ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

УТВЕРЖДЕНА
приказ ректора
от «7» июня 2021 г. № 78

Б1.О.44 Информационная безопасность открытых систем

рабочая программа дисциплины

Специальность – *10.05.03 Информационная безопасность автоматизированных систем*
Специализация –*Специалист по защите информации*
Квалификация выпускника – Специалист
Форма и срок обучения – 5 лет 6 мес. очная форма;
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. –4
Часов по учебному плану (УП) –144

Формы промежуточной аттестации в семестрах/на курсах
очная форма обучения:
зачет 10,

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

Семестр	8	**Итого**
Число недель в семестре	17	
Вид занятий	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/ в форме ПП*	**85**	**85**
– лекции	34	34
– практические (семинарские)	17	17
– лабораторные	34	34
Самостоятельная работа	**59**	**59**
Экзамен		
Итого	**144**	**144**

* В форме ПП – в форме практической подготовки.

ИРКУТСК

Рабочая программа дисциплины разработана в соответствии с федеральным государственным образовательным стандартом высшего образования – магистратура по направлению подготовки 10.03.01 Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности), утверждённым приказом Минобрнауки России от 17.11.2020 г. № 1427.

Программу составил(и):
Ассистент _____ *А.С.Вергасов*

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «*ИСиЗИ*», протокол от «4» июня 2021 г №11/2

Зав. кафедрой*, канд. экон.наук* _____ *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	Привить учащимся основы культуры обеспечения информационной безопасности (ИБ) в ОИС.
2	Сформировать у обучающихся понимание основ построения защищенных ОИС.
3	Ознакомить учащихся с основными уязвимостями и угрозами ИБ характерными для современных ОИС.
4	Ознакомить учащихся с основными подходами и методами обеспечения ИБ ОИС.

1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины

Цель воспитания обучающихся – разностороннее развитие личности будущего конкурентоспособного специалиста с высшим образованием, обладающего высокой культурой, интеллигентностью, социальной активностью, качествами гражданина-патриота.
Задачи воспитательной работы с обучающимися:
– развитие мировоззрения и актуализация системы базовых ценностей личности;
– приобщение студенчества к общечеловеческим нормам морали, национальным устоям и академическим традициям;
– воспитание уважения к закону, нормам коллективной жизни, развитие гражданской и социальной ответственности как важнейшей черты личности, проявляющейся в заботе о своей стране, сохранении человеческой цивилизации;
– воспитание положительного отношения к труду, развитие потребности к творческому труду, воспитание социально значимой целеустремленности и ответственности в деловых отношениях;
– обеспечение развития личности и ее социально-психологической поддержки, формирование личностных качеств, необходимых для эффективной профессиональной деятельности;
– выявление и поддержка талантливых обучающихся, формирование организаторских навыков, творческого потенциала, вовлечение обучающихся в процессы саморазвития и самореализации;

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1 Требования к предварительной подготовке обучающегося

Б1.О.13 Информатика
Б1.О.30 Безопасность операционных систем
Б1.О.31 Безопасность сетей ЭВМ
Б1.О.32 Безопасность систем баз данных
Б1.О.48 Теоретические основы компьютерной безопасности
Б1.О.51 Кибербезопасность
Б1.О.54 Методы и средства криптографической защиты информации
Б1.О.55 Защита объектов критической информационной инфраструктуры

2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее

1	Б2.В.04(Н)	Производственная - научно-исследовательская работа
2	Б2.В.05(Пд)	Производственная - преддипломная
3	Б3.01(Д)	Подготовка к процедуре защиты выпускной квалификационной работы

3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ТРЕБОВАНИЯМИ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код и наименование	Код и наименование индикатора	Планируемые результаты обучения

компетенции	достижения компетенции	
ОПК.13 - Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем;	ОПК.13-1 Знает основы диагностики и тестирования систем защиты информации автоматизированных систем ОПК.13-3 Имеет базовые навыки проведения диагностики и тестирования систем защиты информации автоматизированных систем	Знать: - основные элементы технологии открытых информационных систем; - средства обеспечения информационной безопасности в открытых системах; - основные виды уязвимостей ОИС; - основные правила, процедуры, практические приемы, руководящие принципы, методы, средства для обеспечения информационной безопасности открытых информационных систем. Уметь: – анализировать текущее состояние информационной безопасности ОИС; – разрабатывать политику информационной безопасности ОИС; – внедрять и реализовывать политики ИБ для ОИС на практике, учитывая текущее состояние ОИС и возможности (ресурсы) хозяйствующего субъекта; Владеть: – методами оценки и анализа информационной безопасности ОИС; – опытом и знаниями по разработке политики информационной безопасности ОИС с учетом текущего состояния ОИС и возможности хозяйствующего субъекта - навыками количественной оценки уровня защищенности информационной системы, используя рейтинговые показатели, учитывающие распределение механизмов защиты по уровням иерархической модели средств защиты информации(СЗИ) и изменение вероятности достижения злоумышленником объекта защиты в зависимости от уровня СЗИ.;.
ОПК.5 - Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	ОПК.5-3 Имеет навыки оформления документов по организации защиты информации	Знать: - определение политики безопасности; основные требования к политике безопасности открытых информационных систем; – этапы выработки политики безопасности; содержание политики безопасности; типовые политики безопасности и меры защиты в ОИС; – порядок, способы и технологии внедрения политик информационной безопасности открытых информационных систем; Уметь: – ориентироваться в нормативно-правовой документации по обеспечению информационной безопасности открытой информационной системы, а также определять основные угрозы и уязвимости ОИС; - проверять соответствие обеспечения информационной безопасности ОИС, наличия и содержания документов, технической, правовой, организационно-распорядительной документации в области информационной безопасности; Владеть: – навыками планирования мероприятий (порядка выполнения работ) по реализации политики информационной безопасности открытых информационных системиаудита за проведением политики безопасности; - методами оценки и анализа информационной безопасности ОИС.

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ							
Код	**Наименование разделов, тем и видов работы**	**Семестр**	**Часы**				***Код индикатора достижения компетенции**
			Лек	**Пр**	**Лаб**	**СР**	
1.0	**Раздел 1. Основные элементы технологии открытых информационных систем.**	8	**4**		**4**		
1.1	Основные элементы технологии открытых информационных систем. Совместимость открытых систем. Переносимость и способность к взаимодействию. Базовая модель информационной системы. Расширение базовой модели информационной системы для взаимодействующих систем. Основные модели открытых систем. /Лек/	8	2				ОПК.13
1.2	Интранет как открытая система. Структура интранета. Эталонная модель интранета. Этапы создания интранета. Виды интранета. Стандарты интранета. Интранет как часть среды открытых систем. Интранет и экстранет . Портал и интранет. /Лек/	8	2				ОПК.13
1.3	Исследование нормативно-правовой базы информационной безопасности предприятия. /Лр/	8			*4*		ОПК.13
2.0	**Раздел 2. Уязвимости открытых систем. Атаки на открытые системы.**	8	**14**	**4**	**12**	**27**	
2.1	Уязвимость открытых систем. Основные понятия. Угрозы открытых систем (в том числе интранета) и причины их реализации. Уязвимости архитектуры клиент-сервер: уязвимости операционных систем; уязвимость серверов; уязвимость рабочих станций; уязвимость каналов связи. /Лек/	8	4				ОПК.13
2.2	*Удаленные атаки на открытые системы. Анализ сетевого трафика. Подмена доверенного объекта или субъекта. Ложный объект. Отказ в обслуживании. Удаленный контроль над станцией.* /Лр/	8			4		ОПК.13
2.3	Политика безопасности для открытых систем (определение, причины выработки, этапы и содержание, реализация и аудит политики безопасности). /Пр/	8		4			ОПК.13
2.4	Уязвимость открытых систем. Слабости системных утилит, команд и сетевых сервисов. /Лек/	8	4				ОПК.13
2.5	Классические и современные методы, используемые нападающим для проникновения в открытые системы. Перехват данных и обнаружение прослушивающих приложений. Мониторинг в графических интерфейсах. Подмена системных утилит. Атаки с использованием сетевых протоколов. /Лек/	8	4				ОПК.13
2.6	Примеры политик безопасности. Политика использования ресурсов интранета. Политика в отношении паролей. Политика шифрования. Антивирусная политика. Политика оценки рисков. Политика аудита. Политика для	8			4		ОПК.13

	программных маршрутизаторов. Политика удаленного доступа. /Лр/						
2.7	Слабости современных технологий программирования. Ошибки в программном обеспечении. Сетевые вирусы. /Лек/	8	2				ОПК.13
2.8	Типичные сценарии и уровни атак. Этапы реализации атак. Примеры некоторых атак. /Лр/	8			2		ОПК.13
2.9	Примеры политик безопасности. Политика подключения подразделений к интранету. Политика для конфиденциальной безопасности. Политика для веб-сервера. Политика пересылки электронной почты. Политика подключения новых устройств в интранет. /Лр/	8			2		ОПК.13 ОПК.5
2.10	Средства интранета. /Ср/	8				9	ОПК.13
2.11	Средства создания порталов. /Ср/	8				9	ОПК.13
2.12	Стандарты ISO по защите информации в открытых системах. /Ср/	8				9	ОПК.13 ОПК.5
	Раздел 3. Обеспечение информационной безопасности в открытых системах.	8	**16**	**13**	**18**	**32**	
3.1	Четырехуровневая модель открытой системы. Специфика защиты ресурсов открытых систем на примере интранета. Выбор сетевой топологии интранета при подключении к другим внешним сетям. Физическая изоляция. Изоляция протоколов. Выделенные каналы и маршрутизаторы. Принципы создания защищенных средств связи объектов в открытых системах. /Лек/	8	4				ОПК.13
3.2	Межсетевые экраны. Функции межсетевых экранов. Руководящий документ Гостехкомиссии России по межсетевым экранам. Профили защиты для межсетевых экранов. Типы межсетевых экранов. Основные компоненты межсетевого экрана. /Лек/	8	2				ОПК.13
3.3	Схемы подключения межсетевых экранов. Слабости межсетевых экранов. Выбор реализаций межсетевых экранов. /Лр/	8			4		ОПК.13
3.4	Средства обеспечения информационной безопасности в открытых системах. Создание комплексной системы обеспечения безопасности открытых систем. Управление безопасности открытых систем. Рекомендации по обеспечению информационной безопасности открытых систем. /Лек/	8	2				ОПК.13
3.5	Аутентификация субъектов и объектов взаимодействия в открытых системах. Сетевая аутентификация. Подсистема аутентификации. /Лр/	8			2		ОПК.13
3.6	Изучение российского рынка средств аутентификации. Сравнительный анализ средств аутентификации. /Пр/	8		5			ОПК.13
3.7	Сервисы безопасности (идентификация/аутентификация, разграничение	8	2				ОПК.13

	доступа, экранирование, шифрование, управление и др.). /Лек/						
3.8	Криптографическая защита в открытых системах. Основные понятия и методы криптографии. Стандартизация криптографических функций и механизмов. Криптографические протоколы. Криптографическая инфраструктура. Программные и аппаратные средства криптографической защиты. /Лр/	8			2		ОПК.13
3.9	Исследование поточных и блочных алгоритмов шифрования. Использование хэш-функций. /Лр/	8			4		ОПК.13
3.10	Виртуальные вычислительные сети. Определение виртуальных частных вычислительных сетей. Цели и задачи построения ВЧВС. Специфика построения ВЧВС. Туннелирование в ВЧВС. Схема ВЧВС. Политики безопасности для ВЧВС. Стандартные протоколы построения ВЧВС. Проблемы и уязвимости современных ВЧВС. /Лек/	8	4				ОПК.13
3.11	Системы анализа защищенности. Аудит и мониторинг информационной безопасности в открытых системах. Место и задачи систем анализа защищенности в защите открытых систем. Классификации систем анализа защищенности. Сетевые сканеры. Системные сканеры. Сканеры безопасности для приложений. Критерии выбора сканеров безопасности. /Лр/	8			2		ОПК.13
3.12	Работа с системой контроля защищенности (MaxPatrol – демо-версия). /Лр/	8			2		ОПК.13
3.13	Стандартные протоколы построения ВЧВС. Виды ВЧВС в зависимости от решаемых задач. Топологии ВЧВС. Виртуальные локальные вычислительные сети. /Лек/	8	2				ОПК.13
3.14	Системы обнаружения и предотвращения вторжений. Методы отражения вторжений. Основы построения систем обнаружения вторжений. Системное обнаружение вторжений. Сетевое обнаружение вторжений. Поведенческое обнаружение вторжений. Интеллектуальное обнаружение вторжений. Комплексное обнаружение вторжений. Выбор системы обнаружения вторжений. Развертывание системы обнаружения вторжений. Практика обнаружения вторжений. /Лр/	8			2		ОПК.13
3.15	Системы обнаружения атак, работающие в режиме реального времени. /Ср/	8				6	ОПК.13
3.16	Другие средства обеспечения безопасности в открытых системах. Защита от спама в электронной почте. Многофункциональные устройства защиты от сетевых атак. Системы анализа и управления рисками. Системы обеспечения информационной безопасности на уровне предприятия. /Ср/	8				6	ОПК.13 ОПК.5
3.17	Документы по основным протоколам для виртуальных частных сетей. Сравнительные характеристики ВЧВС-продуктов российских производителей. /Пр/	8		4			ОПК.13 ОПК.5

3.18	Зарубежные средства обеспечения информационной безопасности в сетях. /Пр/	8		4			ОПК.13
3.19	Подготовка докладов к семинарским занятиям. /Ср/	8				10	ОПК.13 ОПК.5
3.20	Проработка лекционного материала. Подготовка промежуточному контролю. /Ср/	8				4	ОПК.13 ОПК.5
4	Подготовка к зачету. /Ср/	8				6	ОПК.13 ОПК.5

* Код индикатора достижения компетенции проставляется или для всего раздела или для каждой темы или для каждого вида работы.

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

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по данной дисциплине 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

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
6.1.1.1	Диогенес Ю. , Озкайя Э.	Кибербезопасность. стратегия атак и обороны [Электронный ресурс] https://e.lanbook.com/book/131717	Москва : ДМК Пресс, 2020	100 % онлайн
6.1.1.2	Коллинз М.	Защита сетей. Подход на основе анализа данных [Электронный ресурс] https://e.lanbook.com/book/131682	Москва : ДМК Пресс, 2020.	100 % онлайн
6.1.1.3	Чио К. , Фримэн Д.	Машинное обучение и безопасность [Электронный ресурс] https://e.lanbook.com/book/131707	Москва : ДМК Пресс, 2020.	100 % онлайн

6.1.2 Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
6.1.2.1	Сафиуллина Л. Х., Касимова А. Р., Рябов Я. С., Садыков А. М., Богомолов В. А.	Информационная безопасность. Практические аспекты: учебник для вузов [Электронный ресурс] https://e.lanbook.com/book/161340	Петербург : Интермедия, 2021.	100 % онлайн
6.1.2.2	Булычев Г. Г.	Программно-аппаратные средства обеспечения информационной безопасности. Часть 2 [Электронный ресурс] https://e.lanbook.com/book/163812	Москва : РТУ МИРЭА, 2020.	100 % онлайн

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

	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/ 100% онлайн
6.1.3.1	Давидюк Н. В., Космачева И. М.	Мониторинг безопасности информационных систем: Практикум для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» и направлений 10.03.01 «Информационная безопасность», 10.04.01 «Информационная безопасность» [Электронный ресурс] https://e.lanbook.com/book/161352	Петербург : Интермедия, 2020.	100 % онлайн

6.1.3.2	Аршинский Л.В., Темникова Е.А.	Открытые информационные системы	Личный кабинет обучающегося	100 % онлайн

6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»	
6.2.1	Википедия: свободная энциклопедия. https://ru.wikipedia.org/wiki/Заглавная_страница
6.2..2	Национальный открытый университет ИНТУИТ http://www.intuit.ru
6.3 Программное обеспечение и информационные справочные системы	
6.3.1 Базовое программное обеспечение	
6.3.1.1	ОС Microsoft Windows 7 Professional, лицензия № 49379844, обновление - контракт №0334100010018000027-0000756-02 от 28.05.2018 АО СофтЛайн Трейд, обновление - контракт № 0334100010019000029-0000756-02 от 17.09.2019г. АО СофтЛайн Трейд, контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд Windows Edu Per Device 10 Education, Соглашение № V6760694, обновление - контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд
6.3.1.2	Офисный пакет Microsoft Office 2010, Лицензия № 48288083, обновление - контракт №0334100010018000027-0000756-02 от 28.05.2018 АО СофтЛайн Трейд, обновление - контракт № 0334100010019000029-0000756-02 от 17.09.2019г. АО СофтЛайн Трейд, обновление - контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд; Office Professional 2019 - Соглашение № V0709762, контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд; LibreOffice v. 5.2, свободно распространяемое ПО, https://ru.libreoffice.org
6.3.2 Специализированное программное обеспечение	
6.3.2.1	Firefox (браузер), (лицензия: бесплатно, количество: не ограничено).
6.3.2.2	MaxPatrol (демонстрационная версия), (лицензия: бесплатно, количество: не ограничено).
6.3.2.3	PacketTracer (лицензия: бесплатно, количество: не ограничено).
6.3.2.4	PEM (лицензия: бесплатно, количество: не ограничено).
6.3.2.5	Wireshark (лицензия: бесплатно, количество: не ограничено).
6.3.3 Информационные справочные системы	
6.3.3.1	Информационно-справочная система Консультант Плюс http://www.consultant.ru
6.4Правовые и нормативные документы	
6.4.1	Не предусмотрено

6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1 Основная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
6.1.1.1	Диогенес Ю. , Озкайя Э.	Кибербезопасность. стратегия атак и обороны [Электронный ресурс] https://e.lanbook.com/book/131717	Москва : ДМК Пресс, 2020	100 % онлайн
6.1.1.2	Коллинз М.	Защита сетей. Подход на основе анализа данных [Электронный ресурс] https://e.lanbook.com/book/131682	Москва : ДМК Пресс, 2020.	100 % онлайн
6.1.1.3	Чио К. , Фримэн Д.	Машинное обучение и безопасность [Электронный ресурс] http://biblioclub.ru/index.php?page= book&id =440285	Москва : ДМК Пресс, 2020.	100 % онлайн

6.1.2 Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
6.1.2.1	Сафиуллина Л. Х., Касимова А. Р., Рябов Я. С., Садыков А. М., Богомолов В. А.	Информационная безопасность. Практические аспекты: учебник для вузов [Электронный ресурс] https://e.lanbook.com/book/161340	Петербург : Интермедия, 2021.	100 % онлайн
6.1.2.2	Булычев Г. Г.	Программно-аппаратные средства обеспечения информационной безопасности.	Москва : РТУ МИРЭА, 2020.	100 % онлайн

		Часть 2 [Электронный ресурс] https://e.lanbook.com/book/163812		
6.1.3 Учебно-методические разработки (в т. ч. для самостоятельной работы обучающихся)				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/ 100% онлайн
6.1.3.1	Давидюк Н. В., Космачева И. М.	Мониторинг безопасности информационных систем: Практикум для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» и направлений 10.03.01 «Информационная безопасность», 10.04.01 «Информационная безопасность» [Электронный ресурс] https://e.lanbook.com/book/161352	Петербург : Интермедия, 2020.	100 % онлайн
6.1.3.2	Аршинский Л.В., Темникова Е.А.	Открытые информационные системы	Личный кабинет обучающегося	100 % онлайн
6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»				
6.2.1	Википедия: свободная энциклопедия. https://ru.wikipedia.org/wiki/Заглавная_страница			
6.2..2	Национальный открытый университет ИНТУИТ http://www.intuit.ru			
6.3 Программное обеспечение и информационные справочные системы				
6.3.1 Базовое программное обеспечение				
6.3.1.1	ОС Microsoft Windows 7 Professional, лицензия № 49379844, обновление - контракт №0334100010018000027-0000756-02 от 28.05.2018 АО СофтЛайн Трейд, обновление - контракт № 0334100010019000029-0000756-02 от 17.09.2019г. АО СофтЛайн Трейд, контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд Windows Edu Per Device 10 Education, Соглашение № V6760694, обновление - контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд		
6.3.1.2	Офисный пакет Microsoft Office 2010, Лицензия № 48288083, обновление - контракт №0334100010018000027-0000756-02 от 28.05.2018 АО СофтЛайн Трейд, обновление - контракт № 0334100010019000029-0000756-02 от 17.09.2019г. АО СофтЛайн Трейд, обновление - контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд; Office Professional 2019 - Соглашение № V0709762, контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд; LibreOffice v. 5.2, свободно распространяемое ПО, https://ru.libreoffice.org		
6.3.2 Специализированное программное обеспечение				
6.3.2.1	Firefox (браузер), (лицензия: бесплатно, количество: не ограничено).			
6.3.2.2	MaxPatrol (демонстрационная версия), (лицензия: бесплатно, количество: не ограничено).			
6.3.2.3	PacketTracer (лицензия: бесплатно, количество: не ограничено).			
6.3.2.4	PEM (лицензия: бесплатно, количество: не ограничено).			
6.3.2.5	Wireshark (лицензия: бесплатно, количество: не ограничено).			
6.3.3 Информационные справочные системы				
6.3.3.1	Информационно-справочная система Консультант Плюс http://www.consultant.ru			
6.4Правовые и нормативные документы				
6.4.1	Не предусмотрено			

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 – по адресу г. Иркутск, ул. Лермонтова, д.80.
2	*Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых проектов, работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническими средствами обучения (ноутбук, проектор, экран), служащими для представления учебной информации большой аудитории. Для проведения занятий лекционного типа имеются учебно-наглядные пособия (презентации, плакаты, таблицы), обеспечивающие тематические иллюстрации*

	содержания дисциплины. Помещения для хранения и профилактического обслуживания учебного оборудования – А-521.
3	*Учебная лаборатория «Средства и методы защиты информации», Д-523. Оснащена компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Перечень установленных программных средств: Microsoft Office 2010, Open Office 3.0.1, 7-zip, Borland Delphi 7, Abode Reader XI, Microsoft Security Essentials.*
4	Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Помещения для самостоятельной работы обучающихся: – читальные залы; – учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507.

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮДИСЦИПЛИНЫ

Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки. Обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии. Уделить внимание следующим понятиям (перечисление понятий) и др.
Лабораторная работа	Внимательно ознакомиться с целью, задачами и описанием лабораторной работы. Изучить теоретический материал, выполнить практическое задание, используя необходимые программные и аппаратно-технические средства, оформить отчет в соответствии с заданием и требованиями нормоконтроля. Ответить на вопросы по теме лабораторной работы. В ходе выполнения лабораторных работ раскрываются основные вопросы в рамках рассматриваемой темы, делаются акценты на наиболее сложные, проблемные и моменты изучаемого материала, которые должны быть приняты студентами во внимание. Особо выделяются аспекты важные для практической подготовки. Основной целью лабораторных занятий является расширение и углубление материала практического характера, контроль качества усвоения пройденного материала и ходом выполнения студентами заданий. При подготовке к зачету необходимо ориентироваться на лекции, результаты выполненных лабораторных работ и рекомендуемую литературу.
Самостоятельная работа	Эффективное освоение дисциплины предполагает самостоятельную внеаудиторную работу, которая включает в себя изучение предлагаемого в рабочей программе и самостоятельно найденного материала по соответствующим разделам и темам для дополнения конспектов лекций, подготовки к практическим занятиям и защиты лабораторных работ. Для более глубокого освоения дисциплины рекомендуется пользоваться учебной литературой, приведенной в рабочей программе дисциплины. Если какие-либо разделы и темы освоить не удается, а также возникают трудности в выполнении практических работ, необходимо пройти консультацию у преподавателя.
Тест	Тест – система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Итоговый тест по дисциплине включает 18 вопросов. Максимальное число баллов 100. Отводимое время на тест – 80 минут.
Конспект	Конспект – средство, позволяющее формировать и оценивать способность обучающегося к восприятию, обобщению и анализу информации. Основу конспекта составляет лекционный материал. Основа должна быть дополнена самостоятельно проработанным материалом. Конспект может быть использовано для оценки знаний и умений обучающихся. Преподаватель на лекции доводит до сведения обучающихся тему конспекта и указывает необходимую учебную литературу. Темы и перечень литературы выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Практические (семинарские) занятия	Обобщение, расширение и углубление пройденного материала на лекции. Решение задач на закрепление практических навыков. Выступление с докладами по заданной теме, формирование навыков самостоятельной работы, анализа литературных источников, публичного выступления и аргументации собственного мнения. Обсуждение вопросов, вызвавших затруднение, с преподавателем. Участие в дискуссиях и коллоквиумах. Контроль качества усвоения пройденного материала.
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.	

Лист регистрации дополнений и изменений рабочей программы дисциплины

№ п/п	Часть текста, подлежавшего изменению в документе	Общее количество страниц	Основание для внесения	Подпись отв. исп.	Дата

	№ раздела	№ пункта	№ подпункта	до внесения изменений	после внесения изменений	изменения, № документа		

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине *Б1.О.44 Информационная безопасность открытых систем*

Приложение № 1 к рабочей программе

Специальность – *10.05.03 Информационная безопасность автоматизированных систем*
Специализация – *Специалист по защите информации*

ИРКУТСК

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 Университета, а так же 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 (модуля)*

– 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 (модуль) «*Информационная безопасность открытых систем*» участвует в формировании компетенций:

ОПК.13-1 Знает основы диагностики и тестирования систем защиты информации автоматизированных систем

ОПК.13-3 Имеет базовые навыки проведения диагностики и тестирования систем защиты информации автоматизированных систем

ОПК.5-3 Имеет навыки оформления документов по организации защиты информации

Программа контрольно-оценочных мероприятий **очная форма обучения**

№	Неделя	Наименование	Объект контроля	Код индикатора	Наименование оценочного средства

		контрольно-оценочного мероприятия	(понятие/тем/раздел и т.д. дисциплины)	достижения компетенции	(форма проведения*)
8 семестр					
1	**2**	**3**	**4**	**5**	**6**
2	**1,2**	Текущий контроль	**Тема «Основные элементы технологии открытых информационных систем».**	ОПК.13-1 ОПК.13-3 ОПК.5-3	Конспект (письменно). Коллоквиум (интерактивная)
3	**2-17**	Текущий контроль	Тема « Основы информационной безопасности открытых информационных систем». Тема «Угрозы информационной безопасности открытых информационных систем». Тема «Уязвимости открытых систем на примере Intranet». Тема «Атаки на открытые системы». Тема «Обеспечение информационной безопасности в открытых системах». Тема «Законодательный уровень информационной безопасности. Политика безопасности».	ОПК.13-1 ОПК.13-3 ОПК.5-3	Сообщение, доклад и презентация (интерактивная)
4	**4**	Текущий контроль	**Тема «Интранет как открытая система».**	ОПК.13-1 ОПК.13-3 ОПК.5-3	Конспект (письменно)
5	**5**	Текущий контроль	**Тема «Уязвимости и угрозы открытых информационных систем».**	ОПК.13-1 ОПК.13-3 ОПК.5-3	Конспект (письменно). Коллоквиум (интерактивная)
6	**6**	Текущий контроль	**Тема «Классические и современные методы, используемые нападающим для проникновения в открытые системы».**	ОПК.13-1 ОПК.13-3 ОПК.5-3	Конспект (письменно)

7	**7**	Текущий контроль	**Тема «Четырехуровневая модель открытой системы. Специфика защиты ресурсов открытых систем на примере интранета».**	ОПК.13-1 ОПК.13-3 ОПК.5-3	Коллоквиум (интерактивная форма)
8	**8**	Текущий контроль	**Тема «Межсетевые экраны».**	ОПК.13-1 ОПК.13-3 ОПК.5-3	Конспект (письменно) Собеседование (устно)
9	**9**	Текущий контроль	Тема «Средства обеспечения информационной безопасности в открытых системах. Создание комплексной системы обеспечения безопасности открытых систем».	ОПК.13-1 ОПК.13-3 ОПК.5-3	Конспект (письменно). Коллоквиум (интерактивная)
10	**10**	Текущий контроль	Тема «Аутентификация субъектов и объектов взаимодействия в открытых системах».	ОПК.13-1 ОПК.13-3 ОПК.5-3	Собеседование (устно)
11	**11**	Текущий контроль	Тема «Криптографическая защита в открытых системах».	ОПК.13-1 ОПК.13-3 ОПК.5-3	Собеседование (устно)
12	**12**	Текущий контроль	Тема «Управление безопасности открытых систем».	ОПК.13-1 ОПК.13-3 ОПК.5-3	Конспект (письменно)
13	**14**	Текущий контроль	Тема «Системы анализа защищенности». Тема «Системы обнаружения и предотвращения вторжений».	ОПК.13-1 ОПК.13-3	Собеседование (устно)

				ОПК.5-3	
14	**15**	Текущий контроль	Тема Сервисы безопасности (идентификация/аутентификация, разграничение доступа, экранирование, шифрование, управление и др.)».	ОПК.13-1 ОПК.13-3 ОПК.5-3	Конспект (письменно)
15	**16**	Текущий контроль	Тема «Виртуальные вычислительные сети».	ОПК.13-1 ОПК.13-3 ОПК.5-3	Конспект (письменно) Собеседование (устно)
16	**17**	Промежуточный контроль – зачет	Раздел 1. Основные элементы технологии открытых информационных систем. Раздел 2. Уязвимости открытых систем. Атаки на открытые системы. Раздел 3. Обеспечение информационной безопасности в открытых системах.	ОПК.13-1 ОПК.13-3 ОПК.5-3	Собеседование (устно)

*Форма проведения контрольно-оценочного мероприятия: устно, письменно, компьютерные технологии.

Описание показателей и критериев оценивания компетенций.
Описание шкал оценивания

Контроль качества освоения дисциплины/прохождения практики 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/или двухбалльная шкала: «зачтено», «не зачтено».

Перечень оценочных средств, используемых для оценивания компетенций, а так же краткая характеристика этих средств приведены в таблице

№	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 по темам/разделам дисциплины
2	Коллоквиум	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися. Может быть использовано для оценки знаний обучающихся	Вопросы по темам/разделам дисциплины
3	Конспект	Средство, позволяющее формировать и оценивать способность обучающегося к восприятию, обобщению и анализу информации. Рекомендуется для оценки знаний и умений обучающихся	Темы конспектов по дисциплине
4	Сообщение, доклад и презентация	Продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы.	Темы докладов, сообщений.

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

Шкалы оценивания		Критерии оценивания	Уровень освоения компетенции
«отлично»	«зачтено»	Обучающийся правильно ответил на теоретические вопросы. Показал отличные знания в рамках учебного материала. Правильно выполнил практические задания. Показал отличные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на все дополнительные вопросы	Высокий
«хорошо»		Обучающийся с небольшими неточностями ответил на теоретические вопросы. Показал 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
«удовлетворительно»		Обучающийся с существенными неточностями ответил на теоретические вопросы. Показал удовлетворительные знания в рамках учебного материала. С существенными неточностями выполнил практические задания. Показал удовлетворительные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Допустил много неточностей при ответе на дополнительные вопросы	Минимальный
«неудовлетворительно»	«не зачтено»	Обучающийся при ответе на теоретические вопросы и при выполнении практических заданий продемонстрировал недостаточный уровень знаний и умений при решении задач в рамках учебного материала. При ответах на дополнительные вопросы было допущено множество неправильных ответов	Компетенция не сформирована

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Собеседование

Шкала оценивания	Критерии оценивания
«отлично»	*В ответе обучающегося отражены основные концепции и теории по данному вопросу, проведен их критический анализ и сопоставление, описанные теоретические положения иллюстрируются практическими примерами и экспериментальными данными. Обучающимся формулируется и обосновывается собственная точка зрения на заявленные проблемы, материал излагается профессиональным языком с использованием соответствующей системы понятий и терминов*
«хорошо»	*В ответе обучающегося описываются и сравниваются основные современные концепции и теории по данному вопросу, описанные теоретические положения иллюстрируются практическими примерами, обучающимся формулируется собственная точка зрения на заявленные проблемы, однако он испытывает затруднения в ее аргументации. Материал излагается профессиональным языком с использованием соответствующей системы понятий и терминов*
«удовлетворительно»	*В ответе обучающегося отражены лишь некоторые современные концепции и теории по данному вопросу, анализ и сопоставление этих теорий не проводится. Обучающийся испытывает значительные затруднения при иллюстрации теоретических положений практическими примерами. У обучающегося отсутствует собственная точка зрения на заявленные проблемы. Материал излагается профессиональным языком с использованием соответствующей системы понятий и терминов*
«неудовлетворительно»	*Ответ обучающегося не отражает современные концепции и теории по данному вопросу. Обучающийся не может привести практических примеров. Материал излагается «житейским» языком, не используются понятия и термины соответствующей научной области.* *Ответ отражает систему «житейских» представлений обучающегося на заявленную проблему, обучающийся не может назвать ни одной научной теории, не дает определения базовым понятиям*

Конспект

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

Сообщение, доклад и презентация

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

Коллоквиум

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

Оценочное средство «Тест».

Тестирование с применением компьютерных технологий проводится по окончанию каждого семестра (если дисциплина не является односеместровой) и по окончанию изучения дисциплины и (или) в течение года по завершению изучения дисциплины (контроль/проверка остаточных знаний, умений, навыков и (или) опыта деятельности).

Тесты формируются из фонда тестовых заданий по дисциплине. Структура фонда тестовых заданий по дисциплине, структуры тестов по итогам каждого семестра (если дисциплина не является односеместровой) и итогового теста по дисциплине и типовые примеры тестов приведены в разделе 3 данного документа.

Результаты тестирования могут быть использованы при проведении промежуточной аттестации, как в форме зачета, так и в форме экзамена.

Промежуточная аттестация в форме зачета:

Критерии оценивания	Шкала оценивания
Обучающийся набрал при тестировании более 69 баллов	«зачтено»
Обучающийся набрал при тестировании менее 69 баллов	«не зачтено»

Преподаватель вправе предусмотреть тесты для самоконтроля обучающихся по разделам дисциплины, сформировав их из материалов фонда тестовых заданий дисциплины. Требования к тестам для самоконтроля аналогичны требованиям к итоговым тестам по семестрам и дисциплине в целом.

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

Конспект

Типовые контрольные задания

Темы конспектов, предусмотренных рабочей программой дисциплины:

1. Основные элементы технологии открытых информационных систем.
   - 1.1 Совместимость открытых систем.
   - 1.2 Переносимость и способность к взаимодействию.
   - 1.3 Базовая модель информационной системы.
   - 1.4 Расширение базовой модели информационной системы для взаимодействующих систем.
   - 1.5 Основные модели открытых систем.
2. Интранет как открытая система.
   - 2.1 Структура интранета.
   - 2.2 Эталонная модель интранета.
   - 2.3 Этапы создания интранета.
   - 2.4 Виды интранета.
   - 2.5 Стандарты интранета.
   - 2.6 Интранет как часть среды открытых систем.
   - 2.7 Интранет и экстранет .
   - 2.8 Портал и интранет.
3. Уязвимость открытых систем. Основные понятия.
4. Угрозы открытых систем (в том числе интранета) и причины их реализации.
5. Уязвимости архитектуры клиент-сервер: уязвимости операционных систем; уязвимость серверов; уязвимость рабочих станций; уязвимость каналов связи.
6. Слабости системных утилит, команд и сетевых сервисов.
7. Классические и современные методы, используемые нападающим для проникновения в открытые системы.
   - 7.1 Перехват данных и обнаружение прослушивающих приложений.
   - 7.2 Мониторинг в графических интерфейсах.
   - 7.3 Подмена системных утилит.
   - 7.4 Атаки с использованием сетевых протоколов.
   - 7.5 Слабости современных технологий программирования.
   - 7.6 Ошибки в программном обеспечении.
   - 7.7 Сетевые вирусы.
8. Четырехуровневая модель открытой системы.
9. Специфика защиты ресурсов открытых систем на примере интранета.
10. Выбор сетевой топологии интранета при подключении к другим внешним сетям.
11. Физическая изоляция.
12. Изоляция протоколов.
13. Выделенные каналы и маршрутизаторы.
14. Принципы создания защищенных средств связи объектов в открытых системах.
15. Межсетевые экраны.
    - 15.1 Функции межсетевых экранов.
    - 15.2 Руководящий документ Гостехкомиссии России по межсетевым экранам.
    - 15.3 Профили защиты для межсетевых экранов.
    - 15. 4 Типы межсетевых экранов.
    - 15.5 Основные компоненты межсетевого экрана.
16. Создание комплексной системы обеспечения безопасности открытых систем.
17. Управление безопасности открытых систем.
18. Рекомендации по обеспечению информационной безопасности открытых систем.

19. Сервисы безопасности (идентификация/аутентификация, разграничение доступа, экранирование, шифрование, управление и др.).

20. Виртуальные вычислительные сети.

20.1 Определение виртуальных частных вычислительных сетей.

20.2 Цели и задачи построения ВЧВС.

20.3 Специфика построения ВЧВС.

20.4 Туннелирование в ВЧВС.

20.5 Схема ВЧВС.

20.6 Политики безопасности для ВЧВС.

20.7 Стандартные протоколы построения ВЧВС.

20.8 Проблемы и уязвимости современных ВЧВС.

20.9 Виртуальные локальные вычислительные сети.

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

Коллоквиум

Типовые контрольные задания

1. Основные принципы по созданию и функционированию информационно-телекоммуникационных систем.
2. Стратегия защиты информации. Основные признаки, по которым различают и формируют разные стратегии защиты.
3. Базовые сетевые технологии и масштабы сетей, в которых они применяются.
4. Возможные уровни взаимодействия открытых систем и их ответственность.
5. Классифицируйте и опишите угрозы безопасности информационной безопасности корпоративных информационных систем, а также их уязвимости.
6. Какие существуют способы защиты от угроз программно-математического воздействия.
7. Опишите программные средства администрирования.
8. Программные средства защиты от несанкционированного выполнения стандартных функций (чтения, записи, копирования, форматирования (и т.д.) информации)?
9. Программные и программно-аппаратные средства криптографической защиты?
10. Наиболее эффективные способы и средства защиты от сетевых атак. Сравните самые популярные из них.
11. Наиболее эффективные средства защиты от сбоев, отказов и ошибок. Сделайте сравнительный анализ.
12. Меры и средства защиты информации от утечки по побочным электромагнитным излучениям и наводкам.
13. Абстрактные теоретические принципы целостности данных в соответствии с Кларком и Вилсоном.
14. Опишите семь классов требований доверия (уверенности) по ГОСТ Р ИСО/МЭК 15/408.

Собеседование

Типовые контрольные задания

Тема «Аутентификация субъектов и объектов взаимодействия в открытых системах»

1. Какие подходы к аутентификации различают?
2. Что такое «однократная регистрация» и в каких ОИС она используется чаще всего?
3. В чем отличия аутентификации в однородных и гетерогенных клиент-серверных системах?
4. Опишите особенности четырех типовых моделей аутентификации: локальной, прямой, непрямой и автономной?

5. Рассмотрите парольную аутентификацию, ее достоинства и недостатки.
6. В чем достоинства и недостатки аутентификации по адресу?
7. Какие аппаратные средства аутентификации применяются в сетевой среде?
8. Каким образом задаются одноразовые пароли?:
9. Для чего и как используется аутентификация на основе электронной подписи?
10. Как реализуется аутентификация на прикладном уровне?
11. Расскажите о простейшем протоколе аутентификации PAP.
12. Каковы особенности протокола аутентификации «запрос-ответ» и в каких системах он используется?
13. Сравните протоколы RADIUS и TACACS/
14. В каких системах и как применяется протокол EAP?
15. Подробно опишите схему работы протокола Kerberos.
16. Что такое серверы аутентификации? На основе каких служб они работают?

Тема «Межсетевые экраны»

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

Тема «Криптографическая защита в открытых системах»

1. Основные задачи защиты ОИС, решаемы криптографическим методом.
2. Основные достоинства и недостатки, а также отличия симметричных и ассиметричных криптосистем.
3. Чем отличаются понятия целостности и подлинности сообщений?
4. Поясните понятие «криптографическая стойкость».
5. Чем определяется длина ключей практически стойких симметричных шифров?
6. Расскажите про шифр Вернама.
7. Для каких целей служит протокол открытого распределения ключей Диффи-Хеллмана?
8. Какие аппаратные средства криптографической защиты существуют?
9. Что такое жизненный цикл криптографического ключа?
10. Что понимается под управлением криптографическими ключами?
11. Какие основные группы протоколов использует инфраструктура открытых ключей (ИОК)?
12. Каковы особенности российского законодательства в сфере организации ИОК?
13. Расскажите о программных средствах криптографической защиты информации.

Тема «Виртуальные вычислительные сети»

1. Какие задачи решает построение виртуальной частной вычислительной сети(ВЧВС)?
2. Возможно ли использование только каналов связи предприятия для создания его ВЧВС?
3. Особенности современных сетей, на основе которых приходится создавать ВЧВС
4. Механизм туннелирования в ВЧВС.
5. Что такое ВЧВС агенты и каковы их функции?
6. Какие бывают виды виртуальных каналов?
7. Какие протоколы создания ВЧВС работают на уровнях модели OSI? Опишите особенности этих протоколов.
8. Какие виды ВЧВС в зависимости от решаемых задач вам известны.
9. Схема построения Intranet VPN.
10. Схема построения Client-server VPN/
11. Схема построения Enternet VPN.
12. Расскажите о VPN с удаленным доступом и их вариантах.

Тема «Системы анализа защищенности»

1. Каково основное назначение и в чем разница аудита и мониторинга информационной безопасности в открытых системах?
2. Какие задачи в защите ОИС решают системы анализа защищенности (САЗ)?
3. Какие уязвимости ОИС выявляют сканеры безопасности?
4. Приведите классификацию сканеров безопасности по различным критериям.
5. Где размещаются агенты сетевых сканеров?
6. Основные этапы работы сетевых сканеров.
7. Что такое системные сканеры безопасности, какие функции они выполняют?
8. Как определяется топология сети при использовании сетевых сканеров безопасности?
9. В чем особенности сканеров безопасности для приложений.
10. Перечислите основные критерии, которыми необходимо руководствоваться при выборе сканеров безопасности.

Тема «Системы обнаружения и предотвращения вторжений (СОВ)»

1. Основные тенденции эволюции методов отражения вторжений.
2. Приведите классификацию методов отражения вторжений в сети.
3. Основные способы прерывания вторжений.
4. Особенности отклонения вторжений.
5. Каково место СОВ в многоуровневой защите интранета?
6. Как можно оценить эффективность работы СОВ?
7. Какие задачи решают системы контроля целостности файлов?
8. На основе какой информации и как работают мониторы регистрационных файлов?
9. Что такое сетевое обнаружение вторжений?
10. Что вам известно о современных комплексах обнаружения вторжений?
11. Какие проблемы еще не решены в современных СОВ?
12. Чем отличаются от СОВ системы предотвращения вторжений?
13. Какова ситуация в области стандартов, регламентирующих обнаружение вторжений и реализующих его систем?

Сообщение, доклад и презентация

Тема « Основы информационной безопасности открытых информационных систем».

1. Необходимость применения объектно-ориентированного подхода к информационной безопасности.
2. Основные понятия объектно-ориентированного подхода.

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

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

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

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

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

Тема «Угрозы информационной безопасности открытых информационных систем».

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

Тема «Уязвимости открытых систем на примере Intranet».

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

Тема «Атаки на открытые системы».

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

Тема «Обеспечение информационной безопасности в открытых системах».

1. Понятия о симметричных криптосистемах (шифры перестановки; шифры сложной замены; одноразовая система шифрования; шифрование методом гаммирования; DES).
2. Понятия об асимметричных криптосистемах (однонаправленные функции; криптосистема шифрования данных RSA; электронная цифровая подпись).
3. Понятие криптоанализа.

4. Аппаратно-программные криптографические средства защиты информации.
5. Системы идентификации и аутентификации пользователей.
6. Системы шифрования дисковых данных.
7. Системы шифрования данных.
8. Системы аутентификации электронных данных.
9. Средства управления ключевой информацией.

Тема «Законодательный уровень информационной безопасности. Политика безопасности».

1. Понятие о законодательном уровне информационной безопасности.
2. Обзор российского законодательства в области информационной безопасности.
3. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности.
4. Закон «Об информации, информатизации и защите информации».
5. Обзор зарубежного законодательства в области информационной безопасности.
6. О текущем состоянии российского законодательства в области информационной безопасности.
7. Политика использования ресурсов Интранета.
8. Политика в отношении паролей.
9. Политика шифрования.
10. Антивирусная политика.
11. Политика управления доступом и регистрации для пользователей Интранета.
12. Политика для пограничных маршрутизаторов подразделений, подключенных к Интранету
13. Политика удаленного доступа мобильных пользователей к Интранету.
14. Политика для конфиденциальной информации, обрабатываемой в Интранете.
15. Политика для оборудования пограничной демилитаризованной зоны подразделений организации.
16. Политика для Экстранета.
17. Политика доступа сотрудников организации к Интернету.
18. Политика для межсетевых экранов
19. Политика пересылки электронной почты для организации.
20. Политика резервирования информации для подразделений организации.

Перечень теоретических вопросов к зачету

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

7. Уязвимость системных утилит, команд и сетевых сервисов. Уязвимость современных технологий программирования. Ошибки в программном обеспечении.
8. Модель угроз ИБ. Модель нарушителей ИБ. Инсайдеры и аутсайдеры.
9. Атаки на открытые системы. Удаленные атаки на открытые системы. Классификация удаленных атак.
10. Анализ сетевого трафика. Подмена доверенного объекта или субъекта системы. Внедрение ложного объекта в систему.
11. Типичные сценарии и уровни атак. Удаленный контроль над станцией в сети.
12. Классические методы взлома (взлом парольной защиты). Современные методы взлома: перехват данных при их перемещении по каналам связи и перехват ввода с клавиатуры; мониторинг в графических интерфейсах; подмена системных утилит; нападения с использованием сетевых протоколов.
13. Обеспечение информационной безопасности в открытых системах. Комплексный и фрагментарный подходы к защите ИС. Четырехуровневая модель открытой системы.
14. Эшелонированная защита ОИС в целом и отдельных ее элементов. топология сети: физическая изоляция; изоляция протокола; выделенные каналы.
15. Организационно-правовые методы защиты открытых систем.
16. Политика информационной безопасности. Разновидности политик ИБ. Основные положения политики ИБ.
17. Информационная безопасность в глобальных сетях. Удаленные атаки и механизмы их реализации в глобальных сетях.
18. Криптографическая защита информации. Понятия о симметричных криптосистемах (шифры перестановки; шифры сложной замены; одноразовая система шифрования; шифрование методом гаммирования; DES).
19. Криптографическая защита информации. Понятия об асимметричных криптосистемах (однонаправленные функции; криптосистема шифрования данных RSA; электронная цифровая подпись).
20. Криптографическая защита информации. Аппаратно-программные криптографические средства защиты информации.
21. Межсетевые экраны (firewall): прикладного уровня; с пакетной фильтрацией; гибридные межсетевые экраны.
22. Организация и эксплуатация виртуальных частных сетей (VPN).
23. Иерархическая модель доверия. Сетевая модель доверия.
24. Управление ключами и сертификация ключей.
25. Протокол конфиденциального обмена данными SSL. Протокол WEP. Протокол 802.1X - контроль доступа в сеть по портам.
26. Стандарты и спецификации в области информационной безопасности.

3.2 Перечень типовых практических заданий к зачету

Раздел дисциплины	Тема раздела	Объекты темы	Количество тестовых заданий (ТЗ), типы ТЗ
Раздел 1. Основные элементы технологии открытых информационных систем.	Основные элементы технологии открытых информационных систем. Совместимость открытых систем. Переносимость и способность к взаимодействию. Базовая модель информационной системы. Расширение базовой модели информационной системы для взаимодействующих систем. Основные модели открытых систем. /Лек/		5 – тип А

	Интранет как открытая система. Структура интранета. Эталонная модель интранета. Этапы создания интранета. Виды интранета. Стандарты интранета. Интранет как часть среды открытых систем. Интранет и экстранет . Портал и интранет. /Лек/		5 – тип А
	Исследование нормативно-правовой базы информационной безопасности предприятия. /Лр/		2 – тип А 2 – тип В
		Итого по разделу	∑ 14 12– тип А 2– тип В
Раздел 2. Уязвимости открытых систем. Атаки на открытые системы.	Уязвимость открытых систем. Основные понятия. Угрозы открытых систем (в том числе интранета) и причины их реализации. Уязвимости архитектуры клиент-сервер: уязвимости операционных систем; уязвимость серверов; уязвимость рабочих станций; уязвимость каналов связи. /Лек/		6 – тип А
	Удаленные атаки на открытые системы. Анализ сетевого трафика. Подмена доверенного объекта или субъекта. Ложный объект. Отказ в обслуживании. Удаленный контроль над станцией. /Лр/		2 – тип А
	Политика безопасности для открытых систем (определение, причины выработки, этапы и содержание, реализация и аудит политики безопасности). /Ср/		4 – тип А
	Уязвимость открытых систем. Слабости системных утилит, команд и сетевых сервисов. /Лек/		4– тип А
	Классические и современные методы, используемые нападающим для проникновения в открытые системы. Перехват данных и обнаружение прослушивающих приложений. Мониторинг в графических интерфейсах. Подмена системных утилит. Атаки с использованием сетевых протоколов. /Лек/		6 – тип А

	Примеры политик безопасности. Политика использования ресурсов интранета. Политика в отношении паролей. Политика шифрования. Антивирусная политика. Политика оценки рисков. Политика аудита. Политика для программных маршрутизаторов. Политика удаленного доступа. /Лр/		2 – тип А 2 – тип В
	Слабости современных технологий программирования. Ошибки в программном обеспечении. Сетевые вирусы. /Лек/		6 – тип А
	Типичные сценарии и уровни атак. Этапы реализации атак. Примеры некоторых атак. /Лр/		2 – тип А
	Примеры политик безопасности. Политика подключения подразделений к интранету. Политика для конфиденциальной безопасности. Политика для веб-сервера. Политика пересылки электронной почты. Политика подключения новых устройств в интранет. /Лр/		2 – тип А
	Средства интранета. /Ср/		2 – тип А
	Средства создания порталов. /Ср/		2 – тип В
	Стандарты ISO по защите информации в открытых системах. /Ср/		2 – тип А
		Итого по разделу	∑ 42 38– тип А 4– тип В
3. СУБД Oracle Express Edition	Четырехуровневая модель открытой системы. Специфика защиты ресурсов открытых систем на примере интранета. Выбор сетевой топологии интранета при подключении к другим внешним сетям. Физическая изоляция. Изоляция протоколов. Выделенные каналы и маршрутизаторы. Принципы создания защищенных средств связи объектов в открытых системах. /Лек/		4 – тип А

	Межсетевые экраны. Функции межсетевых экранов. Руководящий документ Гостехкомиссии России по межсетевым экранам. Профили защиты для межсетевых экранов. Типы межсетевых экранов. Основные компоненты межсетевого экрана. /Лек/		6 – тип А
	Схемы подключения межсетевых экранов. Слабости межсетевых экранов. Выбор реализаций межсетевых экранов. /Лр/		2 – тип А 2 – тип В
	Средства обеспечения информационной безопасности в открытых системах. Создание комплексной системы обеспечения безопасности открытых систем. Управление безопасности открытых систем. Рекомендации по обеспечению информационной безопасности открытых систем. /Лек/		4– тип А
	Аутентификация субъектов и объектов взаимодействия в открытых системах. Сетевая аутентификация. Подсистема аутентификации. /Лр/		2 – тип А 2 – тип В
	Изучение российского рынка средств аутентификации. Сравнительный анализ средств аутентификации. /Ср/		
	Сервисы безопасности (идентификация/аутентификация, разграничение доступа, экранирование, шифрование, управление и др.). /Лек/		6– тип А
	Криптографическая защита в открытых системах. Основные понятия и методы криптографии. Стандартизация криптографических функций и механизмов. Криптографические протоколы. Криптографическая инфраструктура. Программные и аппаратные средства криптографической защиты. /Лр/		2 – тип А 2 – тип В
	Исследование поточных и блочных алгоритмов шифрования. Использование хэш-функций. /Лр/		2 – тип В
	Виртуальные вычислительные сети. Определение виртуальных частных вычислительных сетей.		4– тип А

	Цели и задачи построения ВЧВС. Специфика построения ВЧВС. Туннелирование в ВЧВС. Схема ВЧВС. Политики безопасности для ВЧВС. Стандартные протоколы построения ВЧВС. Проблемы и уязвимости современных ВЧВС. /Лек/		
	Системы анализа защищенности. Аудит и мониторинг информационной безопасности в открытых системах. Место и задачи систем анализа защищенности в защите открытых систем. Классификации систем анализа защищенности. Сетевые сканеры. Системные сканеры. Сканеры безопасности для приложений. Критерии выбора сканеров безопасности. /Лр/		2 – тип А 2 – тип В
	Работа с системой контроля защищенности (MaxPatrol – демо-версия). /Лр/		
	Стандартные протоколы построения ВЧВС. Виды ВЧВС в зависимости от решаемых задач. Топологии ВЧВС. Виртуальные локальные вычислительные сети. /Лек/		2 – тип А
	Системы обнаружения и предотвращения вторжений. Методы отражения вторжений. Основы построения систем обнаружения вторжений. Системное обнаружение вторжений. Сетевое обнаружение вторжений. Поведенческое обнаружение вторжений. Интеллектуальное обнаружение вторжений. Комплексное обнаружение вторжений. Выбор системы обнаружения вторжений. Развертывание системы обнаружения вторжений. Практика обнаружения вторжений. /Лр/		2 – тип А 2 – тип В
	Системы обнаружения атак, работающие в режиме реального времени. /Ср/		2 – тип А
	Другие средства обеспечения безопасности в открытых системах. Защита от спама в электронной почте. Многофункциональные устройства защиты от сетевых атак. Системы анализа и управления рисками. Системы		2 – тип А

	обеспечения информационной безопасности на уровне предприятия. /Ср/		
	Документы по основным протоколам для виртуальных частных сетей. Сравнительные характеристики ВЧВС-продуктов российских производителей. /Ср/		2 – тип А
	Зарубежные средства обеспечения информационной безопасности в сетях. /Ср/		2 – тип А
Итого по разделу			**∑ 52 40– тип А 12– тип В**
Итого по дисциплине			**∑ 108 90– тип А 28– тип В**

Используемые типы тестовых заданий (ТЗ):

ТЗ типа А: тестовое задание закрытой формы (ТЗ с выбором одного или нескольких правильных ответов);

ТЗ типа В: тестовое задание открытой формы (с конструируемым ответом: ТЗ с кратким регламентируемым ответом (ТЗ дополнения); ТЗ свободного изложения (с развернутым ответом в произвольной форме);

ТЗ типа С: тестовое задание на установление соответствия;

ТЗ типа Д: тестовое задание на установление правильной последовательности.

1 Компания пытается снизить затраты на развертывание коммерческого программного обеспечения и рассматривает возможность использования облачных служб. Какая облачная служба будет наилучшей для размещения программного обеспечения?

Платформа как услуга (PaaS)

ПО как услуга (SaaS)

Инфраструктура как услуга (IaaS)

Восстановление как услуга (RaaS)

2 Если лицо сознательно получает доступ к компьютеру, который связан с правительством, без разрешения, какие федеральные законы на него распространяются?

Закон о компьютерном мошенничестве (CFAA)

Закон Сарбейнса — Оксли (SOX)

Закон о тайне обмена электронной информацией (ECPA)

Закон Грэмма — Лича — Блайли (GLBA)

3 Организация внедрила инфраструктуру частного облака. Администратору системы безопасности поручают защитить инфраструктуру от потенциальных угроз. Какие три тактики можно использовать для защиты частного облака? (Выберите три варианта.)

Наем консультанта

Отключение ping-запросов, зондирования и сканирования портов

Установка на устройства последних исправлений и обновлений для системы безопасности

Предоставление административных прав

Отключение межсетевых экранов

Проверка входящего и исходящего трафика

4 В компании, которая обрабатывает информацию о кредитных картах, происходит нарушение безопасности. Какой отраслевой закон регулирует защиту данных кредитной карты?

Закон Сарбейнса — Оксли (SOX)

Закон о тайне обмена электронной информацией (ECPA)

Закон Грэмма — Лича — Блайли (GLBA)

Стандарт безопасности данных индустрии платежных карт (PCI DSS)

5 Аудитору предлагают оценить потенциальные угрозы для локальной сети компании. Какие три потенциальные угрозы может отметить аудитор? (Выберите три варианта.)

Несанкционированное сканирование портов и зондирования сети

Неправильно настроенный межсетевой экран

Закрытый доступ к системам

Сложные пароли

Политика допустимого использования

Открытый доступ к сетевому оборудованию

6 Несанкционированные посетители вошли в офис компании и ходят по зданию. Какие две меры могут предотвратить доступ несанкционированных посетителей в здание? (Выберите два варианта.)

Запрет на выход из здания в рабочее время

Замки на шкафах

Определение правил и процедур для гостей, посещающих здание

Регулярное проведение обучения по вопросам безопасности

7 Что можно использовать для балльной оценки серьезности угроз в целях определения важных уязвимостей?

ACSC

Центр реагирования на компьютерные инциденты (CERT)

ISC

Национальная база данных об уязвимостях (NVD)

8 В компании произошло несколько инцидентов, когда пользователи загружали несанкционированное ПО, использовали запрещенные веб-сайты и личные USB-накопители. ИТ-директор хочет внедрить схему управления угрозами, исходящими от пользователей. Какие три меры могли бы использоваться для управления угрозами? (Выберите три варианта.)

Фильтрация содержимого

Проведение обучения по вопросам безопасности

Дисциплинарное взыскание

Отключение доступа к CD и USB

Отслеживание всех действий пользователей

Переход на тонкие клиенты

9 В рамках кадровой политики компании физическое лицо может отказаться предоставлять информацию любой третьей стороне, кроме работодателя. Какой закон защищает конфиденциальность предоставленной личной информации?

Закон о правах семьи на образование и неприкосновенность частной жизни (FERPA)

Стандарт безопасности данных индустрии платежных карт (PCI)

Закон Сарбейнса — Оксли (SOX)

Закон Грэмма — Лича — Блайли (GLBA)

10 Какие три исключения из правил по обязательному предоставлению информации предусмотрены Законом о свободе информации (FOIA)? (Выберите три варианта.)

Негеологическая информация о скважинах

Информация, не защищенная специальными законами

Информация, касающаяся национальной безопасности и внешней политики

Общедоступная информация финансовых учреждений
Конфиденциальная коммерческая информация
Документация правоохранительных органов, попадающая под перечисленные исключения

11 Администратор учебного заведения обеспокоен раскрытием информации о студентах в результате взлома системы. Какой закон защищает данные студентов?
Закон о преемственности страхования и отчетности в области здравоохранения (HIPPA)
Закон о правах семьи на образование и неприкосновенность частной жизни (FERPA)
Закон о защите личных сведений детей в Интернете (COPPA)
Закон о защите детей в Интернете (CIPA)

12 Специалист по безопасности может иметь доступ к конфиденциальным данным и ресурсам. Что из следующего должен понимать специалист по безопасности для принятия обоснованных, этических решений (выбрать один пункт)?
Возможный бонус
Потенциальная выгода
Поставщики облачных услуг
Законы, регулирующие обработку данных
Партнерства

13 Почему для тестирования безопасности сети организации часто выбирают дистрибутив Kali Linux?
Он может использоваться для проверки слабых мест только с помощью вредоносного ПО.
Он может использоваться для перехвата и регистрации сетевого трафика.
Это инструмент сканирования сети, который определяет приоритеты для угроз безопасности.
Это дистрибутив Linux с открытым исходным кодом, включающий в себя более 300 инструментов для защиты.

14 Какие два вида информации можно найти на веб-сайте Internet Storm Center? (Выберите два варианта.)
Вакансии InfoSec
Отчеты InfoSec
Архивные данные
Действующие законы

15 Для сбора рекомендаций по защите устройств от угроз компания наняла консультанта. Какие три общие рекомендации можно выявить? (Выберите три варианта.)
Включение автоматического антивирусного сканирования
Отмена административных прав для пользователей
Отмена фильтрации содержимого
Включение блокировки экрана
Разрешение съемных носителей информации
Соблюдение строгой кадровой политики

16 Каковы три основные категории должностей по информационной безопасности? (Выберите три варианта.)
Наблюдающие
Исполняющие
Определяющие
Создающие
Творящие
Ищущие

17 Каковы две потенциальные угрозы для приложений? (Выберите два варианта.)

несанкционированный доступ
потеря данных
социальная инженерия
Перебои питания

18 Специалисту по безопасности предлагают выполнить анализ текущего состояния сети компании. Какой инструмент будет использовать специалист по безопасности для сканирования сети исключительно в целях выявления угроз безопасности?
Анализатор пакетов
Сканер уязвимостей
Испытание на проникновение
Вредоносное ПО

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/практики.

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Сообщение, доклад и презентация	Темы сообщений/докладов предоставляются обучающимся вначале семестра, для того, чтобы у них была возможность выбора наиболее интересной, понравившейся темы. Доклады должны сопровождаться презентацией и длиться не более 30 минут. Типовые контрольные задания
Коллоквиум	Коллоквиум проводятся в форме обсуждения по предложенным преподавателем вопросам. Продолжительность коллоквиума для каждого учащегося (либо для группы обучающихся) 40-50 минут. Для этого преподаватель заранее формулирует тему или проблемные вопросы для обсуждения, а также цели и задачи занятия. Группа обучающихся может быть разделена на небольшие группы, примерно, по 4 человека. В порядке, установленном преподавателем, учащиеся зачитывают выработанные, в ходе коллективного обсуждения ответы. Обучающиеся из других микрогрупп задают вопросы докладчику, комментируют и дополняют предложенный ответ. Преподаватель регулирует обсуждения, задавая наводящие вопросы, корректируя неправильные ответы. После обсуждения каждого вопроса необходимо подвести общие выводы и логично перейти к обсуждению следующего вопроса (важно вопросы распределить таким образом, чтобы ответы микрогрупп чередовались). После обсуждения всех предложенных вопросов преподаватель формулирует выводы и заключение.
Конспект	Преподаватель не мене, чем за неделю до срока выполнения конспекта должен довести до сведения обучающихся тему конспекта и указать необходимую учебную литературу. Темы и перечень необходимой учебной литературы выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет. Конспект должен быть выполнены в установленный преподавателем срок. Конспекты в назначенный срок сдаются на проверку.
Собеседование	Собеседование с обучающимися проходит на семинарских занятиях. В момент проведения собеседования пользоваться учебниками, справочниками, конспектами лекций запрещено. Преподаватель заранее оглашает учащимся перечень вопросов, ответы на которые необходимо подготовить учащимся самостоятельно.

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. Оценочные средства и типовые контрольные задания, используемые при текущем контроле, позволяют оценить знания, умения и владения навыками/опытом деятельности обучающихся при освоении дисциплины. 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	*Оценка*
Оценка не менее 3,0 и нет ни одной неудовлетворительной оценки по текущему контролю	*«зачтено»*
Оценка менее 3,0 или получена хотя бы одна неудовлетворительная оценка по текущему контролю	*«не зачтено»*

Если оценка уровня сформированности компетенций обучающегося не соответствует критериям получения зачета без дополнительного аттестационного испытания, то промежуточная аттестация в форме зачета проводится в форме собеседования по перечню теоретических вопросов и типовых практических задач (не более двух теоретических и двух практических). Промежуточная аттестация в форме зачета с проведением аттестационного испытания в форме собеседования проходит на последнем занятии по дисциплине.