимания общественного смысла труда и значимости его для себя лично, ответственного, сознательного и творческого отношения к будущей деятельности, профессиональной этики, способности предвидеть изменения, которые могут возникнуть в профессиональной деятельности, и умению работать в изменённых, вновь созданных условиях труда. Цель достигается по мере решения в единстве следующих задач: – формирование сознательного отношения к выбранной профессии; – воспитание чести, гордости, любви к профессии, сознательного отношения к профессиональному долгу, понимаемому как личная ответственность и обязанность; – формирование психологи профессионала; – формирование профессиональной культуры, этики профессионального общения; – формирование социальной компетентности и другие задачи, связанные с имиджем профессии и авторитетом транспортной отрасли	

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
2.1 Требования к предварительной подготовке обучающегося	
Изучение дисциплины «Информационная безопасность открытых систем» основывается на знаниях и умениях обучающихся, полученных при изучении следующих дисциплин:	
1	Б1.Б.14 Криптографические методы защиты информации
2	Б1.Б.16 Техническая защита информации
3	Б1.Б.17 Сети и системы передачи информации
4	Б1.Б.20 Технологии и методы программирования
5	Б1.Б.25 Информационные технологии
6	Б1.Б.33 Метрология, стандартизация и сертификация
7	Б1.В.03 Безопасность вычислительных сетей
8	Б1.В.04 Безопасность операционных систем
9	Б1.В.07 Аудит информационной безопасности
10	Б1.В.ДВ.03.02 Корпоративные информационные системы
11	Б1.В.ДВ.05.01 Системы управления базами данных
12	Б1.В.ДВ.09.02 Администрирование систем баз данных
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б2.Б.06(Пд) Производственная - преддипломная
2	Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

3 ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
ПСК4-1: способностью учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации	
Минимальный уровень освоения компетенции	
Знать	класса защищенности автоматизированной системы управления;

Уметь	разрабатывать и внедрять систему защиты автоматизированной системы;
Владеть	навыками и методами защиты информации при разработке и внедрении автоматизированной системы;
Базовый уровень освоения компетенции	
Знать	состав мер защиты информации и их базовые наборы для соответствующего класса защищенности автоматизированной системы;
Уметь	обеспечивать защиту информации в ходе эксплуатации автоматизированной системы управления;
Владеть	навыками и методами защиты информации в ходе эксплуатации автоматизированной системы управления;
Высокий уровень освоения компетенции	
Знать	особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации.
Уметь	обеспечивать защиту информации при выводе из эксплуатации автоматизированной системы управления.
Владеть	навыками и методами защиты информации при выводе из эксплуатации автоматизированной системы управления.

ПСК4-2: способностью выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей	
Минимальный уровень освоения компетенции	
Знать	комплекс задач администрирования подсистем информационной безопасности СУБД;
Уметь	устанавливать и конфигурировать новое аппаратное и программное обеспечения;
Владеть	навыками администрирования подсистем информационной безопасности СУБД;
Базовый уровень освоения компетенции	
Знать	комплекс задач администрирования подсистем информационной безопасности ОС;
Уметь	устанавливать и конфигурировать необходимые обновления для операционной системы (ОС) и используемых программ, в том числе СУБД;
Владеть	навыками администрирования подсистем информационной безопасности ОС;
Высокий уровень освоения компетенции	
Знать	комплекс задач администрирования компьютерных сетей.
Уметь	выполнять комплекс задач администрирования компьютерных сетей.
Владеть	навыками администрирования компьютерных сетей.

В результате освоения дисциплины обучающийся должен

Знать	
1	принципы и стандарты построения современных ОИС и подходы к интеграции сетей в ОИС;
2	основные уязвимости и угрозы ИБ для ОИС;
3	основные методы и средства реализации удаленных сетевых атак на ОИС;
4	основные тенденции и закономерности развития средств и методов защиты информации в ОИС;
5	основные понятия администрирования подсистемы информационной безопасности;
6	политики безопасности и меры защиты в ОИС;
7	комплексный подход к построению эшелонированной защиты для ОИС.
Уметь	
1	анализировать текущее состояние ИБ на предприятии с целью разработки требований к защищенным ОИС;
2	определять и устранять основные угрозы ИБ для ОИС;
3	строить модели угроз и нарушителя ИБ для ОИС;
4	выявлять и устранять уязвимости в основных компонентах ОИС;
5	обнаруживать, прерывать и предотвращать удаленные сетевые атаки по их характерным признакам;
6	проектировать защищенные ОИС;
7	применять стандартные решения для защиты информации в ОИС и квалифицированно оценивать их качество;
8	используя современные методы и средства, разрабатывать политику ИБ для ОИС;
9	реализовывать системы защиты информации в ОИС в соответствии со стандартами по оценке защищенных систем;
10	применять комплексный подход к обеспечению ИС для ОИС;
11	осуществлять управление и администрирование защищенных ОИС;
12	администрировать подсистемы информационной безопасности операционных систем, систем

	управления базами данных, компьютерных сетей.
Владеть	
1	терминологией и системным подходом построения защищенных ОИС;
2	навыками анализа угроз ИБ и уязвимостей в ОИС;
3	навыками распознавания сетевых атак на ОИС;
4	навыками разработки политик ИБ для ОИС$
5	навыками администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей.

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр	Часы	Код компетенции	Учебная литература, ресурсы сети «Интернет»
1	**Раздел 1. Основные элементы технологии открытых информационных систем.**				
1.1	Основные элементы технологии открытых информационных систем. Совместимость открытых систем. Переносимость и способность к взаимодействию. Базовая модель информационной системы. Расширение базовой модели информационной системы для взаимодействующих систем. Основные модели открытых систем. /Лек/	8	2	ПСК4-1, ПСК4-2	Л1.2,Л3.1, Э1, Э2
1.2	Интранет как открытая система. Структура интранета. Эталонная модель интранета. Этапы создания интранета. Виды интранета. Стандарты интранета. Интранет как часть среды открытых систем. Интранет и экстранет . Портал и интранет. /Лек/	8	2	ПСК4-1, ПСК4-2	Л1.2, Л3.1, Э1, Э2
1.3	Исследование нормативно-правовой базы информационной безопасности предприятия. /Лр/	8	2	ПСК4-1, ПСК4-2	Л2.1, Л2.2, Э2
2	**Раздел 2. Уязвимости открытых систем. Атаки на открытые системы.**				
2.1	Уязвимость открытых систем. Основные понятия. Угрозы открытых систем (в том числе интранета) и причины их реализации. Уязвимости архитектуры клиент-сервер: уязвимости операционных систем; уязвимость серверов; уязвимость рабочих станций; уязвимость каналов связи. /Лек/	8	2	ПСК4-1, ПСК4-2	Л1.1, Л1.2, Л1.3,Л2.1, Л2.2, Э1, Э2
2.2	Удаленные атаки на открытые системы. Анализ сетевого трафика. Подмена доверенного объекта или субъекта. Ложный объект. Отказ в обслуживании. Удаленный контроль над станцией. /Пр/	8	2	ПСК4-1, ПСК4-2	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Э1, Э2
2.3	Политика безопасности для открытых систем (определение, причины выработки, этапы и содержание, реализация и аудит политики безопасности). /Ср/	8	2	ПСК4-1, ПСК4-2	Л1.2, Л2.1, Л2.2, Э1, Э2

2.4	Уязвимость открытых систем. Слабости системных утилит, команд и сетевых сервисов. /Лек/	8	2	ПСК4-1, ПСК4-2	Л1.2, Л2.1, Л2.2, Э1, Э2
2.5	Классические и современные методы, используемые нападающим для проникновения в открытые системы. Перехват данных и обнаружение прослушивающих приложений. Мониторинг в графических интерфейсах. Подмена системных утилит. Атаки с использованием сетевых протоколов. /Лек/	8	2	ПСК4-1, ПСК4-2	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Э1, Э2
2.6	Примеры политик безопасности. Политика использования ресурсов интранета. Политика в отношении паролей. Политика шифрования. Антивирусная политика. Политика оценки рисков. Политика аудита. Политика для программных маршрутизаторов. Политика удаленного доступа. /Лр/	8	2	ПСК4-1, ПСК4-2	Л1.2,Л2.1, Л2.2, Э1, Э2
2.7	Слабости современных технологий программирования. Ошибки в программном обеспечении. Сетевые вирусы. /Лек/	8	2	ПСК4-1, ПСК4-2	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Э1, Э2
2.8	Типичные сценарии и уровни атак. Этапы реализации атак. Примеры некоторых атак. /Пр/	8	2	ПСК4-1, ПСК4-2	Л1.2, Л1.3, Л2.1,Л2.2, Э1, Э2
2.9	Примеры политик безопасности. Политика подключения подразделений к интранету. Политика для конфиденциальной безопасности. Политика для веб-сервера. Политика пересылки электронной почты. Политика подключения новых устройств в интранет. /Лр/	8	2	ПСК4-1, ПСК4-2	Л1.2, Л2.1, Л2.2, Э1, Э2
2.10	Средства интранета. /Ср/	8	4	ПСК4-1, ПСК4-2	Л2.1, Л2.2, Э1, Э2
2.11	Средства создания порталов. /Ср/	8	4	ПСК4-1, ПСК4-2	Э1, Э2
2.12	Стандарты ISO по защите информации в открытых системах. /Ср/	8	4	ПСК4-1, ПСК4-2	Э1, Э2
3	**Раздел 3. Обеспечение информационной безопасности в открытых системах.**				
3.1	Четырехуровневая модель открытой системы. Специфика защиты ресурсов открытых систем на примере интранета. Выбор сетевой топологии интранета при подключении к другим внешним сетям. Физическая изоляция. Изоляция протоколов. Выделенные каналы и маршрутизаторы. Принципы создания защищенных средств связи объектов в открытых системах. /Лек/	8	2	ПСК4-1, ПСК4-2	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Э1, Э2
3.2	Межсетевые экраны. Функции межсетевых экранов. Руководящий документ Гостехкомиссии России по межсетевым	8	2	ПСК4-1, ПСК4-2	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Э1, Э2

	экранам. Профили защиты для межсетевых экранов. Типы межсетевых экранов. Основные компоненты межсетевого экрана. /Лек/				
3.3	Схемы подключения межсетевых экранов. Слабости межсетевых экранов. Выбор реализаций межсетевых экранов. /Лр/	8	2	ПСК4-1, ПСК4-2	Л1.3, Л2.1, Л2.2, Э1, Э2
3.4	Средства обеспечения информационной безопасности в открытых системах. Создание комплексной системы обеспечения безопасности открытых систем. Управление безопасности открытых систем. Рекомендации по обеспечению информационной безопасности открытых систем. /Лек/	8	2	ПСК4-1, ПСК4-2	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Э1, Э2
3.5	Аутентификация субъектов и объектов взаимодействия в открытых системах. Сетевая аутентификация. Подсистема аутентификации. /Пр/	8	2	ПСК4-1, ПСК4-2	Л1.1, Л2.1, Л1.3, Э1, Э2
3.6	Изучение российского рынка средств аутентификации. Сравнительный анализ средств аутентификации. /Ср/	8	2	ПСК4-1, ПСК4-2	Э1, Э2
3.7	Сервисы безопасности (идентификация/аутентификация, разграничение доступа, экранирование, шифрование, управление и др.). /Лек/	8	2	ПСК4-1, ПСК4-2	Л1.1, Л1.2, Л1.3, Л2.1, Э1, Э2
3.8	Криптографическая защита в открытых системах. Основные понятия и методы криптографии. Стандартизация криптографических функций и механизмов. Криптографические протоколы. Криптографическая инфраструктура. Программные и аппаратные средства криптографической защиты. /Пр/	8	2	ПСК4-1, ПСК4-2	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Э1, Э2
3.9	Исследование поточных и блочных алгоритмов шифрования. Использование хэш-функций. /Лр/	8	2	ПСК4-1, ПСК4-2	Л1.1, Л1.3, Л2.1, Л2.2, Л2.3, Э1, Э2
3.10	Виртуальные вычислительные сети. Определение виртуальных частных вычислительных сетей. Цели и задачи построения ВЧВС. Специфика построения ВЧВС. Туннелирование в ВЧВС. Схема ВЧВС. Политики безопасности для ВЧВС. Стандартные протоколы построения ВЧВС. Проблемы и уязвимости современных ВЧВС. /Лек/	8	2	ПСК4-1, ПСК4-2	Л2.1, Л2.2, Э1, Э2
3.11	Системы анализа защищенности. Аудит и мониторинг информационной безопасности в открытых системах. Место и задачи систем анализа защищенности в защите открытых систем. Классификации систем анализа защищенности. Сетевые	8	2	ПСК4-1, ПСК4-2	Э1, Э2

	сканеры. Системные сканеры. Сканеры безопасности для приложений. Критерии выбора сканеров безопасности. /Пр/				
3.12	Работа с системой контроля защищенности (MaxPatrol – демо-версия). /Лр/	8	2	ПСК4-1, ПСК4-2	Э1, Э2
3.13	Стандартные протоколы построения ВЧВС. Виды ВЧВС в зависимости от решаемых задач. Топологии ВЧВС. Виртуальные локальные вычислительные сети. /Лек/	8	2	ПСК4-1, ПСК4-2	Л2.1, Л2.2, Э1, Э2
3.14	Системы обнаружения и предотвращения вторжений. Методы отражения вторжений. Основы построения систем обнаружения вторжений. Системное обнаружение вторжений. Сетевое обнаружение вторжений. Поведенческое обнаружение вторжений. Интеллектуальное обнаружение вторжений. Комплексное обнаружение вторжений. Выбор системы обнаружения вторжений. Развертывание системы обнаружения вторжений. Практика обнаружения вторжений. /Пр/	8	2	ПСК4-1, ПСК4-2	Э1, Э2
3.15	Системы обнаружения атак, работающие в режиме реального времени. /Ср/	8	2	ПСК4-1, ПСК4-2	Э1, Э2
3.16	Другие средства обеспечения безопасности в открытых системах. Защита от спама в электронной почте. Многофункциональные устройства защиты от сетевых атак. Системы анализа и управления рисками. Системы обеспечения информационной безопасности на уровне предприятия. /Ср/	8	6	ПСК4-1, ПСК4-2	Л1.2, Л2.1, Л2.2, Э1, Э2
3.17	Документы по основным протоколам для виртуальных частных сетей. Сравнительные характеристики ВЧВС-продуктов российских производителей. /Ср/	8	4	ПСК4-1, ПСК4-2	Л2.1, Л2.2
3.18	Зарубежные средства обеспечения информационной безопасности в сетях. /Ср/	8	4	ПСК4-1, ПСК4-2	Э1, Э2
3.19	Подготовка докладов к семинарским занятиям. /Ср/	8	8	ПСК4-1, ПСК4-2	Л1.2, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Э1, Э2
3.20	Проработка лекционного материала. Подготовка промежуточному контролю. /Ср/	8	8	ПСК4-1, ПСК4-2	Л1.2, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Э1, Э2
4	Подготовка к зачету. /Ср/	8	12	ПСК4-1, ПСК4-2	Л1.2, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Э1, Э2

5 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ

АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине разрабатывается в соответствии с Положением о формировании фондов оценочных средств для проведения текущего контроля успеваемости, промежуточной и государственной итоговой аттестации № П.312000.06.7.188-2017.

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по данной дисциплине оформляется в виде приложения № 1 к рабочей программе дисциплины и размещаются в электронной информационно-образовательной среде Университета, доступной обучающемуся через его личный кабинет.

6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1 Основная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
Л1.1	Малюк А.А., Горбатов В.С., Королев В.И.	Введение в информационную безопасность : учебное пособие. [Электронный ресурс] http://e.lanbook.com/books/element.php? pl1_id=5171	Горячая линия-Телеком, 2012.	100 % онлайн
Л1.2	Милославская Н. Г.	Сетевые атаки на открытые системы на примере Интранета: учебное пособие. [Электронный ресурс] http://biblioclub.ru/index.php?page=book&id=231630	М.:МИФИ, 2012.	100 % онлайн
Л1.3	Сердюк В.А.	Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие. [Электронный ресурс] http://biblioclub.ru/index.php?page= book&id=440285	М.: Издательский дом Высшей школы экономики, 2015.	100 % онлайн

6.1.2 Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
Л2.1	Прохорова О.В.	Информационная безопасность и защита информации : учебник. [Электронный ресурс] http://biblioclub.ru/index.php?page=book&id=438331	Самара : СГАСУ, 2014.	100 % онлайн
Л2.2	Мэйволд Э.	Безопасность сетей : учебное пособие. [Электронный ресурс] http://biblioclub.ru/index.php?page=book&id=429035	М : ИНТУИТ, 2016.	100 % онлайн
Л2.3	Иванов М.А., Чугунков И.В.	Криптографические методы защиты информации в компьютерных системах и сетях : учебное пособие. [Электронный ресурс] http://biblioclub.ru/index.php?page=book&id=231673	М. : МИФИ, 2012.	100 % онлайн

6.1.3 Методические разработки

	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/ 100% онлайн
Л3.1	Кудряшов В. А	Открытые информационные системы и сети: учебное пособие.	М.: УМК МПС России, 2001.	42

6.1.4 Перечень учебно-методического обеспечения для самостоятельной работы

обучающихся по дисциплине				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/ 100% онлайн
Л4.1	Аршинский Л.В., Темникова Е.А.	Открытые информационные системы	Личный кабинет обучающегося	100 % онлайн
6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»				
Э.1	Википедия: свободная энциклопедия. https://ru.wikipedia.org/wiki/Заглавная_страница			
Э.2	Национальный открытый университет ИНТУИТ http://www.intuit.ru			
6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)				
6.3.1 Перечень базового программного обеспечения				
6.3.1.1	ОС Microsoft Windows XP Professional, количество – 227, лицензия № 44718499; ОС Microsoft Windows 7 Professional, количество – 100, лицензия № 49379844			
6.3.1.2	Офисный пакет Microsoft Office 2010, количество – 155, Лицензия № 48288083; Libre Office v. 5.2, свободно распространяемое ПО, https://ru.libreoffice.org			
6.3.2Переченьспециализированного программного обеспечения				
6.3.2.1	Firefox (браузер), (лицензия: бесплатно, количество: не ограничено).			
6.3.2.2	MaxPatrol (демонстрационная версия), (лицензия: бесплатно, количество: не ограничено).			
6.3.2.3	PacketTracer (лицензия: бесплатно, количество: не ограничено).			
6.3.2.4	PEM (лицензия: бесплатно, количество: не ограничено).			
6.3.2.5	Wireshark (лицензия: бесплатно, количество: не ограничено).			
6.3.3 Перечень информационных справочных систем				
6.3.3.1	Информационно-справочная система Консультант Плюс http://www.consultant.ru			
6.4 Перечень правовых и нормативных документов				
6.4.1	Не предусмотрено			

7 ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ	
1	Корпуса А, Б, В, Г, Д, Е ИрГУПС находятся по адресу г. Иркутск, ул. Чернышевского, д. 15; корпус Л – по адресу г. Иркутск, ул. Лермонтова, д.80.
2	Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых проектов, работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническими средствами обучения (ноутбук, проектор, экран), служащими для представления учебной информации большой аудитории. Для проведения занятий лекционного типа имеются учебно-наглядные пособия (презентации, плакаты, таблицы), обеспечивающие тематические иллюстрации содержания дисциплины. Помещение для хранения и профилактического обслуживания учебного оборудования – А-521.
3	Учебная лаборатория «Средства и методы защиты информации», Д-523. Оснащена компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Перечень установленных программных средств: Microsoft Office 2010, Open Office 3.0.1, 7-zip, Borland Delphi 7, Abode Reader XI, Microsoft Security Essentials.
4	Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Помещения для самостоятельной работы обучающихся: – читальные залы; – учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507.

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ	
Вид учебной деятельности	Организация учебной деятельности обучающегося

Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки. Обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии. Уделить внимание следующим понятиям (перечисление понятий) и др.
Лабораторная работа	Внимательно ознакомиться с целью, задачами и описанием лабораторной работы. Изучить теоретический материал, выполнить практическое задание, используя необходимые программные и аппаратно-технические средства, оформить отчет в соответствии с заданием и требованиями нормоконтроля. Ответить на вопросы по теме лабораторной работы. В ходе выполнения лабораторных работ раскрываются основные вопросы в рамках рассматриваемой темы, делаются акценты на наиболее сложные, проблемные и моменты изучаемого материала, которые должны быть приняты студентами во внимание. Основной целью лабораторных занятий является расширение и углубление материала практического характера, контроль качества усвоения пройденного материала и ходом выполнения студентами заданий. При подготовке к зачету необходимо ориентироваться на лекции, результаты выполненных лабораторных работ и рекомендуемую литературу.
Практические (семинарские) занятия	Обобщение, расширение и углубление пройденного материала на лекции. Решение задач на закрепление практических навыков. Выступление с докладами по заданной теме, формирование навыков самостоятельной работы, анализа литературных источников, публичного выступления и аргументации собственного мнения. Обсуждение вопросов, вызвавших затруднение, с преподавателем. Участие в дискуссиях и коллоквиумах. Контроль качества усвоения пройденного материала.
Самостоятельная работа	Эффективное освоение дисциплины предполагает самостоятельную внеаудиторную работу, которая включает в себя изучение предлагаемого в рабочей программе и самостоятельно найденного материала по соответствующим разделам и темам для дополнения конспектов лекций, подготовки к практическим занятиям и защиты лабораторных работ. Для более глубокого освоения дисциплины рекомендуется пользоваться учебной литературой, приведенной в рабочей программе дисциплины. Если какие-либо разделы и темы освоить не удается, а также возникают трудности в выполнении практических работ, необходимо пройти консультацию у преподавателя.
Коллоквиум	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися.
Конспект	Конспект – средство, позволяющее формировать и оценивать способность обучающегося к восприятию, обобщению и анализу информации. Основу конспекта составляет лекционный материал. Основа должна быть дополнена самостоятельно проработанным материалом. Конспект может быть использовано для оценки знаний и умений обучающихся. Преподаватель на лекции доводит до сведения обучающихся тему конспекта и указывает необходимую учебную литературу. Темы и перечень литературы выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет. Конспекты должны быть выполнены в установленный преподавателем срок. Конспекты сдаются на проверку. Предусматривается выполнение конспектов по всем темам дисциплины.
Собеседование	Средство контроля, организованное как специальная беседа педагогического работника с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определен-ному разделу, теме, проблеме и т.п.
Сообщение, доклад и презентация	Продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы
Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины, размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.	

Приложение 1 к рабочей программе по дисциплине Б1.В.ДВ.06.01 «Информационная безопасность открытых систем»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине Б1.В.ДВ.06.01 «Информационная безопасность открытых систем»

1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Дисциплина «Теория языков программирования и методы трансляции» участвует в формировании компетенции:

ПСК4-1: способностью учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации;

ПСК4-2: способностью выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей.

1.1 Таблица траекторий формирования у обучающихся компетенций ПСК4-1, ПСК4-2 при освоении образовательной программы

Код компе-тенции	Наименование компетенции	Индекс и наименование дисциплин, практик, участвующих в формировании компетенции	Семестр изучения дисциплины	Этапы формирования компетенции
ПСК4-1	Способностью учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации	Б1.Б.25 Информационные технологии	2	1
		Б1.В.ДВ.03.02 Корпоративные информационные системы	3	2
		Б2.В.03(П) Производственная практика - эксплуатационная	6	3
		Б1.В.ДВ.06.01 Информационная безопасность открытых систем	8	4
		Б2.В.04(Пд) Производственная практика - преддипломная	8	4
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8	4
ПСК4-2	Способностью выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей	Б1.Б.17 Сети и системы передачи информации	4	1
		Б1.В.04 Безопасность операционных систем	5	2
		Б1.В.ДВ.05.01 Системы управления базами данных	5	2
		Б1.В.ДВ.05.02 Средства сетевых систем управления базами данных	5	2
		Б1.В.ДВ.09.02 Администрирование систем баз данных	5	2
		Б1.В.03 Безопасность вычислительных сетей	7	3
		Б1.В.06 Безопасность систем баз данных	8	4
		Б1.В.ДВ.06.01 Информационная безопасность открытых систем	8	4
		Б1.В.ДВ.06.02 Сетевое администрирование	8	4
		Б2.В.04(Пд) Производственная практика - преддипломная	8	4
		Б3.Б.01 Защита выпускной квалификационной работы, включая	8	4

		подготовку к процедуре защиты и процедуру защиты		

1.2 Таблица соответствия уровней освоения компетенций ПСК4-1, ПСК4-2 планируемым результатам обучения

Код компетенции	Наименование компетенции	Наименования разделов дисциплины	Уровни освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции)
ПСК-4.1	Способностью учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации	**Раздел 1.** Основные элементы технологии открытых информационных систем. **Раздел 2.** Уязвимости открытых систем. Атаки на открытые системы. **Раздел 3.** Обеспечение информационной безопасности в открытых системах.	Минимальный уровень	**Знать:** классы защищенности автоматизированной системы управления. **Уметь:** разрабатывать и внедрять систему защиты автоматизированной системы. **Владеть:** навыками и методами защиты информации при разработке и внедрении автоматизированной системы.
			Базовый уровень	**Знать:** состав мер защиты информации и их базовые наборы для соответствующего класса защищенности автоматизированной системы. **Уметь:** обеспечивать защиту информации в ходе эксплуатации автоматизированной системы управления. **Владеть:** навыками и методами защиты информации в ходе эксплуатации автоматизированной системы управления.
			Высокий уровень	**Знать:** особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации. **Уметь:** обеспечивать

				защиту информации при выводе из эксплуатации автоматизированной системы управления. **Владеть**: навыками и методами защиты информации при выводе из эксплуатации автоматизированной системы управления.
ПСК-4.2	Способностью выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей	**Раздел 1.** Основные элементы технологии открытых информационных систем. **Раздел 2.** Уязвимости открытых систем. Атаки на открытые системы. **Раздел 3.** Обеспечение информационной безопасности в открытых системах.	Минимальный уровень	**Знать** комплекс задач администрирования подсистем информационной безопасности СУБД. **Уметь**: устанавливать и конфигурировать новое аппаратное и программное обеспечения. **Владеть**: навыками администрирования подсистем информационной безопасности СУБД.
			Базовый уровень	**Знать**: комплекс задач администрирования подсистем информационной безопасности ОС **Уметь**: устанавливать и конфигурировать необходимые обновления для операционной системы (ОС) и используемых программ, в том числе СУБД **Владеть**: навыками администрирования подсистем информационной безопасности ОС
			Высокий уровень	**Знать**: комплекс задач администрирования компьютерных сетей. **Уметь**: выполнять комплекс задач администрирования компьютерных сетей **Владеть**: навыками администрирования компьютерных сетей.

1.3 Программа контрольно-оценочных мероприятий за период изучения дисциплины

Контроль качества освоения дисциплины включает в себя текущий контроль успеваемости и промежуточную аттестацию. Текущий контроль успеваемости и промежуточная аттестация обучающихся проводятся в целях установления соответствия достижений обучающихся поэтапным требованиям образовательной программы к результатам обучения и формирования компетенций.

№	Неделя	Наименование оценочного мероприятия	Объект контроля (понятия, тема / раздел дисциплины, компетенция, и т.д.)		Наименование оценочного средства (форма проведения)
1	2	3	4	5	6
1	1,2	Текущий контроль	Тема «Основные элементы технологии открытых информационных систем».	ПСК-4.1, ПСК-4.2	Конспект (письменно). Коллоквиум (интерактивная)
2	2-12	Текущий контроль	Тема « Основы информационной безопасности открытых информационных систем». Тема «Угрозы информационной безопасности открытых информационных систем». Тема «Уязвимости открытых систем на примере Intranet». Тема «Атаки на открытые системы». Тема «Обеспечение информационной безопасности в открытых системах». Тема «Законодательный уровень информационной безопасности. Политика безопасности».	ПСК-4.1, ПСК-4.2	Сообщение, доклад и презентация (интерактивная)
3	3	Текущий контроль	Тема «Интранет как открытая система».	ПСК-4.1, ПСК-4.2	Конспект (письменно)
4	4,5	Текущий контроль	Тема «Уязвимости и угрозы открытых информационных систем».	ПСК-4.1, ПСК-4.2	Конспект (письменно). Коллоквиум (интерактивная)
5	6	Текущий контроль	Тема «Классические и современные методы, используемые нападающим для проникновения в открытые системы».	ПСК-4.1, ПСК-4.2	Конспект (письменно)
6	6	Текущий контроль	Тема «Четырехуровневая модель открытой системы. Специфика защиты ресурсов открытых систем на примере интранета».	ПСК-4.1, ПСК-4.2	Коллоквиум (интерактивная форма)
7	7	Текущий контроль	Тема «Межсетевые экраны».	ПСК-4.1, ПСК-4.2	Конспект (письменно) Собеседование (устно)
8	8,9	Текущий контроль	Тема «Средства обеспечения информационной безопасности в	ПСК-4.1,	Конспект (письменно).

			открытых системах. Создание комплексной системы обеспечения безопасности открытых систем».	ПСК-4.2	Коллоквиум (интерактивная)
9	9	Текущий контроль	Тема «Аутентификация субъектов и объектов взаимодействия в открытых системах».	ПСК-4.1, ПСК-4.2	Собеседование (устно)
10	10	Текущий контроль	Тема «Криптографическая защита в открытых системах».	ПСК-4.1, ПСК-4.2	Собеседование (устно)
11	11	Текущий контроль	Тема «Управление безопасности открытых систем».	ПСК-4.1, ПСК-4.2	Конспект (письменно)
12	11	Текущий контроль	Тема «Системы анализа защищенности». Тема «Системы обнаружения и предотвращения вторжений».		Собеседование (устно)
13	12	Текущий контроль	Тема Сервисы безопасности (идентификация/аутентификация, разграничение доступа, экранирование, шифрование, управление и др.)».	ПСК-4.1, ПСК-4.2	Конспект (письменно)
14	13	Текущий контроль	Тема «Виртуальные вычислительные сети».	ПСК-4.1, ПСК-4.2	Конспект (письменно) Собеседование (устно)
15	13	Промежуточный контроль – зачет	Раздел 1. Основные элементы технологии открытых информационных систем. Раздел 2. Уязвимости открытых систем. Атаки на открытые системы. Раздел 3. Обеспечение информационной безопасности в открытых системах.	ПСК-4.1, ПСК-4.2	Собеседование (устно)

1.4 Перечень используемых оценочных средств для текущего контроля успеваемости с описанием показателей и критериев оценивания результатов обучения, описанием шкал оценивания, типовыми контрольными заданиями и методическими материалами, определяющими процедуру оценивания результатов

Текущий контроль успеваемости – основной вид систематической проверки знаний, умений, навыков обучающихся. Задача текущего контроля – оперативное и регулярное управление учебной деятельностью обучающихся на основе обратной связи и корректировки. Текущий контроль позволяет получать первичную информацию о ходе и качестве усвоения учебного материала, а также стимулировать регулярную целенаправленную работу обучающихся.

В ходе текущего контроля проводится оценивание результатов усвоения отдельных тем. Для оценивания результатов обучения используется четырехбалльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и двухбалльная шкала: «зачтено», «не зачтено». Результаты оценивания заносятся преподавателем в журнал и учитываются в виде интегральной оценки при проведении промежуточной аттестации.

В ходе текущего контроля успеваемости используются различные формы оценочных средств, соответствующие программе контрольно-оценочных мероприятий на период изучения дисциплины.

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
Текущий контроль успеваемости			
1	Конспект	Средство, позволяющее формировать и оценивать способность обучающегося к восприятию, обобщению и анализу информации. Рекомендуется для оценки знаний и умений обучающихся	Темы конспектов по дисциплине
2	Коллоквиум	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися.	Вопросы по темам/разделам дисциплины
3	Собеседование	Средство контроля на практическом занятии, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п. Рекомендуется для оценки знаний, умений и владений обучающихся	Комплект вопросов для устного опроса учащихся по разделам / темам дисциплины
4	Сообщение, доклад и презентация	Продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы.	Темы докладов, сообщений.

Конспект

Преподаватель не мене, чем за неделю до срока выполнения конспекта должен довести до сведения обучающихся тему конспекта и указать необходимую учебную литературу. Темы и перечень необходимой учебной литературы выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет. Конспект должен быть выполнены в установленный преподавателем срок. Конспекты в назначенный срок сдаются на проверку.

Типовые контрольные задания

Темы конспектов, предусмотренных рабочей программой дисциплины:

1. Основные элементы технологии открытых информационных систем.
   1.1 Совместимость открытых систем.
   1.2 Переносимость и способность к взаимодействию.
   1.3 Базовая модель информационной системы.
   1.4 Расширение базовой модели информационной системы для взаимодействующих систем.
   1.5 Основные модели открытых систем.
2. Интранет как открытая система.
   2.1 Структура интранета.
   2.2 Эталонная модель интранета.
   2.3 Этапы создания интранета.
   2.4 Виды интранета.
   2.5 Стандарты интранета.

2.6 Интранет как часть среды открытых систем.
2.7 Интранет и экстранет .
2.8 Портал и интранет.

3. Уязвимость открытых систем. Основные понятия.
4. Угрозы открытых систем (в том числе интранета) и причины их реализации.
5. Уязвимости архитектуры клиент-сервер: уязвимости операционных систем; уязвимость серверов; уязвимость рабочих станций; уязвимость каналов связи.
6. Слабости системных утилит, команд и сетевых сервисов.
7. Классические и современные методы, используемые нападающим для проникновения в открытые системы.

7.1 Перехват данных и обнаружение прослушивающих приложений.
7.2 Мониторинг в графических интерфейсах.
7.3 Подмена системных утилит.
7.4 Атаки с использованием сетевых протоколов.
7.5 Слабости современных технологий программирования.
7.6 Ошибки в программном обеспечении.
7.7 Сетевые вирусы.

8. Четырехуровневая модель открытой системы.
9. Специфика защиты ресурсов открытых систем на примере интранета.
10. Выбор сетевой топологии интранета при подключении к другим внешним сетям.
11. Физическая изоляция.
12. Изоляция протоколов.
13. Выделенные каналы и маршрутизаторы.
14. Принципы создания защищенных средств связи объектов в открытых системах.
15. Межсетевые экраны.

15.1 Функции межсетевых экранов.
15.2 Руководящий документ Гостехкомиссии России по межсетевым экранам.
15.3 Профили защиты для межсетевых экранов.
15. 4 Типы межсетевых экранов.
15.5 Основные компоненты межсетевого экрана.

16. Создание комплексной системы обеспечения безопасности открытых систем.
17. Управление безопасности открытых систем.
18. Рекомендации по обеспечению информационной безопасности открытых систем.
19. Сервисы безопасности (идентификация/аутентификация, разграничение доступа, экранирование, шифрование, управление и др.).
20. Виртуальные вычислительные сети.

20.1 Определение виртуальных частных вычислительных сетей.
20.2 Цели и задачи построения ВЧВС.
20.3 Специфика построения ВЧВС.
20.4 Туннелирование в ВЧВС.
20.5 Схема ВЧВС.
20.6 Политики безопасности для ВЧВС.
20.7 Стандартные протоколы построения ВЧВС.
20.8 Проблемы и уязвимости современных ВЧВС.
20.9 Виртуальные локальные вычислительные сети.

Учебная литература представлена в Пункте 6.1 Рабочей программы дисциплины «Теория языков программирования и методы трансляции».

Критерии и шкала оценивания конспекта

Оценка	Критерий оценки
«отлично»	Конспект полный. В конспектируемом материале выделена

	главная и второстепенная информация. Установлена логическая связь между элементами конспектируемого материала. Даны определения основных понятий, приведены примеры, схемы.
«хорошо»	Конспект полный. В конспектируемом материале выделена главная и второстепенная информация. Установлена не в полном объеме логическая связь между элементами конспектируемого материала. Даны определения основных понятий. Примеры приведены частично.
«удовлетворительно»	Конспект не полный. В конспектируемом материале не выделена главная и второстепенная информация. Не установлена логическая связь между элементами конспектируемого материала. Даны определения основных понятий. Примеры отсутствуют
«неудовлетворительно»	Конспект не удовлетворяет ни одному из критериев, приведенных выше

Коллоквиум

Коллоквиум проводятся в форме обсуждения по предложенным преподавателем вопросам. Продолжительность коллоквиума для каждого учащегося (либо для группы обучающихся) 40-50 минут. Для этого преподаватель заранее формулирует тему или проблемные вопросы для обсуждения, а также цели и задачи занятия. Группа обучающихся может быть разделена на небольшие группы, примерно, по 4 человека.

В порядке, установленном преподавателем, учащиеся зачитывают выработанные, в ходе коллективного обсуждения ответы. Обучающиеся из других микрогрупп задают вопросы докладчику, комментируют и дополняют предложенный ответ.

Преподаватель регулирует обсуждения, задавая наводящие вопросы, корректируя неправильные ответы. После обсуждения каждого вопроса необходимо подвести общие выводы и логично перейти к обсуждению следующего вопроса (важно вопросы распределить таким образом, чтобы ответы микрогрупп чередовались). После обсуждения всех предложенных вопросов преподаватель формулирует выводы и заключение.

Коллоквиум проходит в устной форме и ставит следующие задачи:

- проверка и контроль полученных знаний по изучаемой теме;
- расширение проблематики в рамках дополнительных вопросов по данной теме;
- углубление знаний при помощи использования дополнительных материалов при подготовке к занятию;
- обучающиеся должны продемонстрировать умения работы с различными видами источников;
- формирование навыков работы в коллективе.

Типовые контрольные задания

1. Основные принципы по созданию и функционированию информационно-телекоммуникационных систем.
2. Стратегия защиты информации. Основные признаки, по которым различают и формируют разные стратегии защиты.
3. Базовые сетевые технологии и масштабы сетей, в которых они применяются.
4. Возможные уровни взаимодействия открытых систем и их ответственность.
5. Классифицируйте и опишите угрозы безопасности информационной безопасности корпоративных информационных систем, а также их уязвимости.
6. Какие существуют способы защиты от угроз программно-математического воздействия.
7. Опишите программные средства администрирования.
8. Программные средства защиты от несанкционированного выполнения

стандартных функций (чтения, записи, копирования, форматирования (и т.д.) информации)?

9. Программные и программно-аппаратные средства криптографической защиты?

10. Наиболее эффективные способы и средства защиты от сетевых атак. Сравните самые популярные из них.

11. Наиболее эффективные средства защиты от сбоев, отказов и ошибок. Сделайте сравнительный анализ.

12. Меры и средства защиты информации от утечки по побочным электромагнитным излучениям и наводкам.

13. Абстрактные теоретические принципы целостности данных в соответствии с Кларком и Вилсоном.

14. Опишите семь классов требований доверия (уверенности) по ГОСТ Р ИСО/МЭК 15/408.

Критерии и шкала оценивания коллоквиума

Оценка	Критерий оценки
«отлично»	Ответ обучающегося полный развернутый без принципиальных ошибок, а содержание ответа логически выстроенное. Обучающиеся демонстрируют владение основной терминологией, нормативными документами, а также способность быстро ответить на дополнительный вопрос по рассматриваемой теме.
«хорошо»	Ответ обучающегося полный развернутый с несущественными ошибками. Учащиеся демонстрирует владение основной терминологией, нормативными документами, а также способность (с уточнениями преподавателя) ответить на дополнительный вопрос по рассматриваемой теме
«удовлетворительно»	Ответ обучающегося на поставленный вопрос не проработан; неполное знание основной терминологии; неумение без дополнительных источников (справочников, лекций, подсказок одногруппников) ответить на вопросы, возникающие в процессе обсуждения.
«неудовлетворительно»	Ответ обучающегося не удовлетворяет ни одному из критериев, описанных выше.

Собеседование

Собеседование с обучающимися проходит на семинарских занятиях. В момент проведения собеседования пользоваться учебниками, справочниками, конспектами лекций запрещено.

Преподаватель заранее оглашает учащимся перечень вопросов, ответы на которые необходимо подготовить учащимся самостоятельно.

Задачи проведения собеседования с обучающимися:

- проверка и контроль полученных знаний по изученной теме;
- расширение проблематики в рамках дополнительных вопросов по изученной теме;
- углубление знаний;
- формирование навыков беседы, декларирования знаний и рассуждения.

Типовые контрольные задания

Тема «Аутентификация субъектов и объектов взаимодействия в открытых системах»

1. Какие подходы к аутентификации различают?
2. Что такое «однократная регистрация» и в каких ОИС она используется чаще всего?
3. В чем отличия аутентификации в однородных и гетерогенных клиент-серверных системах?
4. Опишите особенности четырех типовых моделей аутентификации: локальной, прямой, непрямой и автономной?
5. Рассмотрите парольную аутентификацию, ее достоинства и недостатки.
6. В чем достоинства и недостатки аутентификации по адресу?
7. Какие аппаратные средства аутентификации применяются в сетевой среде?
8. Каким образом задаются одноразовые пароли?:
9. Для чего и как используется аутентификация на основе электронной подписи?
10. Как реализуется аутентификация на прикладном уровне?
11. Расскажите о простейшем протоколе аутентификации PAP.
12. Каковы особенности протокола аутентификации «запрос-ответ» и в каких системах он используется?
13. Сравните протоколы RADIUS и TACACS/
14. В каких системах и как применяется протокол EAP?
15. Подробно опишите схему работы протокола Kerberos.
16. Что такое серверы аутентификации? На основе каких служб они работают?

Тема «Межсетевые экраны»

1. Каково основное назначение межсетевого экрана (МЭ)? Перечислите его основные функции.
2. Что такое машина-бастион? Какие требования к ее защите предъявляются?
3. Какие основные вопросы рассмотрены в руководящем документе Гостехкомиссии России по МЭ?
4. Какие профили защиты посвящены МЭ?
5. Сравните программные и аппаратные МЭ.
6. Принцип работы экранирующих коммутаторов.
7. Охарактеризуйте МЭ с фильтрацией пакетов и приведите примеры таких систем.
8. Предназначение серверов-посредников.
9. Основные функции шлюзов сеансового уровня, достоинства и недостатки.
10. Основные функции шлюзов прикладного уровня, достоинства и недостатки.
11. Какие подходы используют в своей работе МЭ экспертного уровня?
12. Что такое «Персональный МЭ», разновидности таких МЭ?
13. Какие схемы подключения МЭ используются в настоящее время?
14. Что такое демилитаризованная зона?
15. Перечислите основные недостатки МЭ.
16. Кто проводит сертификацию МЭ в России и за рубежом?

Тема «Криптографическая защита в открытых системах»

1. Основные задачи защиты ОИС, решаемы криптографическим методом.
2. Основные достоинства и недостатки, а также отличия симметричных и ассиметричных криптосистем.
3. Чем отличаются понятия целостности и подлинности сообщений?
4. Поясните понятие «криптографическая стойкость».
5. Чем определяется длина ключей практически стойких симметричных шифров?
6. Расскажите про шифр Вернама.
7. Для каких целей служит протокол открытого распределения ключей Диффи-Хеллмана?

8. Какие аппаратные средства криптографической защиты существуют?

9. Что такое жизненный цикл криптографического ключа?

10. Что понимается под управлением криптографическими ключами?

11. Какие основные группы протоколов использует инфраструктура открытых ключей (ИОК)?

12. Каковы особенности российского законодательства в сфере организации ИОК?

13. Расскажите о программных средствах криптографической защиты информации.

Тема «Виртуальные вычислительные сети»

1. Какие задачи решает построение виртуальной частной вычислительной сети(ВЧВС)?

2. Возможно ли использование только каналов связи предприятия для создания его ВЧВС?

3. Особенности современных сетей, на основе которых приходится создавать ВЧВС

4. Механизм туннелирования в ВЧВС.

5. Что такое ВЧВС агенты и каковы их функции?

6. Какие бывают виды виртуальных каналов?

7. Какие протоколы создания ВЧВС работают на уровнях модели OSI? Опишите особенности этих протоколов.

8. Какие виды ВЧВС в зависимости от решаемых задач вам известны.

9. Схема построения Intranet VPN.

10. Схема построения Client-server VPN/

11. Схема построения Enternet VPN.

12. Расскажите о VPN с удаленным доступом и их вариантах.

Тема «Системы анализа защищенности»

1. Каково основное назначение и в чем разница аудита и мониторинга информационной безопасности в открытых системах?

2. Какие задачи в защите ОИС решают системы анализа защищенности (САЗ)?

3. Какие уязвимости ОИС выявляют сканеры безопасности?

4. Приведите классификацию сканеров безопасности по различным критериям.

5. Где размещаются агенты сетевых сканеров?

6. Основные этапы работы сетевых сканеров.

7. Что такое системные сканеры безопасности, какие функции они выполняют?

8. Как определяется топология сети при использовании сетевых сканеров безопасности?

9. В чем особенности сканеров безопасности для приложений.

10. Перечислите основные критерии, которыми необходимо руководствоваться при выборе сканеров безопасности.

Тема «Системы обнаружения и предотвращения вторжений (СОВ)»

1. Основные тенденции эволюции методов отражения вторжений.

2. Приведите классификацию методов отражения вторжений в сети.

3. Основные способы прерывания вторжений.

4. Особенности отклонения вторжений.

5. Каково место СОВ в многоуровневой защите интранета?

6. Как можно оценить эффективность работы СОВ?

7. Какие задачи решают системы контроля целостности файлов?

8. На основе какой информации и как работают мониторы регистрационных файлов?

9. Что такое сетевое обнаружение вторжений?

10. Что вам известно о современных комплексах обнаружения вторжений?

11. Какие проблемы еще не решены в современных СОВ?

12. Чем отличаются от СОВ системы предотвращения вторжений?

13. Какова ситуация в области стандартов, регламентирующих обнаружение вторжений и реализующих его систем?

Критерии и шкала оценивания собеседования

Оценка	Критерий оценки
«отлично»	Дан полный ответ на предложенный вопрос (обучающийся владеет терминологией, умеет анализировать и рассуждать). Даны правильные ответы на дополнительные вопросы преподавателя в рамках рассматриваемого вопроса, приведены примеры.
«хорошо»	Дан полный ответ на предложенный вопрос (обучающийся владеет терминологией, умеет анализировать и рассуждать). Частично даны правильные ответы на дополнительные вопросы преподавателя в рамках рассматриваемого вопроса, не приведены примеры.
«удовлетворительно»	Полные ответы на предложенные вопросы не даны (приведены только определения основных терминов).
«неудовлетворительно»	Учащийся не смог ответить на поставленные вопрос и дополнительные вопросы по заданной теме.

Сообщение, доклад и презентация

Темы сообщений/докладов предоставляются обучающимся вначале семестра, для того, чтобы у них была возможность выбора наиболее интересной, понравившейся темы.

Доклады должны сопровождаться презентацией и длиться не более 30 минут.

Типовые контрольные задания

Тема « Основы информационной безопасности открытых информационных систем».

1. Необходимость применения объектно-ориентированного подхода к информационной безопасности.

2. Основные понятия объектно-ориентированного подхода.

3. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем.

4. Недостатки традиционного подхода к информационной безопасности с объектной точки зрения.

5. Стандарт ISO/IEC 15408 «Общие критерии оценки безопасности информационных технологий» (основные понятия; функциональные требования; требования доверия безопасности).

6. Руководящие документы Гостехкомиссии России. _Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт (основные понятия; механизмы безопасности; классы безопасности).

7. Информационная безопасность распределенных систем. Рекомендации X.800 (сетевые сервисы безопасности; сетевые механизмы безопасности; администрирование средств безопасности

Тема «Угрозы информационной безопасности открытых информационных систем».

1. Виды угроз информационной безопасности РФ.
2. Источники угроз информационной безопасности РФ.
3. Угрозы информационной безопасности для автоматизированных систем обработки информации.
4. Модели угроз информационной безопасности для операционных систем компьютеров пользователей.
5. различных подразделений организации.
6. Модели угроз информационной безопасности для систем управления базами данных различных подразделений организации.
7. Модели угроз информационной безопасности для системы электронного документооборота организации.

Тема «Уязвимости открытых систем на примере Intranet».

1. Основные понятия административного уровня информационной безопасности.
2. Политика безопасности.
3. Программа безопасности.
4. Синхронизация программы безопасности с жизненным циклом систем.
5. Понятие об управлении рисками.
6. Основные классы мер процедурного уровня.
7. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ.

Тема «Атаки на открытые системы».

1. Межсетевые экраны (firewall): прикладного уровня; с пакетной фильтрацией; гибридные межсетевые экраны. Пример конфигурирования межсетевого экрана.
2. Организация и эксплуатация виртуальных частных сетей (VPN).
3. Системы предотвращения вторжений (IDS).
4. Цифровые подписи. Управление ключами и сертификация ключей
5. Иерархическая модель доверия. Сетевая модель доверия.
6. Протокол конфиденциального обмена данными SSL.
7. Обеспечение безопасности беспроводных сетей (прослушивание; активные атаки). Протокол WEP. Протокол 802.1X - контроль доступа в сеть по портам.
8. Обеспечение безопасности электронной почты.

Тема «Обеспечение информационной безопасности в открытых системах».

1. Понятия о симметричных криптосистемах (шифры перестановки; шифры сложной замены; одноразовая система шифрования; шифрование методом гаммирования; DES).
2. Понятия об асимметричных криптосистемах (однонаправленные функции; криптосистема шифрования данных RSA; электронная цифровая подпись).
3. Понятие криптоанализа.
4. Аппаратно-программные криптографические средства защиты информации.
5. Системы идентификации и аутентификации пользователей.
6. Системы шифрования дисковых данных.
7. Системы шифрования данных.
8. Системы аутентификации электронных данных.
9. Средства управления ключевой информацией.

Тема «Законодательный уровень информационной безопасности. Политика безопасности».

1. Понятие о законодательном уровне информационной безопасности.
2. Обзор российского законодательства в области информационной безопасности.
3. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности.
4. Закон «Об информации, информатизации и защите информации».
5. Обзор зарубежного законодательства в области информационной безопасности.

6. О текущем состоянии российского законодательства в области информационной безопасности.
7. Политика использования ресурсов Интранета.
8. Политика в отношении паролей.
9. Политика шифрования.
10. Антивирусная политика.
11. Политика управления доступом и регистрации для пользователей Интранета.
12. Политика для пограничных маршрутизаторов подразделений, подключенных к Интранету
13. Политика удаленного доступа мобильных пользователей к Интранету.
14. Политика для конфиденциальной информации, обрабатываемой в Интранете.
15. Политика для оборудования пограничной демилитаризованной зоны подразделений организации.
16. Политика для Экстранета.
17. Политика доступа сотрудников организации к Интернету.
18. Политика для межсетевых экранов
19. Политика пересылки электронной почты для организации.
20. Политика резервирования информации для подразделений организации.

Критерии и шкала оценивания сообщения, доклада и презентации

Оценка	Критерий оценки
«отлично»	Учащийся в докладе полностью раскрыл тему, ответил на все дополнительные вопросы, использовал демонстративный материал, который отлично оформлен, и прекрасно в нем ориентировался.
«хорошо»	Учащийся в докладе полностью раскрыл тему, использовал демонстративный материал, который хорошо оформлен, но есть незначительные неточности, и хорошо в нем ориентировался.
«удовлетворительно»	Учащийся не полностью раскрыл тему, демонстративный материал либо не использовался, либо учащийся в нем не достаточно хорошо ориентировался.
«неудовлетворительно»	Учащийся не подготовил доклад.

2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Критерии определения сформированности компетенций на различных этапах их формирования даны в пункте 1.2. Шкалы и критерии оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета, а также шкала для оценивания уровня освоения компетенций представлена в нижеследующей таблице.

Шкалы оценивания		Критерии оценивания	Уровень освоения компетенций
«отлично»	«зачтено»	Обучающийся правильно ответил на теоретические вопросы. Показал отличные знания в рамках учебного материала. Правильно выполнил практические задания. Показал отличные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на все дополнительные вопросы	Высокий
«хорошо»		Обучающийся с небольшими неточностями ответил на теоретические вопросы. Показал	Базовый

		хорошие знания в рамках учебного материала. С небольшими неточностями выполнил практические задания. Показал хорошие умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на большинство дополнительных вопросов	
«удовлетворительно»		Обучающийся с существенными неточностями ответил на теоретические вопросы. Показал удовлетворительные знания в рамках учебного материала. С существенными неточностями выполнил практические задания. Показал удовлетворительные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Допустил много неточностей при ответе на дополнительные вопросы	Минимальный
«неудовлетворительно»	«не зачтено»	Обучающийся при ответе на теоретические вопросы и при выполнении практических заданий продемонстрировал недостаточный уровень знаний и умений при решении задач в рамках учебного материала. При ответах на дополнительные вопросы было допущено множество неправильных ответов	Компетенции не сформированы

3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Зачет проходит в устной и/или письменной формах по предложенным ниже вопросам. В программу зачета включен материал по изученным разделам дисциплины «Информационная безопасность открытых систем».

Перечень вопросов к зачету

1. Угрозы информационной безопасности (основные определения и критерии классификации угроз). Средства защиты.
2. Сценарии реализации угроз информационной безопасности (разглашение конфиденциальной информации и обход средств защиты от разглашения конфиденциальной информации; кража конфиденциальной информации; нарушение авторских прав на информацию; нецелевое использование ресурсов).
3. Вредоносная программа. Классификация вредоносных программ (вирусы; черви; троянские программы; спам; другие вредоносные программы). Способы распространения вредоносных программ.
4. Основы борьбы с вредоносными программами. Диагностика заражения вредоносными программами. Антивирусное программное обеспечение. Комплексные средства антивирусной защиты.
5. Уязвимости ОИС. Причины уязвимости ИС. Классификация уязвимостей.
6. Уязвимости архитектуры клиент-сервер (конфигурация системы, уязвимость операционных систем, уязвимость серверов, уязвимость рабочих станций, уязвимость каналов связи).
7. Уязвимость системных утилит, команд и сетевых сервисов. Уязвимость современных технологий программирования. Ошибки в программном обеспечении.

8. Модель угроз ИБ. Модель нарушителей ИБ. Инсайдеры и аутсайдеры.

9. Атаки на открытые системы. Удаленные атаки на открытые системы. Классификация удаленных атак.

10. Анализ сетевого трафика. Подмена доверенного объекта или субъекта системы. Внедрение ложного объекта в систему.

11. Типичные сценарии и уровни атак. Удаленный контроль над станцией в сети.

12. Классические методы взлома (взлом парольной защиты). Современные методы взлома: перехват данных при их перемещении по каналам связи и перехват ввода с клавиатуры; мониторинг в графических интерфейсах; подмена системных утилит; нападения с использованием сетевых протоколов.

13. Обеспечение информационной безопасности в открытых системах. Комплексный и фрагментарный подходы к защите ИС. Четырехуровневая модель открытой системы.

14. Эшелонированная защита ОИС в целом и отдельных ее элементов. топология сети: физическая изоляция; изоляция протокола; выделенные каналы.

15. Организационно-правовые методы защиты открытых систем.

16. Политика информационной безопасности. Разновидности политик ИБ. Основные положения политики ИБ.

17. Информационная безопасность в глобальных сетях. Удаленные атаки и механизмы их реализации в глобальных сетях.

18. Криптографическая защита информации. Понятия о симметричных криптосистемах (шифры перестановки; шифры сложной замены; одноразовая система шифрования; шифрование методом гаммирования; DES).

19. Криптографическая защита информации. Понятия об асимметричных криптосистемах (однонаправленные функции; криптосистема шифрования данных RSA; электронная цифровая подпись).

20. Криптографическая защита информации. Аппаратно-программные криптографические средства защиты информации.

21. Межсетевые экраны (firewall): прикладного уровня; с пакетной фильтрацией; гибридные межсетевые экраны.

22. Организация и эксплуатация виртуальных частных сетей (VPN).

23. Иерархическая модель доверия. Сетевая модель доверия.

24. Управление ключами и сертификация ключей.

25. Протокол конфиденциального обмена данными SSL. Протокол WEP. Протокол 802.1X - контроль доступа в сеть по портам.

26. Стандарты и спецификации в области информационной безопасности.

Критерии и шкала оценивания зачета

Оценка	Критерий оценки
«зачтено»	Обучающийся прочно усвоил основные разделы дисциплины, смог ответить в полном объеме на предложенные вопросы, показал глубокие систематизированные знания.
«не зачтено»	Обучающийся не смог дать грамотные, развернутые ответы на предложенные вопросы, допуская неточности, не смог ответить на наводящие вопросы, предложенные преподавателем.

4 Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Задание для текущего контроля и проведения промежуточной аттестации должны быть направлены на оценивание:

– уровня освоения теоретических понятий, научных основ профессиональной деятельности;

– степени готовности обучающегося применять теоретические знания и профессионально значимую информацию, сформированности когнитивных умений;

– приобретенных умений, профессионально значимых для профессиональной деятельности.

Задания для оценивания когнитивных умений (знаний) должны предусматривать необходимость проведения аттестуемым интеллектуальных действий:

– по дифференциации информации на взаимозависимые части, выявлению взаимосвязей между ними и т.п.;

– по интерпретации и творческому усвоению информации из разных источников, ее системного структурирования;

– по выявлению значения предмета учебной дисциплины для достижения конкретной цели, на основе проникновения в суть общественных явлений и процессов;

– по комплексному использованию интеллектуальных инструментов дисциплины для решения учебных и практических проблем.

При составлении заданий необходимо иметь в виду, что они должны носить практико-ориентированный комплексный характер, быть направлены на формирование и закрепление общекультурных и профессиональных компетенций.

Проведение промежуточной аттестации в форме зачета позволяет сформировать среднюю оценку по дисциплине по результатам текущего контроля. Так как оценочные средства, используемые при текущем контроле, позволяют оценить знания, умения и владения навыками/опытом деятельности обучающихся при освоении дисциплины. Для чего преподаватель находит среднюю оценку уровня сформированности компетенций у обучающегося, как сумму всех полученных оценок деленную на число этих оценок.

Шкала и критерии оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета по результатам текущего контроля

Средняя оценка уровня сформированности компетенций по результатам текущего контроля	Оценка
Оценка не менее 3,0 и нет ни одной неудовлетворительной оценки по текущему контролю	«зачтено»
Оценка менее 3,0 или получена хотя бы одна неудовлетворительная оценка по текущему контролю	«не зачтено»

Если оценка уровня сформированности компетенций обучающегося не соответствует критериям получения зачета, то обучающийся сдает зачет. Зачет проводится в форме собеседования по перечню вопросов. Перечень вопросов разного уровня сложности обучающиеся получают в начале семестра через электронную информационно-образовательную среду ИрГУПС (личный кабинет обучающегося).

Примеры вопросов тестирования

1. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

A. сотрудники;
B. хакеры;
C. атакующие;
D. контрагенты (лица, работающие по договору).

2. Что такое политики безопасности?

A. пошаговые инструкции по выполнению задач безопасности;
B. общие руководящие требования по достижению определенного уровня безопасности;
C. широкие, высокоуровневые заявления руководства;
D. детализированные документы по обработке инцидентов безопасности.

3. Что представляет собой стандарт ISO/IEC 27799?

A. стандарт по защите персональных данных о здоровье;
B. новая версия BS 17799;
C. определения для новой серии ISO 27000;
D. новая версия NIST 800-60.

4. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:

A. гаммирования;
B. подстановки;
C. кодирования;
D. перестановки;
E. аналитических преобразований.

5. Искусственные угрозы безопасности информации вызваны:

A. деятельностью человека;
B. ошибками при проектировании ОИС, ее элементов или разработке программных компонентов;
C. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
корыстными устремлениями злоумышленников;
E. ошибками при действиях персонала.

Критерии оценки результатов тестирования:

– оценка «зачтено» выставляется обучающемуся, если он набрал 70% при ответах на вопросы теста;

– оценка «незачтено» выставляется обучающемуся, если он набрал менее 70% при ответах на вопросы теста.