Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курганский государственный университет»
(КГУ)

Кафедра «Безопасность информационных и автоматизированных систем»

УТВЕРЖДАЮ:
Первый проректор
_____ /С.Н. Щербич/
«30» сентября 2019 г.

Рабочая программа учебной дисциплины

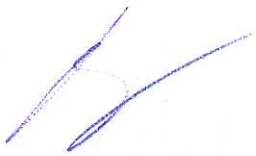
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОТКРЫТЫХ СИСТЕМ

образовательной программы высшего образования –
программы специалитета
10.05.03 Информационная безопасность автоматизированных систем
Направленность: (специализация№7) обеспечение информационной безопасности распределенных информационных систем
Форма обучения: очная

Курган 2019

Рабочая программа дисциплины «Информационная безопасность открытых систем» составлена в соответствии с учебным планом по программе специалитета «Информационная безопасность автоматизированных систем» (Обеспечение информационной безопасности распределенных информационных систем), утвержденным для очной формы обучения « 29 » августа 2019 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» 27 сентября 2019 года, протокол № 2.

Рабочую программу составил:
ст. преподаватель  В.В. Москвин

Согласовано:

Зав. кафедрой «БИАС»
канд. пед. наук, доцент  Е.Н. Полякова

Начальник Управления
образовательной деятельности  С.Н. Синицын

Специалист по учебно-методической
работе Учебно-методического
отдела  Г.В. Казанкова

1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 6 зачетных единицы трудоемкости (216 академических часа)

Очная форма обучения

Вид учебной работы	На всю дисциплину	Семестр
		7
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**80**	**80**
Лекции	32	32
Лабораторные работы	16	16
Практические занятия	32	32
Самостоятельная работа, всего часов в том числе:	**136**	**136**
Подготовка к экзамену	27	27
Другие виды самостоятельной работы (подготовка к практическим занятиям, лабораторным работам и рубежному контролю)	73	73
Курсовая работа	36	36
Вид промежуточной аттестации	**экзамен**	**экзамен**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**216**	**216**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Информационная безопасность открытых систем» относится к дисциплинам вариативной части по выбору Блока 1.

Изучение дисциплины базируется на результатах обучения, сформированных при изучении дисциплины «Основы информационной безопасности».

В свою очередь, данная дисциплина обеспечивает прохождение практик, а также подготовку выпускной квалификационной работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Учебная дисциплина «Информационная безопасность открытых систем» реализует требования федерального государственного образовательного стандарта высшего профессионального образования и является важной составляющей профессиональной подготовки специалистов в области обеспечения информационной безопасности.

Целью преподавания дисциплины «Информационная безопасность открытых систем» является формирование целостного представления об организации информационной безопасности открытых информационных систем, получение теоретических знаний о принципах построения и архитектуре открытых систем (в том числе распределенных), обеспечивающих организацию вычислительных процессов в корпоративных информационных системах экономического, управленческого, производственного, научного и другие назначения, а также практических навыков по созданию (настройке) конфигурации информационной системы для реализации бизнес процессов в корпоративных сетях предприятий.

Задачами дисциплины являются:

- раскрытие сущности, целей и задач открытых информационных систем;
- изучение и исследование механизмов обеспечения информационной безопасности в открытых информационных системах;
- знакомство с процессами обеспечения информационной безопасности в открытых информационных системах и освоение подходов их моделирования.

Компетенции, формируемые в результате освоения дисциплины:

– способность проводить анализ защищенности автоматизированных систем (ПК-3);

– способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);

– способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);

– способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23);

– способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели наруши-

теля информационной безопасности в распределенных информационных системах (ПСК-7.1)

– способность проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах (ПСК-7.2).

В результате изучения дисциплины обучающийся должен

знать:

- основные методы и средства реализации удаленных сетевых атак на открытые информационные системы (для ПК-20, ПК-23);
- политику безопасности и меры защиты в открытых информационных системах (для ПК-23, ПСК-7.1, ПСК-7.2);
- комплексный подход к построению эшелонированной защиты для открытых информационных систем (для ПК-3, ПК-23);

уметь:

- определять и устранять основные угрозы информационной безопасности для открытых информационных систем (для ПК-23, ПСК-7.1, ПСК-7.2);
- строить модель нарушителя информационной безопасности для открытых информационных систем (для ПК-4, ПСК-7.1, ПСК-7.2);
- реализовывать системы защиты информации в открытых информационных системах в соответствии со стандартами по оценке защищенных систем (для ПК-3,ПК-20);

владеть:

- терминологией и системным подходом построения защищенных открытых информационных систем (для ПК-3,ПК-23);
- навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах (для ПК-20, ПСК-7.1, ПСК-7.2).

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план. Очная форма обучения

Рубеж	Номер темы	Наименование темы	Количество часов контактной работы с преподавателем		
			Лекции	Практич. занятия	Лаборатор. работы
Семестр 7					
Рубеж 1	1	Стандартизация и модельное представление открытых информационных систем.	2	2	-
	2	Профили открытых систем. Интранет как открытая система.	4	6	-
	3	Уязвимость открытых систем на примере интранета.	4	-	10
	4	Атаки на открытые системы.	4	-	6
Рубеж 2	5	Обеспечение информационной безопасности в открытых системах.	6	20	-
	6	Аутентификация субъектов и объектов взаимодействия в открытых системах.	4	4	-

	7	Виртуальные вычислительные сети.	4	-	-
	8	Межсетевые экраны.	4	-	-
		Всего:	**32**	**32**	**16**

4.2. Содержание лекционных занятий

Тема 1.Стандартизация и модельное представление открытых информационных систем.

Понятие открытых систем. Основные элементы технологии открытых информационных систем. Совместимость открытых систем. Переносимость. Способность к взаимодействию. Методологический базис открытых систем. Эталонные модели среды и взаимосвязи открытых систем. Эталонная модель среды открытых систем (модель OSE). Базовая эталонная модель взаимосвязи открытых систем (модель OSI).

Международные структуры в области стандартизации открытых систем. Роль стандартов в технологии открытых систем. Основные группы стандартов и организации по стандартизации.

Тема 2. Профили открытых систем. Интранет как открытая система.

Понятие профиля открытой системы. Классификация профилей. Основные свойства и назначение профилей. Пример компоновки функционального профиля.

Понятие интранета. Интранет как часть среды открытых систем. Интранет и экстранет. Портал и интранет. Разработка и управление политикой использования ресурсов интранета.

3.Уязвимость открытых систем на примере интранета.

Основные понятия. Угрозы ресурсам интранета и причины их реализации. Анализ угроз ИБ ресурсам интранета и причины их реализации.

Уязвимости операционных систем, серверов, рабочих станций, каналов связи.

Уязвимость архитектуры клиент-сервер. Слабости системных утилит, команд и сетевых сервисов: Telnet, FTP, NFS, DNS, NIS, World Wide Web, Команды удаленного выполнения, Sendmail и электронная почта. Слабости современных технологий программирования.

Ошибки в программном обеспечении. Сетевые вирусы.

4.Атаки на открытые системы.

Атаки на открытые системы: анализ сетевого трафика, подмена доверенного объекта или субъекта, ложный объект, «отказ в обслуживании», удаленный контроль над станцией в сети.

Этапы реализации и уровни атак. Атаки с использованием сетевых протоколов. Удаленные атаки на открытые системы. Типичные сценарии и уровни атак.

Классические и современные методы, используемые нападающими для проникновения в открытые системы: перехват данных и обнаружение прослушивающих приложений, мониторинг в графических интерфейсах, подмена системных утилит, атаки с использованием сетевых протоколов.

5.Обеспечение информационной безопасности в открытых системах.

Четырехуровневая модель открытой системы. Специфика защиты ресурсов открытых систем на примере интранета. Выбор сетевой топологии интранета при подключении к другим внешним сетям. Принципы создания защищенных средств связи объектов в открытых системах. Создания защищенных средств связи объектов в открытых системах на основе стандартов ISO 7498-2, 17799, 15408. Разработка политики безопасности для открытых систем. Сервисы безопасности: идентификация/аутентификация, разграничение доступа, протоколирование и аудит, экранирование, туннелирование, шифрование, контроль целостности, контроль защищенности, обнаружение отказов и оперативное восстановление, управление. Средства обеспечения информационной безопасности в открытых системах. Создание комплексной системы обеспечения безопасности открытых систем.

6. Аутентификация субъектов и объектов взаимодействия в открытых системах.

Построение единых систем аутентификации, авторизации, персонализации, делегированного управления данными о субъектах и объектах и аудита доступа. Сетевая аутентификация – «первый рубеж» защиты открытой системы. Подсистема аутентификации. Российский рынок средств аутентификации.

Анализ типовой модели аутентификации.

7. Виртуальные вычислительные сети.

Определение виртуальных частных вычислительных сетей (ВЧВС). Цели и задачи построения ВЧВС. Специфика построения ВЧВС. Туннелирование в ВЧВС. Схема ВЧВС.

Политики безопасности для ВЧВС. Стандартные протоколы построения ВЧВС. Варианты построения ВЧВС. Виды ВЧВС в зависимости от решаемых задач: Intranet VPN, Client/server VPN, Extranet VPN, Remote Access VPN. Топологии ВЧВС.

VPN-консорциум о ВЧВС. Рекомендации специалистов по выбору решений для построения ВЧВС. Проблемы и уязвимости современных ВЧВС. Виртуальные локальные вычислительные сети.

8.Межсетевые экраны.

Системы анализа защищенности. Системы обнаружения и предотвращения вторжений Функции межсетевых экранов. Руководящий документ Гостехкомиссии России по межсетевым экранам. Профили защиты для межсетевых экранов. Типы межсетевых экранов. Основные компоненты межсетевого экрана. Схемы подключения межсетевых экранов. Слабости межсетевых экранов. Выбор реализаций межсетевых экранов.

Аудит и мониторинг информационной безопасности в открытых системах. Место и задачи систем анализа защищенности в защите открытых систем. Классификации систем анализа защищенности. Сетевые сканеры. Сканеры безопасности для приложений.

Критерии выбора сканеров безопасности. 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.

4.3 Практические занятия

Номер темы	Наименование темы	Наименование тем практических занятий	Норматив времени, час.
1	Стандартизация и модельное представление открытых информационных систем.	*Практическая работа №1.* Эталонные модели среды и взаимосвязи открытых систем	2
2	Интранет как открытая система.	*Практическая работа №2.* Сетевые технологии обработки данных. Основы компьютерной коммуникации	6
5	Обеспечение информационной безопасности в открытых системах	*Практическая работа №3.* Информационная безопасность открытых систем.	2
	1-ый рубежный контроль	***Контрольный опрос***	***2***
	Обеспечение информационной безопасности в открытых системах	*Практическая работа №4.* Концепции и аспекты обеспечения информационной безопасности	4
		Практическая работа №5-6. Принципы создания защищенных средств связи объектов в открытых системах.	6
		Практическая работа №7. Примеры политик безопасности	6
6	Аутентификация субъектов и объектов взаимодействия в открытых системах.	*Практическая работа №8.* Основы аутентификации	2
	2-ой рубежный контроль	***Презентация докладов***	***2***
	Итого		**32**

4.4. Лабораторные работы

Номер темы	Наименование темы	Наименование лабораторных работ	Норматив времени, час.
3	Уязвимость открытых систем на примере интранета.	*Лабораторная работа №1.* Уязвимость архитектуры клиент-сервер	2
		Лабораторная работа №2. Слабости системных утилит, команд и сетевых сервисов	2
		Лабораторная работа №3. Ошибки в программном обеспечении	2
		Лабораторная работа №4. Сетевые вирусы	4
4	Атаки на открытые системы	*Лабораторная работа №5.* Ложный объект	2
		Лабораторная работа №6. Подмена доверенного	2

		объекта или субъекта	
		Лабораторная работа №7. «Отказ в обслуживании»	2
	Итого:		**16**

4.5 Курсовая работа

Написание и защита курсовой работы «Построение защищенной информационной системы на основе выбранной модели среды открытых систем» является одним из вариантов завершения изучения курса «Информационная безопасность открытых систем». Выполнение курсовой работ способствует повышению теоретической и профессиональной подготовки студентов, а также лучшему усвоению учебного материала. Студент выбирает самостоятельно любое предприятие, самостоятельно готовит презентацию и выносит на обсуждение.

Результат работы оформляется в виде пояснительной записки, объемом 20-25 страниц.

Структура курсовой работы:

1) Титульный лист.
2) Оглавление (содержание) курсового проекта.
3) Введение.
4) Постановка задачи:
   а) исходные данные;
   б) цель курсовой работы;
   в) задачи, подлежащие рассмотрению (решению) в курсовой работе.
5) Содержательная часть (может быть в виде глав, разделов, параграфов, привязанных к задачам курсовой работы).
6) Заключение и выводы.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

При прослушивании лекций рекомендуется в конспекте отмечать все важные моменты, на которых заостряет внимание преподаватель, в частности те, которые направлены на качественное выполнение соответствующей лабораторной или практической работы.

Преподавателем запланировано использование при чтении лекций технологии учебной дискуссии. Поэтому рекомендуется фиксировать для себя интересные моменты с целью их активного обсуждения на дискуссии в конце лекции.

Залогом качественного выполнения лабораторных и практических работ является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Рекомендуется подготовить вопросы по неясным моментам и обсудить их с преподавателем в начале лабораторной или практической работы.

Преподавателем запланировано применение на практических и лабораторных занятиях технологий развивающейся кооперации, коллективного взаимодействия, разбора конкретных ситуаций.

Для текущего контроля успеваемости по очной форме обучения преподавателем используется балльно-рейтинговая система контроля и оценки академической активности. Поэтому настоятельно рекомендуется тщательно прорабатывать материал дисциплины при самостоятельной работе, участвовать во всех формах обсуждения и взаимодействия, как на лекциях, так и на практических и лабораторных занятиях в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает самостоятельное изучение разделов дисциплины, подготовку к лабораторным и практическим занятиям, к рубежным контролям, выполнение курсовой работы и подготовку к экзамену.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Самостоятельное изучение тем раздела	35
Стандартизация и модельное представление открытых информационных систем	4
Профили открытых систем. Интранет как открытая система	4
Уязвимость открытых систем на примере интранета	4
Атаки на открытые системы	5
Обеспечение информационной безопасности в открытых системах	6
Аутентификация субъектов и объектов взаимодействия в открытых системах	4
Виртуальные вычислительные сети	4
Межсетевые экраны	4
Подготовка к практическим занятиям (по 2 часа на тему)	16
Подготовка к лабораторным работам (по 2 часа на работу)	14
Подготовка к рубежным контролям (по 4 часа на каждый рубежный контроль)	8
Курсовая работа	36
Подготовка к экзамену	27
Всего:	***136***

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Перечень оценочных средств

1. Балльно-рейтинговая система контроля и оценки академической активности студентов в КГУ.
2. Отчеты студентов по лабораторным работам.
3. Отчеты студентов по практическим занятиям.
4. Курсовая работа.

5. Задания к рубежным контролям № 1, № 2.
5. Вопросы к экзамену.

6.2. Система балльно-рейтинговой оценки работы студентов по дисциплине

<table>
<tr><td>№</td><td>Наименование</td><td colspan="7">Содержание</td></tr>
<tr><td rowspan="4">1</td><td rowspan="4">Распределение баллов за семестры по видам учебной работы, сроки сдачи учебной работы (доводятся до сведения студентов на первом учебном занятии)</td><td colspan="7">Распределение баллов</td></tr>
<tr><td>Вид учебной работы:</td><td>Посещение лекций</td><td>Выполнение и защита отчетов по лабораторным работам</td><td>Выполнение практической работы</td><td>Рубежный контроль №1</td><td>Рубежный контроль №2</td><td>Экзамен</td></tr>
<tr><td>Балльная оценка:</td><td>$1_б$ x16=$16_б$</td><td>$3_б$ x 7 = $21_б$</td><td>$3_б$ x 8 =$24_б$</td><td>4</td><td>5</td><td>30</td></tr>
<tr><td colspan="7">Курсовая работа</td></tr>
<tr><td></td><td>Качество пояснительной записки</td><td>Качество программной части</td><td>Ритмичность выполнения</td><td>Качество защиты</td><td colspan="2">Всего</td></tr>
<tr><td></td><td>до 20</td><td>до 30</td><td>до 20</td><td>до 30</td><td colspan="2">100</td></tr>
<tr><td>2</td><td>Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и экзамена</td><td colspan="7">60 и менее баллов – неудовлетворительно; не зачтено;
61…73 – удовлетворительно; зачтено;
74… 90 – хорошо;
91…100 – отлично</td></tr>
<tr><td>3</td><td>Критерии допуска к промежуточной аттестации, возможности получения «автоматом» экзамена по дисциплине, возможность получения бонусных баллов</td><td colspan="7">Для допуска к промежуточной аттестации (экзамену) студент должен набрать по итогам текущего и рубежного контроля не менее 50 баллов и должен выполнить все лабораторные и практические работы.
Для получения экзаменационной оценки «удовлетворительно» «автоматически» студенту необходимо набрать 68 баллов.
По согласованию с преподавателем студенту, набравшему минимум 68 балл, могут быть добавлены дополнительные (бонусные) баллы за активность на практических занятиях и лабораторных работах, активное участие в научной и методической работе, оригинальность принятых решений в ходе выполнения практических и лабораторных работ, за участие в значимых учебных и внеучебных мероприятиях кафедры и выставлена за экзамен «автоматически» оценка «хорошо» или «отлично».</td></tr>
</table>

4	Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) студентов для получения недостающих баллов в конце семестра	В случае если к промежуточной аттестации (экзамену) набрана сумма менее 50 баллов, студенту необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. При этом необходимо проработать материал всех пропущенных лабораторных и практических работ. Формы дополнительных заданий (назначаются преподавателем): выполнение и защита пропущенной лабораторной или практической работы (при невозможности дополнительного проведения лабораторной или практической работы преподаватель устанавливает форму дополнительного задания по тематике пропущенной работы самостоятельно) – до 3 баллов. Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем.

6.3. Процедура оценивания результатов освоения дисциплины

1 рубежный контроль проводятся в форме письменных ответов на контрольные вопросы. Перед проведением рубежного контроля преподаватель прорабатывает со студентами основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии. На рубежный контроль студенту отводится 2 академических часа.

2-ой рубежный контроль проводится в виде презентации реферата по темам, предложенным преподавателем.

Преподаватель оценивает в баллах результаты рубежных контролей каждого студента и заносит в ведомость учета текущей успеваемости.

Экзамен проводится в традиционной форме, по билетам. Билет состоит из 2 вопросов. Вопросы к экзамену доводятся до студентов на последней лекции в семестре. Каждый вопрос оценивается в 15 баллов. На подготовку ответа студенту отводится 1 астрономический час.

Результаты текущего контроля успеваемости и экзамена заносятся преподавателем в экзаменационную ведомость, которая сдается в организационный отдел института в день экзамена, а также выставляются в зачетную книжку студента.

6.4. Примеры оценочных средств для рубежных контролей и экзамена

1-ый рубежный контроль

Примерные контрольные вопросы для письменного опроса

1. Как можно определить понятие «открытая информационная или программная система»?
2. Какими свойствами обладает открытая система?
3. Какие организации образуют структуру международной стандартизации в области информационных технологий?

4. Что составляет методологическую основу базиса открытых систем?
5. Каким образом определяют понятие «профиль открытой системы»?
6. Уязвимость открытых систем на примере интранета.

2-ой рубежный контроль

Подготовка рефератов студентами с презентацией на 5-7 минут. Подготовка и защита студентами рефератов по темам, не входящим в план лекций, позволяет расширить научный кругозор студентов, повысить навык работы с учебной и научной отечественной и зарубежной литературой, развить языковые навыки, повысить математическую подготовку, укрепить междисциплинарные связи, повысить навык программирования, развить навык систематизировать и свободно излагать перед аудиторией материал по заданной теме.

Примерный перечень рефератов:

1. Политика использования ресурсов интранета
2. Политика в отношении паролей
3. Политика шифрования
4. Антивирусная политика
5. Политика оценки рисков
6. Политика аудита
7. Политика для пограничных маршрутизаторов
8. Политика удаленного доступа
9. Политика построения виртуальных частных сетей
10. Политика для экстранета
11. Политика для оборудования пограничной демилитаризованной зоны
12. Политика подключения подразделений к интранету
13. Политика подключения к интранету с применением модема
14. Политика для конфиденциальной информации
15. Политика для веб-сервера
16. Политика пересылки электронной почты
17. Политика хранения электронной почты
18. Политика для межсетевых экранов
19. Политика специального доступа
20. Политика подключения новых устройств в интранет

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Основные элементы технологии открытых информационных систем
2. Совместимость открытых систем
3. Базовая модель информационной системы
4. Основные модели открытых систем
5. Понятие интранета. Структура интранета. Эталонная модель интранета.
6. Этапы создания интранета. Виды интранета. Стандарты создания интранета
7. Интранет как часть среды открытых систем
8. Интранет и экстранет
9. Портал и интранет
10. Угрозы ресурсам интранета и причины их реализации
11. Уязвимость архитектуры клиент-сервер

12. Слабости системных утилит, команд и сетевых сервисов
13. Сетевые вирусы
14. Удаленные атаки на открытые системы
15. Типичные сценарии и уровни атак
16. Классические и современные методы, используемые нападающими для проникновения в открытые системы
17. Четырехуровневая модель открытой системы
18. Специфика защиты ресурсов открытых систем на примере интранета
19. Выбор сетевой топологии интранета при подключении к другим внешним сетям
20. Принципы создания защищенных средств связи объектов в открытых системах
21. Сервисы безопасности
22. Средства обеспечения информационной безопасности в открытых системах
23. Управление безопасностью открытых систем
24. Организационно-правовые методы защиты открытых систем
25. Аутентификация субъектов и объектов взаимодействия в открытых системах
26. Виртуальные вычислительные сети
27. Системы анализа защищенности
28. Системы обнаружения и предотвращения вторжений

6.5. Фонд оценочных средств

Полный банк заданий для текущего, рубежных контролей и промежуточной аттестации по дисциплине, показатели, критерии, шкалы оценивания компетенций, методические материалы, определяющие процедуры оценивания образовательных результатов, приведены в учебно-методическом комплексе дисциплины.

7. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

7.1. Основная учебная литература

1. Мельников Д.А. Информационная безопасность открытых систем: учебник / Д.А. Мельников. – М.: Изд-во «Флинта», 2014. – 448с. Доступ из ЭБС «Консультант студента»

2. Милославская, Н.Г. Сетевые атаки на открытые системы на примере интранета: учебное пособие / Н.Г. Милославская. - М.: МИФИ, 2012. - 64 с.

3. М.И. Барабанова, В.И. Кияево. Информационные технологии: открытые системы, сети, безопасность в системах и сетях: Учебное пособие.– СПб.: Изд-во СПбГУЭФ, 2010. – 267 с.. Доступ из ЭБС «Консультант студента»

7.2 Дополнительная литература

1. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс: учебное пособие / А.Н. Андрончик, А.С. Коллеров, Н.И. Синадский, М.Ю. Щербаков ; Министерство образования и науки Российской Федерации, Уральский федеральный университет имени первого Президента России Б. Н. Ельцина ; под общ. ред. Н.И. Синадский. - Екатеринбург : Издательство Уральского университета, 2014. - 179 с.

Режим доступ: http://biblioclub.ru/index.php?page=book&id=275694

7.3 Учебно-методическая литература

1. Москвин В.В. Методические указания к практическим занятиям по дисциплине «Информационная безопасность открытых систем» для студентов очной формы обучения направлений 10.05.03 и 10.03.01. Курган, КГУ, 2017 – 7 с.

2. Москвин В.В. Методические указания к выполнению лабораторных работ по дисциплине «Информационная безопасность открытых систем» для студентов очной формы обучения направлений 10.05.03 и 10.03.01. Курган, КГУ, 2017 – 11 с.

8. РЕСУРСЫ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. ЭБС htt://www.iprbookshop.ru/
2. ЭБС htt://www.znanium.com/
3. ЭБС htt://www.studentlibrary.ru
4. http://nio.kgsu.ru/ Сайт КГУ. Научно-исследовательский отдел
5. http://window.edu.ru/. Единое окно доступа к образовательным ресурсам
6. http://elibrary.ru/. Научная электронная библиотека
7. http://dspace.kgsu.ru/xmlui/ Электронная библиотека КГУ

9. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

Информационно-справочная система «КонсультантПлюс».

При чтении лекций используются слайдовые презентации.

Минимальные требования к операционной системе и программному обеспечению компьютера, используемого при показе слайдовых презентаций: Windows XP, Libre Office.

Операционная система Windows;

Среда разработки MS Visual Studio;

СУБД MS SQL Server.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Переносной проектор BENQ PB6110 с экраном, локальная сеть компьютеров на базе Intel Core i3-2120 - 16 шт. с выходом в Internet, коммутатор 2-го уровня D-LINK DGS-101D/E1A.

ПРИЛОЖЕНИЕ 1

Аннотация к рабочей программе дисциплины

«Информационная безопасность открытых систем»

образовательной программы высшего образования –
программы специалитета

10.05.03 – Информационная безопасность автоматизированных систем

Направленность: (специализация №7)

Обеспечение информационной безопасности распределенных информационных систем

Трудоемкость дисциплины: 6 з.е. (216 академических часа)

*Семестр:*7 (очная форма обучения)

Форма промежуточной аттестации: экзамен

Содержание дисциплины. Основные разделы

Интеграция сетей в открытых информационных системах. Проектирование защищенных открытых информационных систем. Основные угрозы информационной безопасности для открытых информационных систем. Модель нарушителя информационной безопасности для открытых информационных систем. Сетевые протоколы и технологии передачи данных в открытых информационных системах. Уязвимость открытых информационных систем. Удаленные сетевые атаки. Методы и средства реализации удаленных сетевых атак на открытые информационные системы.