ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

УТВЕРЖДЕНА
приказом ректора
от «31» мая 2024 г. № 425-1

Б1.В.ДВ.06.01 Информационная безопасность открытых систем

рабочая программа дисциплины

Специальность/направление подготовки – 10.03.01 Информационная безопасность
Специализация/профиль – Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)
Квалификация выпускника – Бакалавр
Форма и срок обучения – очная форма 4 года
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 2
Часов по учебному плану (УП) – 72
В том числе в форме практической подготовки (ПП) – 18
(очная)

Формы промежуточной аттестации
очная форма обучения:
зачет 8 семестр

Очная форма обучения **Распределение часов дисциплины по семестрам**

Семестр	8	**Итого**
Вид занятий	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*	48/18	**48/18**
– лекции	24	**24**
– практические (семинарские)		
– лабораторные	24/18	**24/18**
Самостоятельная работа	24	**24**
Итого	72/18	**72/18**

* В форме ПП – в форме практической подготовки.

ИРКУТСК

Рабочая программа дисциплины разработана в соответствии с федеральным государственным образовательным стандартом высшего образования – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность, утвержденным Приказом Министерства науки и высшего образования Российской Федерации от 17.11.2020 № 1427.

Программу составил(и):
Старший преподаватель кафедры ИСиЗИ, П.Н. Наседкин

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «Информационные системы и защита информации», протокол от «21» мая 2024 г. № 11

Зав. кафедрой, к. э. н, доцент Т.К. Кириллова

1 ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ	
1.1 Цели 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 дисциплины	
1	ознакомить учащихся с основами построения защищенных ОИС
2	познакомить учащихся с базовыми уязвимостями и угрозами информационной безопасности (ИБ) ОИС
3	обучение учащихся различным подходам и методам обеспечения информационной безопасности
1.3 Цель воспитания и задачи воспитательной работы в рамках 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 психологии 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	
Блок/часть ОПОП	Блок 1. Дисциплины / Часть, формируемая участниками образовательных отношений
2.1 Дисциплины и практики, на которых основывается изучение данной дисциплины	
1	Б1.В.ДВ.02.01 Защита и обработка конфиденциальных документов
2	Б1.В.ДВ.07.01 Экономика защиты информации
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б2.В.02(Пд) Производственная - преддипломная практика
2	Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы
3	Б3.02(Д) Защита выпускной квалификационной работы

3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ТРЕБОВАНИЯМИ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ		
Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения**
ПК-2 Способен использовать методы обеспечения работоспособности систем защиты информации	ПК-2.1 Организует настройки средств защиты информации в автоматизированных системах	Знать: принципы и стандарты построения современных ОИС и подходы к интеграции сетей в ОИС; основные методы и средства реализации удаленных сетевых атак на ОИС; комплексный подход к построению эшелонированной защиты для ОИС; основные уязвимости и угрозы ИБ для ОИС; основные тенденции и закономерности развития средств и методов защиты информации в ОИС ;основные понятия администрирования подсистемы информационной безопасности; политики безопасности и меры защиты в ОИС
		Уметь: анализировать текущее состояние ИБ на предприятии с целью разработки требований к защищенным ОИС; определять и устранять основные угрозы ИБ для ОИС; выявлять и устранять уязвимости в основных компонентах ОИС; обнаруживать, прерывать и предотвращать удаленные сетевые атаки по их характерным признакам; применять стандартные решения для защиты информации в ОИС и

		квалифицированно оценивать их качество; реализовывать системы защиты информации в ОИС в соответствии со стандартами по оценке защищенных систем; применять комплексный подход к обеспечению ИС для ОИС; осуществлять управление и администрирование защищенных ОИС; администрировать подсистемы информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей; строить модели угроз и нарушителя ИБ для ОИС; проектировать защищенные ОИС; используя современные методы и средства, разрабатывать политику ИБ для ОИС
		Владеть: навыками распознавания сетевых атак на ОИС; навыками администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей; терминологией и системным подходом построения защищенных ОИС; навыками анализа угроз ИБ и уязвимостей в ОИС; навыками разработки политик ИБ для ОИС

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
1.0	**Раздел 1. Основные элементы технологии открытых информационных систем.**						
1.1	Тема 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.	8	2			2	ПК-2.1
1.2	Тема 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.	8	2			2	ПК-2.1
1.3	Лабораторная работа № 1. Исследование нормативно-правовой базы информационной безопасности предприятия.	8			4/4		ПК-2.1
2.0	**Раздел 2. Уязвимости открытых систем. Атаки на открытые системы.**						
2.1	Тема 3. 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.	8	2			2	ПК-2.1
2.2	Тема 4. Уязвимость открытых систем. Слабости системных утилит, команд и сетевых сервисов.	8	2			2	ПК-2.1
2.3	Тема 5. Классические и современные методы, используемые нападающим для проникновения в открытые системы. 1. Перехват данных и обнаружение прослушивающих приложений. 2. Мониторинг в графических интерфейсах. 3. Подмена системных утилит. 4. Атаки с использованием сетевых протоколов.(358)	8	2			2	ПК-2.1
2.4	Тема 6. Слабости современных технологий программирования. Ошибки в программном обеспечении. Сетевые вирусы.	8	2			2	ПК-2.1
2.5	Лабораторная работа № 2. Примеры политик безопасности. Политика использования ресурсов интранета. Политика в отношении паролей. Политика	8			4/4		ПК-2.1

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ							
Код	**Наименование разделов, тем и видов работ**	**Очная форма**					***Код индикатора достижения компетенции**
		Семестр	**Часы**				
			Лек	**Пр**	**Лаб**	**СР**	
	шифрования. Антивирусная политика. Политика оценки рисков. Политика аудита. Политика для программных маршрутизаторов. Политика удаленного доступа.						
2.6	Лабораторная работа № 3. 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.	8			4/4		ПК-2.1
3.0	**Раздел 3. Обеспечение информационной безопасности в открытых системах.**						
3.1	Тема 7. 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.	8	2			2	ПК-2.1
3.2	Тема 8. Межсетевые экраны. Функции межсетевых экранов. Руководящий документ Гостехкомиссии России по межсетевым экранам. Профили защиты для межсетевых экранов. Типы межсетевых экранов. Основные компоненты межсетевого экрана.	8	2			2	ПК-2.1
3.3	Тема 9. 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.	8	2			2	ПК-2.1
3.4	Тема 10. Сервисы безопасности (идентификация/аутентификация, разграничение доступа, экранирование, шифрование, управление и др.).	8	2			2	ПК-2.1
3.5	Тема 11. 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.	8	2			2	ПК-2.1
3.6	Тема 12. Стандартные протоколы построения ВЧВС. Виды ВЧВС в зависимости от решаемых задач. Топологии ВЧВС. Виртуальные локальные вычислительные сети.	8	2			2	ПК-2.1
3.7	Лабораторная работа № 4. Схемы подключения межсетевых экранов. Слабости межсетевых экранов. Выбор реализаций межсетевых экранов.	8			6/3		ПК-2.1
3.8	Лабораторная работа № 5. Исследование поточных и блочных алгоритмов шифрования. Использование хэш-функций.	8			6/3		ПК-2.1
	Форма промежуточной аттестации – зачет	8					ПК-2.1
	Итого часов (без учёта часов на промежуточную аттестацию)		24		24/18	24	

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 оформлен в виде приложения № 1 к рабочей программе дисциплины и размещен 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

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.1.1	Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Юрайт, 2023. — 349 с. — URL: https://urait.ru/bcode/511890 (дата обращения: 22.04.2024). — Текст : электронный.	Онлайн
6.1.1.2	Гвоздева, Т. В. Проектирование информационных систем. Стандартизация : учебное пособие / Т. В. Гвоздева, Б. А. Баллод. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 252 с. — URL: https://e.lanbook.com/book/169810 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн
6.1.1.3	Милославская, Н. Г. Сетевые атаки на открытые системы на примере Интранета : учебное пособие для вузов / Н. Г. Милославская. — Москва : НИЯУ МИФИ, 2012. — 64 с. — URL: http://e.lanbook.com/books/element.php?pl1_id=75789 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн
6.1.1.4	Кудряшов, В.А. Открытые информационные системы и сети : Учебное иллюстрированное пособие для студентов вузов, техникумов и колледжей железнодорожного транспорта / рец.: А. А. Черников [и др.]. — Москва : Издательство УМК МПС России, 2001. — 43 с. — URL: https://umczdt.ru/books/1201/18665/ (дата обращения: 26.04.2024). — Текст : электронный.	Онлайн

6.1.2 Дополнительная литература

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.2.1	Истомин, Е. П. Вычислительные системы, сети и телекоммуникации : учебник / Е. П. Истомин, С. Ю. Неклюдов, А. А. Чертков ; Рос. гос. гидрометеорolог. ун-т. — СПб. : Андреев. издат. дом, 2007. — 255 с. — Текст : непосредственный.	1
6.1.2.2	Череватова, Т. Ф. Нормативное обеспечение в сфере информационных технологий и систем : учебное пособие для вузов / Т. Ф. Череватова. — 2-е изд., стер. — Санкт-Петербург : Лань, 2023. — 84 с. — URL: https://e.lanbook.com/book/349997 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн

6.1.3 Учебно-методические разработки (в т. ч. для самостоятельной работы обучающихся)

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.3.1	Наседкин П.Н. Методические указания по изучению дисциплины Б1.В.ДВ.06.01 Информационная безопасность открытых систем по направлению подготовки 10.03.01 Информационная безопасность, профиль: Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности) / П.Н. Наседкин ; ИрГУПС. – Иркутск : ИрГУПС, 2024. – 13 с. - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_47526_1480_2024_1_signed.pdf	Онлайн

6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»

6.2.1	Электронная библиотека Учебно-методического центра по образованию на железнодорожном транспорте «ЭБ УМЦ ЖДТ» — https://umczdt.ru/books/
6.2.2	Электронно-библиотечная система «Издательство Лань», https://e.lanbook.com/
6.2.3	Электронно-библиотечная система «Образовательная платформа ЮРАЙТ», https://urait.ru/

6.3 Программное обеспечение и информационные справочные системы

6.3.1 Базовое программное обеспечение

6.3.1.1	Microsoft Windows Professional 10, государственный контракт от 20.07.2021 № 0334100010021000013-01
6.3.1.2	Microsoft Office Russian 2010, государственный контракт от 20.07.2021 № 0334100010021000013-01
6.3.1.3	FoxitReader, свободно распространяемое программное обеспечение http://free-software.com.ua/pdf-viewer/foxit-reader/

6.3.1.4	Adobe Acrobat Reader DC свободно распространяемое программное обеспечение https://get.adobe.com/ru/reader/enterprise/
6.3.1.5	Яндекс. Браузер. Прикладное программное обеспечение общего назначения, Офисные приложения, лицензия – свободно распространяемое программное обеспечение по лицензии BSD License
6.3.2 Специализированное программное обеспечение	
6.3.2.1	https://docs.python.org/3/license.html
6.3.2.2	Dev-C++, свободная интегрированная среда разработки приложений для языков программирования C/C++, https://code-live.ru/post/dev-cpp-free-cpp-ide-for-windows/
6.3.2.3	MatLab Classroom, R2015a, R2015b, контракт от 09.07.2014 № 0334100010014000028-0000756-01.
6.3.2.4	MatLab Classroom, R2010a, R2010b, лицензия от 16.03.2011 № 689810, ГК № 0334100010011000032-00000756-01. Прогр.средство защиты от НСД Secret Net4.0, клиент серв.безоп. Secret Net 4.0, сервер безопасности С Secret Net4.0, система разгр.доступа Dallas Lock 7.0
6.3.2.5	MathCAD_student 15.0 Academic_License, Customer Number 434692, контракт от 03.12.2012 № 0334100010012000148-0000756-01
6.3.2.6	Python 3.9, свободно распространяемое программное обеспечение https://docs.python.org/3/license.html
6.3.2.9	MatLab Classroom, R2010a, R2010b, лицензия от 16.03.2011 № 689810, ГК № 0334100010011000032-00000756-01.
6.3.3 Информационные справочные системы	
6.3.3.1	Не предусмотрены
6.4 Правовые и нормативные документы	
6.4.1	Не предусмотрены

7 ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ УЧЕБНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

1	Корпуса А, Б, В, Г, Д, Е ИрГУПС находятся по адресу г. Иркутск, ул. Чернышевского, д. 15; корпус Л ИрГУПС находится – по адресу г. Иркутск, ул. Лермонтова, д.80
2	Учебная аудитория Д-521 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор, экран, (ноутбук переносной)
3	Лаборатория Д-523 «Моделирование и разработка программных систем и защита информации».«Безопасность программно-аппаратных средств защиты информации» для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор (переносной), экран (переносной), компьютер измеритель шумов и вибрации 003-МЗ
4	Учебная аудитория Д-518 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации Основное оборудование: специализированная мебель, мультимедиапроектор, экран, (ноутбук переносной)
5	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; – помещения для хранения и профилактического обслуживания учебного оборудования – А-521

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Лекция (от латинского «lection» – чтение) – вид аудиторных учебных занятий. Лекция: закладывает основы научных знаний в систематизированной, последовательной, обобщенной форме; раскрывает состояние и перспективы развития соответствующей области науки и техники; концентрирует внимание обучающихся на наиболее сложных, узловых вопросах; стимулирует познавательную активность обучающихся.

	Во время лекционных занятий обучающийся должен уметь сконцентрировать внимание на изучаемых проблемах и включить в работу все виды памяти: словесную, образную и моторно-двигательную. Для этого весь материал, излагаемый преподавателем, обучающемуся необходимо конспектировать. На полях конспекта следует помечать вопросы, выделенные обучающимся для консультации с преподавателем. Выводы, полученные в виде формул, рекомендуется в конспекте подчеркивать или обводить рамкой, чтобы лучше запоминались. Полезно составить краткий справочник, содержащий определения важнейших понятий лекции. К каждому занятию следует разобрать материал предыдущей лекции. Изучая материал по учебнику или конспекту лекций, следует переходить к следующему вопросу только в том случае, когда хорошо усвоен предыдущий вопрос. Ряд вопросов дисциплины может быть вынесен на самостоятельное изучение. Такое задание требует оперативного выполнения. В конспекте лекций необходимо оставить место для освещения упомянутых вопросов. 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
Практическое занятие	Практическое занятие – вид аудиторных учебных занятий, целенаправленная форма организации учебного процесса, при реализации которой обучающиеся по заданию и под руководством преподавателя выполняют практические задания. Практические задания направлены на углубление научно-теоретических знаний и овладение определенными методами работы, в процессе которых вырабатываются умения и навыки выполнения тех или иных учебных действий в данной сфере науки. Практические занятия развивают научное мышление и речь, позволяют проверить знания обучающихся, выступают как средства оперативной обратной связи; цель практических занятий – углублять, расширять, детализировать знания, полученные на лекции, в обобщенной форме и содействовать выработке навыков профессиональной деятельности. На практических занятиях подробно рассматриваются основные вопросы дисциплины, разбираются основные типы задач. К каждому практическому занятию следует заранее самостоятельно выполнить домашнее задание и выучить лекционный материал к следующей теме. Систематическое выполнение домашних заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины
Лабораторная работа	Основной целью лабораторных работ является теоретическое обоснование, наглядное и/или экспериментальное подтверждение и/или проверка существенных теоретических положений (законов, закономерностей) анализ существующих методик и методов их реализации и т.д. Они занимают преимущественное место при изучении дисциплин обязательной части и части, формируемой участниками образовательных отношений Блока 1. Исходя из цели, содержанием лабораторных работ могут быть: - экспериментальная проверка формул, методик расчета; - проведение натурных измерений свойств, рабочих параметров, режимов работы при помощи лабораторного оборудования и/или стендов и макетов; - ознакомление, анализ и теоретические выкладки по устройству, принципу действия и способам обслуживания аппаратов, деталей машин, механизмов, процессов, протекающих в них при этом и т.д.; - наглядная графическая интерпретация чертежей, схем, объемных поверхностей и т.д., воспроизводимых с помощью специализированного программного обеспечения; - имитационное моделирование процессов, протекающих в сложных химических, физических, механических, электрических и пр. объектах; - наглядное представление о работе персонала конкретной организации или подразделения ОАО «РЖД» посредством моделирования штатных и внештатных ситуаций в виртуальных специализированных АРМ (автоматизированных рабочих мест); - установление и подтверждение закономерностей (путем сравнения проведенного эксперимента и рассчитанных значений) и т.д.; - ознакомление с методиками проведения экспериментов, наглядным устройством стенд-макетов и пр.; - установление свойств веществ, их качественных и количественных характеристик; - анализ различных характеристик процессов, в том числе производственных и иных процессов; - расчет параметров различных явлений и процессов, смоделировать которые не возможно в реальных условиях (например, чрезвычайные ситуации и пр.); - наблюдение развития явлений, процессов и др. Допускается иное содержание лабораторных работ, если это будет способствовать реализации целей и задач дисциплины и формированию соответствующих компетенций. По характеру выполняемых лабораторных работ возможны:

	- ознакомительные работы, используемые для закрепления изученного теоретического материалы; - аналитические работы, используемые для получения новой информации на основе формализованных методов; - творческие работы, ориентированные на самостоятельный выбор подходов решения задач. Прежде, чем приступить к лабораторным занятиям, обучающимся необходимо повторить теоретический материал по теме работы. Каждая лабораторная работа оснащена методическими указаниями, разработанными преподавателями, ведущими дисциплину
Самостоятельная работа	Обучение по дисциплине «Информационная безопасность открытых систем» предусматривает активную самостоятельную работу обучающегося. В разделе 4 рабочей программы, который называется «Структура и содержание дисциплины», все часы самостоятельной работы расписаны по темам и вопросам, а также указана необходимая учебная литература: обучающийся изучает учебный материал, разбирает примеры и решает разноуровневые задачи в рамках выполнения как общих домашних заданий, так и индивидуальных домашних заданий (ИДЗ) и других видов работ, предусмотренных рабочей программой дисциплины. При выполнении домашних заданий обучающемуся следует обратиться к задачам, решенным на предыдущих практических занятиях, решенным домашним работам, а также к примерам, приводимым лектором. Если этого будет недостаточно для выполнения всей работы можно дополнительно воспользоваться учебными пособиями, приведенными в разделе 6.1 «Учебная литература». Если, несмотря на изученный материал, задание выполнить не удается, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия, и/или консультацию лектора. Домашние задания, индивидуальные домашние задания и другие работы, предусмотренные рабочей программой дисциплины должны быть выполнены обучающимся в установленные преподавателем сроки в соответствии с требованиями к оформлению текстовой и графической документации, сформулированным в Положении «Требования к оформлению текстовой и графической документации. Нормоконтроль»
Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины (модуля), размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет	

Приложение № 1 к рабочей программе

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации

1. Общие положения

Фонд оценочных средств (ФОС) является составной частью нормативно-методического обеспечения системы оценки качества освоения обучающимися образовательной программы.

Фонд оценочных средств предназначен для использования обучающимися, преподавателями, администрацией ИрГУПС, а также сторонними образовательными организациями для оценивания качества освоения образовательной программы и уровня сформированности компетенций у обучающихся.

Задачами ФОС являются:

– оценка достижений обучающихся в процессе изучения дисциплины;

– обеспечение соответствия результатов обучения задачам будущей профессиональной деятельности через совершенствование традиционных и внедрение инновационных методов обучения в образовательный процесс;

– самоподготовка и самоконтроль обучающихся в процессе обучения.

Фонд оценочных средств сформирован на основе ключевых принципов оценивания: валидность, надежность, объективность, эффективность.

Для оценки уровня сформированности компетенций используется трехуровневая система:

– минимальный уровень освоения, обязательный для всех обучающихся по завершению освоения образовательной программы; дает общее представление о виде деятельности, основных закономерностях функционирования объектов профессиональной деятельности, методов и алгоритмов решения практических задач;

– базовый уровень освоения, превышение минимальных характеристик сформированности компетенций; позволяет решать типовые задачи, принимать профессиональные и управленческие решения по известным алгоритмам, правилам и методикам;

– высокий уровень освоения, максимально возможная выраженность характеристик компетенций; предполагает готовность решать практические задачи повышенной сложности, нетиповые задачи, принимать профессиональные и управленческие решения в условиях неполной определенности, при недостаточном документальном, нормативном и методическом обеспечении.

2. Перечень компетенций, в формировании которых участвует дисциплина.
Программа контрольно-оценочных мероприятий.
Показатели оценивания компетенций, критерии оценки

Дисциплина «Информационная безопасность открытых систем» участвует в формировании компетенций:

ПК-2. Способен использовать методы обеспечения работоспособности систем защиты информации

Программа контрольно-оценочных мероприятий очная форма обучения

№	Наименование контрольно-оценочного мероприятия	Объект контроля	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
8 семестр				
1.0	**Раздел 1. Основные элементы технологии открытых информационных систем**			
1.1	Текущий контроль	Тема 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.	ПК-2.1	Собеседование (устно)
1.2	Текущий контроль	Тема 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.	ПК-2.1	Собеседование (устно)
1.3	Текущий контроль	Лабораторная работа № 1. Исследование нормативно-правовой базы информационной безопасности предприятия.	ПК-2.1	Лабораторная работа (письменно/устно) В рамках ПП**: Лабораторная работа (письменно/устно)
2.0	**Раздел 2. Уязвимости открытых систем. Атаки на открытые системы**			
2.1	Текущий контроль	Тема 3. 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.	ПК-2.1	Собеседование (устно)
2.2	Текущий контроль	Тема 4. Уязвимость открытых систем. Слабости системных утилит, команд и сетевых сервисов.	ПК-2.1	Собеседование (устно)
2.3	Текущий контроль	Тема 5. Классические и современные методы, используемые нападающим для проникновения в открытые системы. 1. Перехват данных и обнаружение прослушивающих	ПК-2.1	Собеседование (устно)

		приложений. 2. Мониторинг в графических интерфейсах. 3. Подмена системных утилит. 4. Атаки с использованием сетевых протоколов.(358)		
2.4	Текущий контроль	Тема 6. Слабости современных технологий программирования. Ошибки в программном обеспечении. Сетевые вирусы.	ПК-2.1	Собеседование (устно)
2.5	Текущий контроль	Лабораторная работа № 2. 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.	ПК-2.1	Лабораторная работа (письменно/устно) В рамках ПП**: Лабораторная работа (письменно/устно)
2.6	Текущий контроль	Лабораторная работа № 3. 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.	ПК-2.1	Лабораторная работа (письменно/устно) В рамках ПП**: Лабораторная работа (письменно/устно)
3.0	**Раздел 3. Обеспечение информационной безопасности в открытых системах**			
3.1	Текущий контроль	Тема 7. 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.	ПК-2.1	Собеседование (устно)
3.2	Текущий контроль	Тема 8. Межсетевые экраны. Функции межсетевых экранов. Руководящий документ Гостехкомиссии России по межсетевым экранам. Профили защиты для межсетевых экранов. Типы межсетевых экранов. Основные компоненты межсетевого экрана.	ПК-2.1	Собеседование (устно)
3.3	Текущий контроль	Тема 9. 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.	ПК-2.1	Собеседование (устно)

3.4	Текущий контроль	Тема 10. Сервисы безопасности (идентификация/аутентификация, разграничение доступа, экранирование, шифрование, управление и др.).	ПК-2.1	Собеседование (устно)
3.5	Текущий контроль	Тема 11. 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.	ПК-2.1	Собеседование (устно)
3.6	Текущий контроль	Тема 12. Стандартные протоколы построения ВЧВС. Виды ВЧВС в зависимости от решаемых задач. Топологии ВЧВС. Виртуальные локальные вычислительные сети.	ПК-2.1	Собеседование (устно)
3.7	Текущий контроль	Лабораторная работа № 4. Схемы подключения межсетевых экранов. Слабости межсетевых экранов. Выбор реализаций межсетевых экранов.	ПК-2.1	Лабораторная работа (письменно/устно) В рамках ПП**: Лабораторная работа (письменно/устно)
3.8	Текущий контроль	Лабораторная работа № 5. Исследование поточных и блочных алгоритмов шифрования. Использование хэш-функций.	ПК-2.1	Лабораторная работа (письменно/устно) В рамках ПП**: Лабораторная работа (письменно/устно)
	Промежуточная аттестация	Все разделы	ПК-2.1	Зачет (собеседование) Зачет - тестирование (компьютерные технологии)

*Форма проведения контрольно-оценочного мероприятия: устно, письменно, компьютерные технологии.
**ПП – практическая подготовка

Описание показателей и критериев оценивания компетенций.
Описание шкал оценивания

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.

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. Результаты оценивания учитываются в виде средней оценки при проведении промежуточной аттестации.

Для оценивания результатов обучения используется четырехбалльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и двухбалльная шкала: «зачтено», «не зачтено».

Перечень оценочных средств, используемых для оценивания компетенций, а также краткая характеристика этих средств приведены в таблице.

Текущий контроль

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	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. Может быть использовано для оценки знаний обучающихся	Вопросы для собеседования по темам/разделам дисциплины
2	Лабораторная работа	Средство, позволяющее оценить умение обучающегося письменно/устно излагать суть поставленной задачи, самостоятельно применять стандартные методы решения поставленной задачи с использованием имеющейся лабораторной базы, проводить анализ полученного результата работы. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся	Образец задания для выполнения лабораторной работы и примерный перечень вопросов для ее защиты

Промежуточная аттестация

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Зачет	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень теоретических вопросов и практических заданий к зачету
2	Тест – промежуточная аттестация в форме зачета	Система автоматизированного контроля освоения компетенций (части компетенций) обучающимся по дисциплине (модулю) с использованием информационно-коммуникационных технологий. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий

Критерии и шкалы оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета. Шкала оценивания уровня освоения компетенций

Шкала оценивания	Критерии оценивания	Уровень освоения компетенции
«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
	Обучающийся с небольшими неточностями ответил на теоретические вопросы. Показал 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	Базовый
	Обучающийся с существенными неточностями ответил на теоретические вопросы. Показал удовлетворительные знания в рамках учебного материала. С существенными неточностями выполнил	Минимальный

	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	
«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	Компетенция не сформирована

Тест – промежуточная аттестация в форме зачета

Шкала оценивания	Критерии оценивания
«зачтено»	Обучающийся верно ответил на 70 % и более тестовых заданий при прохождении тестирования
«не зачтено»	Обучающийся верно ответил на 69 % и менее тестовых заданий при прохождении тестирования

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Собеседование

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Глубокое и прочное усвоение программного материала. Полные, последовательные, грамотные и логически излагаемые ответы при видоизменении задания. Обучающийся свободно справляется с поставленными задачами, может обосновать принятые решения, демонстрирует владение разносторонними навыками и приемами выполнения практических работ
«хорошо»		Знание программного материала, грамотное изложение, без существенных неточностей в ответе на вопрос, правильное применение теоретических знаний, владение необходимыми навыками при выполнении практических задач
«удовлетворительно»		Обучающийся демонстрирует усвоение основного материала, при ответе допускаются неточности, при ответе недостаточно правильные формулировки, нарушение последовательности в изложении программного материала, затруднения в выполнении практических заданий Слабое знание программного материала, при ответе возникают ошибки, затруднения при выполнении практических работ
«неудовлетворительно»	«не зачтено»	Не было попытки выполнить задание

Лабораторная работа

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Лабораторная работа выполнена в обозначенный преподавателем срок, письменный отчет без замечаний. Лабораторная работа выполнена обучающимся в полном объеме с соблюдением необходимой последовательности. Обучающийся работал полностью самостоятельно; показал необходимые для проведения работы теоретические знания, практические умения и навыки. Работа (отчет) оформлена аккуратно, в наиболее оптимальной для фиксации результатов форме
«хорошо»		Лабораторная работа выполнена в обозначенный преподавателем срок, письменный отчет с небольшими недочетами. Лабораторная работа выполнена обучающимся в полном объеме и самостоятельно. Допущены отклонения от необходимой последовательности выполнения, не влияющие на правильность конечного результата. Работа показывает знание обучающимся основного теоретического материала и овладение умениями, необходимыми для самостоятельного выполнения работы.

		Допущены неточности и небрежность в оформлении результатов работы (отчета)
«удовлетворительно»		Лабораторная работа выполнена с задержкой, письменный отчет с недочетами. Лабораторная работа выполняется и оформляется обучающимся при посторонней помощи. На выполнение работы затрачивается много времени. Обучающийся показывает знания теоретического материала, но испытывает затруднение при самостоятельной работе с источниками знаний или приборами
«неудовлетворительно»	«не зачтено»	Лабораторная работа не выполнена, письменный отчет не представлен. Результаты, полученные обучающимся, не позволяют сделать правильных выводов и полностью расходятся с поставленной целью. Показывается плохое знание теоретического материала и отсутствие необходимых умений. Лабораторная работа не выполнена, у учащегося отсутствуют необходимые для проведения работы теоретические знания, практические умения и навыки

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности

3.1 Типовые контрольные задания для проведения собеседования

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типовых вариантов заданий для проведения собеседований.

Образец типового варианта вопросов для проведения собеседования

«Тема 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.»

1. Какие основные элементы включает в себя технология открытых информационных систем?
2. Что такое совместимость открытых систем и почему она важна для их функционирования?
3. Какие модели открытых систем существуют, и как они помогают в понимании взаимодействия между системами?

Образец типового варианта вопросов для проведения собеседования

«Тема 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.»

1. Какова структура интранета, и как она отличается от других типов информационных систем?
2. Какие этапы необходимо пройти для создания интранета, и какие этапы разработки он включает?
3. Как интранет связан с понятиями экстранета и портала, и как они дополняют друг друга?

Образец типового варианта вопросов для проведения собеседования

«Тема 3. 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.»

1. Какие уязвимости могут существовать в архитектуре клиент-серверных систем, и как они могут быть использованы злоумышленниками?
2. Какие угрозы представляют уязвимости операционных систем, серверов и рабочих станций в открытых системах?
3. Какие меры могут быть предприняты для защиты от угроз, связанных с уязвимостями открытых систем?

Образец типового варианта вопросов для проведения собеседования
«Тема 4. Уязвимость открытых систем. Слабости системных утилит, команд и сетевых сервисов.»

1. Какие примеры слабостей системных утилит и команд могут быть найдены в операционных системах?
2. Какие могут быть последствия использования слабостей системных утилит и команд злоумышленниками?
3. Каким образом сетевые сервисы могут стать объектом атак, и какие уязвимости они могут иметь?

Образец типового варианта вопросов для проведения собеседования
«Тема 5. Классические и современные методы, используемые нападающим для проникновения в открытые системы. 1. Перехват данных и обнаружение прослушивающих приложений. 2. Мониторинг в графических интерфейсах. 3. Подмена системных утилит. 4. Атаки с использованием сетевых протоколов.(358)»

1. Какие методы используются злоумышленниками для перехвата данных и обхода механизмов защиты?
2. Какие виды атак могут быть осуществлены через мониторинг графических интерфейсов и подмену системных утилит?
3. Как можно обнаружить и предотвратить атаки с использованием сетевых протоколов?

Образец типового варианта вопросов для проведения собеседования
«Тема 6. Слабости современных технологий программирования. Ошибки в программном обеспечении. Сетевые вирусы.»

1. Какие типичные ошибки в программном обеспечении могут стать причиной уязвимостей?
2. Какие методы существуют для обнаружения и устранения ошибок в программном коде?
3. Как сетевые вирусы могут быть использованы злоумышленниками для атак на информационные системы?

Образец типового варианта вопросов для проведения собеседования
«Тема 7. 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.»

1. Что представляет собой четырехуровневая модель открытой системы, и какие уровни она включает?
2. Какие специфические методы и меры безопасности могут быть использованы для защиты ресурсов открытых систем, в частности, интранета?
3. Как выбор сетевой топологии влияет на безопасность интранета при подключении к другим внешним сетям?

Образец типового варианта вопросов для проведения собеседования «Тема 8. Межсетевые экраны. Функции межсетевых экранов. Руководящий документ Гостехкомиссии России по межсетевым экранам. Профили защиты для межсетевых экранов. Типы межсетевых экранов. Основные компоненты межсетевого экрана.»

1. Какие функции выполняют межсетевые экраны, и почему они важны для безопасности сетей?
2. Какие руководящие документы регламентируют работу межсетевых экранов
3. Какие типы межсетевых экранов существуют, и в чем заключается их специфика?
4. Какие компоненты составляют основу межсетевого экрана, и как они взаимодействуют для обеспечения безопасности сети?
5. Какие профили защиты могут быть установлены для межсетевых экранов, и как они влияют на общую безопасность сети?

Образец типового варианта вопросов для проведения собеседования «Тема 9. 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.»

1. Как можно создать комплексную систему обеспечения безопасности открытых систем, и какие элементы она включает?
2. Как происходит управление безопасностью открытых систем, и какие методы могут быть использованы для обеспечения безопасности?
3. Какие рекомендации могут быть предложены для обеспечения информационной безопасности открытых систем, учитывая основные угрозы и уязвимости?

Образец типового варианта вопросов для проведения собеседования «Тема 10. Сервисы безопасности (идентификация/аутентификация, разграничение доступа, экранирование, шифрование, управление и др.).»

1. Какие основные сервисы безопасности используются для защиты открытых информационных систем, и как они работают?
2. Какие методы и протоколы применяются для реализации идентификации и аутентификации пользователей в открытых системах?
3. Каким образом шифрование данных и управление доступом способствуют обеспечению безопасности информации в открытых системах?

Образец типового варианта вопросов для проведения собеседования «Тема 11. 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.»

1. В чем заключается понятие виртуальных частных вычислительных сетей, и какие задачи они решают?
2. Какие существуют стандартные протоколы для построения виртуальных частных сетей, и как они обеспечивают защиту информации?
3. Какие проблемы и уязвимости могут возникнуть при использовании современных виртуальных вычислительных сетей, и как их можно решить?

Образец типового варианта вопросов для проведения собеседования «Тема 12. Стандартные протоколы построения ВЧВС. Виды ВЧВС в зависимости от решаемых задач. Топологии ВЧВС. Виртуальные локальные вычислительные сети.»

1. Какие виды виртуальных частных сетей существуют, и как они отличаются по функциональности и применению?
2. Какие топологии могут быть использованы при построении виртуальных частных сетей, и как они влияют на общую безопасность сети?
3. Как виртуальные локальные вычислительные сети способствуют защите информации и обеспечивают ее конфиденциальность?

3.2 Типовые задания для выполнения лабораторной работы и примерный перечень вопросов для ее защиты

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типовых вариантов заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 1. Исследование нормативно-правовой базы информационной безопасности предприятия.»

Задания:

1. Изучите нормативные документы, регулирующие информационную безопасность на предприятии.
2. Определите ключевые требования к защите информации, установленные нормативными актами.
3. Проанализируйте соответствие действующих положений и реализованных на предприятии мер по обеспечению информационной безопасности.

Вопросы для защиты:

— Какие нормативно-правовые акты регулируют информационную безопасность на предприятии?
— Какие основные требования к защите информации установлены в этих актах?
— Какие меры по обеспечению информационной безопасности реализованы на предприятии?

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 2. 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.»

Задания:

1. Изучите примеры политик безопасности, охватывающих различные аспекты информационной безопасности.
2. Опишите политику использования ресурсов интранета, включая правила доступа к веб-сайтам, загрузке файлов и обмену информацией.
3. Разработайте политику в отношении паролей, определяющую требования к созданию, хранению и использованию паролей сотрудниками.
4. Определите политику шифрования, устанавливающую требования к использованию шифрования для защиты конфиденциальной информации в хранилищах данных и при передаче данных по сети.

5. Разработайте антивирусную политику, определяющую процедуры по обнаружению, предотвращению и удалению вирусов на компьютерах и серверах.
6. Подготовьте политику оценки рисков, определяющую методы и критерии оценки уязвимостей и потенциальных угроз информационной безопасности.
7. Разработайте политику аудита, определяющую процедуры мониторинга и анализа событий безопасности для обнаружения инцидентов.
8. Определите политику для программных маршрутизаторов, устанавливающую правила фильтрации трафика и защиты сетевой инфраструктуры.
9. Разработайте политику удаленного доступа, устанавливающую правила и процедуры для безопасного подключения к корпоративной сети извне.

Примерные вопросы для защиты:

— Какие основные элементы должны быть включены в политику использования ресурсов интранета?
— Какие требования должны предъявляться к паролям согласно политике безопасности?
— Какие методы шифрования могут использоваться в соответствии с политикой шифрования?
— Какие шаги предпринимаются в рамках антивирусной политики для защиты от вредоносных программ?
— Какие основные шаги включает в себя процесс оценки рисков в соответствии с политикой оценки рисков?
— Какие меры предусмотрены в политике аудита для обнаружения и реагирования на инциденты безопасности?
— Какие правила фильтрации трафика применяются к программным маршрутизаторам в соответствии с политикой для программных маршрутизаторов?
— Какие методы удаленного доступа разрешены согласно политике удаленного доступа, и какие меры безопасности применяются к такому доступу?

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 3. 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.»

Задания:

1. Изучите примеры политик безопасности, охватывающих различные аспекты информационной безопасности.
2. Разработайте политику подключения подразделений к интранету, устанавливающую процедуры и правила для безопасного подключения к корпоративной сети.
3. Определите политику для обеспечения конфиденциальности информации, включая правила классификации данных, механизмы шифрования и контроль доступа.
4. Разработайте политику для безопасности веб-сервера, определяющую конфигурацию сервера, правила аутентификации и авторизации, а также меры защиты от атак.
5. Определите политику пересылки электронной почты, включающую требования к безопасности при передаче конфиденциальной информации по электронной почте.
6. Разработайте политику для подключения новых устройств к интранету, определяющую процедуры регистрации, аутентификации и проверки на безопасность новых устройств.

Примерные вопросы для защиты:

— Какие основные правила и процедуры предусмотрены в политике подключения подразделений к интранету?
— Какие меры безопасности применяются в политике для обеспечения

конфиденциальности информации?
- Какие конфигурационные параметры включены в политику безопасности веб-сервера?
- Какие механизмы аутентификации используются в политике для веб-сервера?
- Какие меры безопасности применяются при пересылке конфиденциальной информации по электронной почте в соответствии с политикой?
- Какие процедуры предусмотрены в политике для подключения новых устройств к интранету, и какие проверки проходят новые устройства перед разрешением доступа к сети?

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты
«Лабораторная работа № 4. Схемы подключения межсетевых экранов. Слабости межсетевых экранов. Выбор реализаций межсетевых экранов.»

Задания:

1. Изучите схемы подключения межсетевых экранов.
2. Определите основные слабости межсетевых экранов.
3. Выберите подходящие реализации межсетевых экранов.

Вопросы для защиты:

- Какие типы схем подключения межсетевых экранов существуют?
- Какие уязвимости могут присутствовать у межсетевых экранов?
- Какие критерии следует учитывать при выборе реализации межсетевого экрана?

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты
«Лабораторная работа № 5. Исследование поточных и блочных алгоритмов шифрования. Использование хэш-функций.»

Задания для лабораторной работы № 5:
1. Изучите принципы работы поточных и блочных алгоритмов шифрования.
2. Проведите исследование поточных алгоритмов шифрования, включая их особенности, преимущества и недостатки.
3. Проведите исследование блочных алгоритмов шифрования, оценив их эффективность и стойкость к атакам.
4. Изучите принципы работы хэш-функций и их применение в криптографии.
5. Оцените эффективность и безопасность различных хэш-функций при использовании в различных криптографических протоколах и приложениях.

Примерные вопросы для защиты:

- В чем основные различия между поточными и блочными алгоритмами шифрования?
- Какие алгоритмы относятся к поточным шифрам, и как они работают?
- Какие алгоритмы относятся к блочным шифрам, и каковы основные этапы их работы?
- Какие криптографические характеристики важны при выборе хэш-функции для конкретного приложения?
- Какие методы атаки могут быть использованы для взлома блочных алгоритмов шифрования?
- Какие существуют стандартные хэш-функции, и для каких целей они обычно используются?

3.3 Типовые контрольные задания для проведения тестирования

Фонд тестовых заданий по дисциплине содержит тестовые задания, распределенные по разделам и темам, с указанием их количества и типа.

Структура фонда тестовых заданий по дисциплине

Индикатор достижения компетенции	Тема в соответствии с РПД	Характеристика ТЗ	Количество тестовых заданий, типы ТЗ
ПК-2.1	Тема 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.	Знание	2 – ОТЗ 1 – ЗТЗ
		Умение	2 – ОТЗ 1 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ПК-2.1	Тема 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.	Знание	2 – ОТЗ 1 – ЗТЗ
		Умение	2 – ОТЗ 1 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ПК-2.1	Тема 3. 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.	Знание	2 – ОТЗ 1 – ЗТЗ
		Умение	2 – ОТЗ 1 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ПК-2.1	Тема 4. Уязвимость открытых систем. Слабости системных утилит, команд и сетевых сервисов.	Знание	2 – ОТЗ 1 – ЗТЗ
		Умение	2 – ОТЗ 1 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ПК-2.1	Тема 5. Классические и современные методы, используемые нападающим для проникновения в открытые системы. 1. Перехват данных и обнаружение прослушивающих приложений. 2. Мониторинг в графических интерфейсах. 3. Подмена системных утилит. 4. Атаки с использованием сетевых протоколов.(358)	Знание	2 – ОТЗ 1 – ЗТЗ
		Умение	2 – ОТЗ 1 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ПК-2.1	Тема 6. Слабости современных технологий программирования. Ошибки в программном обеспечении. Сетевые вирусы.	Знание	2 – ОТЗ 1 – ЗТЗ
		Умение	2 – ОТЗ 1 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ПК-2.1	Тема 7. 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.	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ПК-2.1	Тема 8. Межсетевые экраны. Функции межсетевых экранов. Руководящий документ Гостехкомиссии России по межсетевым экранам. Профили защиты для межсетевых экранов. Типы межсетевых экранов. Основные компоненты межсетевого экрана.	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ПК-2.1	Тема 9. Средства обеспечения информационной безопасности в открытых системах. Создание комплексной системы обеспечения безопасности открытых систем. Управление безопасности открытых систем. Рекомендации по	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ

	обеспечению информационной безопасности открытых систем.	Действие	0 – ОТЗ 0 – ЗТЗ
ПК-2.1	Тема 10. Сервисы безопасности (идентификация/аутентификация, разграничение доступа, экранирование, шифрование, управление и др.).	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ПК-2.1	Тема 11. 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.	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ПК-2.1	Тема 12. Стандартные протоколы построения ВЧВС. Виды ВЧВС в зависимости от решаемых задач. Топологии ВЧВС. Виртуальные локальные вычислительные сети.	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
		Итого	36 – ОТЗ 24 – ЗТЗ

Полный комплект ФТЗ хранится в электронной информационно-образовательной среде ИрГУПС и обучающийся имеет возможность ознакомиться с демонстрационным вариантом ФТЗ.

Ниже приведен образец типового варианта итогового теста, предусмотренного рабочей программой дисциплины.

3.4 Перечень теоретических вопросов к зачету

(для оценки знаний)

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.

3.5 Перечень типовых простых практических заданий к зачету

(для оценки умений)

1 Диагностика заражения вредоносными программами.
2 Анализ сетевого трафика.
3 Удаленный контроль над станцией в сети.
4. Настройка политик информационной безопасности.
5. Настройка межсетевого экрана.
6. Организация и настройка виртуальной частной сети.

3.6 Перечень типовых практических заданий к зачету

(для оценки навыков и (или) опыта деятельности)

1 Диагностика заражения вредоносными программами.
2 Анализ сетевого трафика.
3 Удаленный контроль над станцией в сети.
4. Настройка политик информационной безопасности.
5. Настройка межсетевого экрана.
6. Организация и настройка виртуальной частной сети.

4. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности

В таблице приведены описания процедур проведения контрольно-оценочных мероприятий и процедур оценивания результатов обучения с помощью оценочных средств в соответствии с рабочей программой дисциплины.

Наименование оценочного	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения

средства	
Собеседование	Собеседование, предусмотренное рабочей программой дисциплины, проводится на практическом занятии. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся тему, вопросы для подготовки к собеседованию. Результаты собеседования преподаватель доводит до обучающихся сразу после завершения собеседования
Лабораторная работа	Защита лабораторных работ проводится во время лабораторных занятий. Во время проведения защиты лабораторной работы пользоваться учебниками, справочниками, конспектами лекций, тетрадями не разрешено. Преподаватель на лабораторной работе, предшествующей занятию проведения защиты лабораторной работы, доводит до обучающихся: номер защищаемой лабораторной работы, время на защиту лабораторной работы. Преподаватель информирует обучающихся о результатах защиты лабораторной работы сразу после ее контрольно-оценочного мероприятия

Для организации и проведения промежуточной аттестации составляются 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.

Перечень теоретических вопросов и типовые практические задания разного уровня сложности для проведения промежуточной аттестации обучающиеся получают в начале семестра через электронную информационно-образовательную среду ИрГУПС (личный кабинет обучающегося).

Описание процедур проведения промежуточной аттестации в форме зачета и оценивания результатов обучения

При проведении промежуточной аттестации в форме зачета преподаватель может воспользоваться результатами текущего контроля успеваемости в течение семестра. С целью использования результатов текущего контроля успеваемости, преподаватель подсчитывает среднюю оценку уровня сформированности компетенций обучающегося (сумма оценок, полученных обучающимся, делится на число оценок).

Шкала и критерии оценивания уровня сформированности компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета по результатам текущего контроля (без дополнительного аттестационного испытания)

Средняя оценка уровня сформированности компетенций по результатам текущего контроля	Шкала оценивания
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 без дополнительного аттестационного испытания, то промежуточная аттестация проводится в форме собеседования по перечню теоретических вопросов и типовых практических задач или в форме компьютерного тестирования.

Промежуточная аттестация в форме зачета с проведением аттестационного испытания проходит на последнем занятии по дисциплине.

При проведении промежуточной аттестации в форме компьютерного тестирования вариант тестового задания формируется из фонда тестовых заданий по дисциплине случайным образом, но с условием: 50 % заданий должны быть заданиями открытого типа и 50 % заданий – закрытого типа.