ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

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

Б1.Б.1.28 Программно-аппаратные средства обеспечения информационной безопасности

рабочая программа дисциплины

Специальность – 10.05.03 Информационная безопасность автоматизированных систем
Специализация – Безопасность открытых информационных систем
Квалификация выпускника – специалист по защите информации
Форма обучения – очная
Нормативный срок обучения – 5 лет
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 8
Часов по учебному плану – 288

Формы промежуточной аттестации в семестрах:
зачет (8), экзамен (9)

Распределение часов дисциплины по семестрам

Семестр	8	9	**Итого**
Число недель в семестре	18	18	
Вид занятий	Часов по учебному плану	Часов по учебному плану	**Часов по учебному плану**
Аудиторная контактная работа по видам учебных занятий	**72**	**54**	**126**
– лекции	36	18	**54**
– практические (семинарские)	18	18	**36**
– лабораторные	18	18	**36**
Самостоятельная работа	**72**	**54**	**126**
Экзамен		**36**	**36**
Итого	**144**	**144**	**288**

ИРКУТСК

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1 Цели освоения дисциплины	
1	обучение студентов технологиям построения современных систем защиты информации (СЗИ) на базе программно-аппаратных средств;
2	освоение студентами способов экономически обоснованного выбора и рационального использования программно-аппаратных средств обеспечения информационной безопасности (ИБ).
1.2 Задачи освоения дисциплины	
1	получение знаний о принципах функционирования и возможностях программно-аппаратных средствах защиты информации (ПАСЗИ) в автоматизированных системах (АС);
2	изучение технологических особенностей представителей различных классов ПАСЗИ;
3	получение практических навыков администрирования добавочных ПАСЗИ;
4	анализ рынка современных программно-аппаратных средств обеспечения ИБ АС.
1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины	
Профессионально-трудовое воспитание обучающихся	
Цель профессионально-трудового воспитания – формирование у обучающихся осознанной профессиональной ориентации, понимания общественного смысла труда и значимости его для себя лично, ответственного, сознательного и творческого отношения к будущей деятельности, профессиональной этики, способности предвидеть изменения, которые могут возникнуть в профессиональной деятельности, и умению работать в изменённых, вновь созданных условиях труда. Цель достигается по мере решения в единстве следующих задач: – формирование сознательного отношения к выбранной профессии; – воспитание чести, гордости, любви к профессии, сознательного отношения к профессиональному долгу, понимаемому как личная ответственность и обязанность; – формирование психологии профессионала; – формирование профессиональной культуры, этики профессионального общения; – формирование социальной компетентности и другие задачи, связанные с имиджем профессии и авторитетом транспортной отрасли	

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
2.1 Требования к предварительной подготовке обучающегося	
1	Б1.Б.1.13 Информатика
2	Б1.Б.1.18 Электроника и схемотехника
3	Б1.Б.1.19 Безопасность операционных систем
4	Б1.Б.1.20 Безопасность сетей ЭВМ
5	Б1.Б.1.22 Основы информационной безопасности
6	Б1.Б.1.23 Криптографические методы защиты информации
7	Б1.Б.1.24 Организация ЭВМ и вычислительных систем
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б1.Б.1.ДС.03 Информационная безопасность открытых систем
2	Б1.Б.1.ДС.04 Виртуальные частные сети
3	Б1.Б.1.ДС.05 Аудит информационных технологий и систем обеспечения информационной безопасности
4	Б1.Б.1.29 Разработка и эксплуатация защищенных автоматизированных систем
5	Б1.В.06 Комплексная защита в информационных системах персональных данных
6	Б2.Б.03(П) Производственная - эксплуатационная
7	Б2.Б.05(П) Производственная - технологическая
8	Б2.Б.06(Пд) Производственная - преддипломная

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕС ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
ПК-14: способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	
Минимальный уровень освоения компетенции	
Знать	методики проведения проверки эффективности работы ПАСЗИ;
Уметь	организовать проверки эффективности работы ПАСЗИ;
Владеть	навыками тестирования работоспособности ПАСЗИ;

Базовый уровень освоения компетенции	
Знать	способы устранения нештатных ситуаций в процессе функционирования ПАСЗИ;
Уметь	проводить проверки эффективности работы ПАСЗИ;
Владеть	навыками анализа работы ПАСЗИ и выявления наличия нештатных ситуаций;
Высокий уровень освоения компетенции	
Знать	методики проведения проверки эффективности работы и способы устранения нештатных ситуаций;
Уметь	проводить проверки эффективности работы ПАСЗИ и устранять нештатные ситуации;
Владеть	навыками тестирования работоспособности ПАСЗИ и анализа его результатов.

ПК-26: способность администрировать подсистему информационной безопасности автоматизированной системы	
Минимальный уровень освоения компетенции	
Знать	основные классы штатных и добавочных ПАСЗИ;
Уметь	устанавливать добавочные программно-аппаратные средства обеспечения ИБ;
Владеть	навыками администрирования отдельных защитных механизмов ПАСЗИ;
Базовый уровень освоения компетенции	
Знать	базовые сервисы безопасности ПАСЗИ;
Уметь	настраивать основные механизмы в соответствии с политикой ИБ;
Владеть	навыками анализа рынка современных ПАСЗИ;
Высокий уровень освоения компетенции	
Знать	функциональные возможности представителей классов ПАСЗИ;
Уметь	в полной мере администрировать механизмы безопасности ПАСЗИ;
Владеть	навыками администрирования комплексной системы ПАСЗИ.

В результате освоения дисциплины обучающийся должен

Знать	
1	методические основы использования программно-аппаратных средств обеспечения ИБ АС;
3	принципы функционирования ПАСЗИ;
4	функциональные возможности представителей основных классов ПАСЗИ;
5	условия эксплуатации программно-аппаратных средств обеспечения ИБ АС;
6	способы устранения нештатных ситуаций в процессе функционирования ПАСЗИ;
7	основные тенденции развития современного рынка ПАСЗИ.
Уметь	
1	проводить выбор ПАСЗИ для использования их в составе АС с целью обеспечения требуемого уровня ее защищенности;
2	администрировать ПАСЗИ;
3	создавать необходимые условия использования ПАСЗИ для обеспечения ИБ;
4	экономически эффективно использовать программно-аппаратные средства обеспечения ИБ в профессиональной деятельности;
5	проводить проверки работоспособности ПАСЗИ и устранять нештатные ситуации.
Владеть	
1	практическими навыками использования программно-аппаратных средств обеспечения информационной безопасности АС (на основе программно-технических и программных образцов).

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр	Часы	Код компетенции	Учебная литература, ресурсы сети «Интернет»
	Раздел 1. Основные категории требований к программно-аппаратной реализации средств обеспечения ИБ				
1.1	Руководящие и методические документы Гостехкомиссии и ФСТЭК РФ /Лек/	8	2	ПК-14, ПК-26	Э1
1.2	Профили защиты средств защиты информации /Лек/	8	4	ПК-14, ПК-26	Э1

1.3	Комплекс национальных стандартов Российской Федерации ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» /Пр/	8	2	ПК-14, ПК-26	Э1
1.4	Работа с пакетом «КриптоАРМ»/Лаб/	8	3	ПК-14, ПК-26	Л1.3-Л.1.4, Л2.1, Л2.3
1.5	Руководящий документ (РД) ГТК РФ «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации». РД ГТК РФ «Средства вычислительной техники Защита от несанкционированного доступа к информации Показатели защищенности от несанкционированного доступа к информации». Профили защиты средств защиты информации ФСТЭК /Ср/	8	24	ПК-14, ПК-26	Э1
	Раздел 2. Базовые принципы применения ПАСЗИ, основные классы ПАСЗИ				
2.1	Обоснование необходимости применения добавочных ПАСЗИ, принципы использования /Лек/	8	2	ПК-14, ПК-26	Л1.1-Л1.4, Л4.1. Э8
2.2	Основные классы добавочных программно-аппаратных средств, обеспечивающих повышенный уровень защиты /Лек/	8	4	ПК-14, ПК-26	Л1.1-Л1.4, Л2.1-Л2.5, Л4.1, Э8
2.3	Работа с пакетом «Криптосейф» /Лаб/	8	3	ПК-14, ПК-26	Л.2.1, Л2.3
2.4	Профили защиты средств защиты информации ФСТЭК /Ср/	8	20	ПК-14, ПК-26	Э1
	Раздел 3. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их технологические особенности, взаимодействие с общесистемными компонентами АС				
3.1	Характеристика, основные сервисы и механизмы добавочных ПАСЗИ /Лек/	8	4	ПК-14, ПК-26	Л1.1-Л1.4, Л2.1-Л2.5, Л4.1, Э8
3.2	Типы технологий усиленной идентификации и аутентификации, разграничения доступа к информации /Лек/	8	2	ПК-14, ПК-26	Л1.1-Л1.4, Л2.1-Л2.5, Л4.1, Э8
3.3	Биометрические методы идентификации и аутентификации. Процедуры биометрического опознания. Устройства биометрической идентификации и аутентификации для автоматизированных систем и виды контроля /Пр/	8	4	ПК-14, ПК-26	Л1.1-Л1.4, Л2.1-Л2.5, Л4.1, Э8
3.4	Линейка СЗИ Acronis /Пр/	8	3	ПК-14, ПК-26	Л1.3-Л.1.4, Л2.1, Л2.3
3.5	АПК Аргус /Пр/	8	2	ПК-14, ПК-26	Э8
3.6	Средства выявления уязвимостей узлов сетей, средства обнаружения атак на узлы, протоколы и сетевые службы. Назначение, возможности, принципы работы /Пр/	8	2	ПК-14, ПК-26	Э8
3.7	Работа с пакетом «Криптоофис» /Лаб/	8	3	ПК-14, ПК-26	Э8
3.8	Проработка лекционного материала, подготовка к семинарским занятиям и лабораторным работам /Ср/	8	14	ПК-14, ПК-26	Л1.1-Л1.4, Л2.1-Л2.5, Л4.1, Э8
	Раздел 4. Аппаратные средства аутентификации; методы и средства хранения ключевой информации				

4.1	Общие сведения о методах аутентификации. Магнитные диски. Магнитные и интеллектуальные карты. Устройство хранения ключей типа Touch Memory (iButton). Электронные идентификаторы ruToken. ПСКЗИ ШИПКА /Лек/	8	4	ПК-14, ПК-26	Л1.1-Л1.4, Л2.1-Л2.4, Э8
4.2	Микропроцессорные или интеллектуальные карточки. Бесконтактные карточки. Среда использования смарт-карт в персональных компьютерах /Пр/	8	2	ПК-14, ПК-26	Л1.1-Л1.4, Л2.1-Л2.5, Э8
4.3	Электронные идентификаторы eToken /Пр/	8	3		Э8
4.4	Использование ключевого носителя ruToken (на базе пакета Rohos) /Лаб/	8	3	ПК-14, ПК-26	Л1.1-Л.1.4, Л2.1, Л2.3, Э3
4.5	Идентификационные карточки с магнитной полосой. Карточки с интегральной микросхемой и металлическими контактами. Карточки с незащищенной памятью /Ср/	8	4	ПК-14, ПК-26	Л1.1, Э1
4.6	Проработка лекционного материала, подготовка к семинарским занятиям и лабораторным работам /Ср/	8	10	ПК-14, ПК-26	Л1.1-Л1.4, Л2.1-Л2.4, Л4.1, Э8
	Раздел 5. Методы и средства разграничения доступа к компонентам АС; технологии защиты от несанкционированного доступа (НСД) к информации				
5.1	Виды и способы реализации НСД /Лек/	8	2	ПК-14, ПК-26	Л1.2
5.2	Электронный замок (ЭЗ) «Соболь»: назначение, варианты применения, требования к оборудованию и ПО, комплектация. ЭЗ «Соболь»: основные принципы функционирования. ЭЗ «Соболь»: настройка и эксплуатация устройства /Лек/	8	4	ПК-14, ПК-26	Л.3.1, Э4
5.3	СЗИ от НСД «Dallas Lock» (DL): назначение и состав системы защиты. DL: общие принципы организации защиты ресурсов. DL: механизмы управления доступом и защиты объектов /Лек/	8	6	ПК-14, ПК-26	Э5
5.4	СЗИ SecretNet ОС Windows (автономный вариант) (SN AB): архитектура и компоненты системы. SN AB: защитные механизмы. SN (сетевой вариант) (SN CB): назначение и варианты применения системы. SN CB: общая архитектура и компоненты. SN CB: управление доступом пользователей к ресурсам. SN CB: средства централизованного и оперативного управления /Лек/	9	6	ПК-14, ПК-26	Л.3.1, Э4
5.5	СЗИ Страж NT /Лек/	9	2	ПК-14, ПК-26	Э9
5.6	Программно-аппаратный комплекс защиты информации от НСД “Аккорд”/Пр/	9	2	ПК-14, ПК-26	Э6
5.7	СЗИ Device Lock. DLP-система Info Watch Traffic Monitor Enterprise Edition /Пр/	9	3	ПК-14, ПК-26	Л2.2
5.8	СЗИ Secret Net Studio. СЗИ vGate for VMvare Infrastructure /Пр/	9	4	ПК-14, ПК-26	Э4
5.9	ЭЗ Соболь-PCI. Настройка и эксплуатация. Управление пользователями. Диагностика устройства. Настройка контроля целостности. Регистрация событий /Лаб/	8	3	ПК-14, ПК-26	Э4

5.10	СЗИ НСД DL: установка средства, настройка параметров входа в систему; реализация дискреционного разграничения доступа /Лаб/	8	3	ПК-14, ПК-26	Э5
5.11	СЗИ НСД DL: реализация мандатного разграничения доступа; механизм замкнутой программной среды /Лаб/	9	3	ПК-14, ПК-26	Э5
5.12	СЗИ НСД DL: протоколирование событий; настройка механизма контроля целостности; администрирование системы защиты /Лаб/	9	3	ПК-14, ПК-26	Э5
5.13	СЗИ от НСД SN AB: установка средства, дискреционное разграничение доступа /Лаб/	9	2	ПК-14, ПК-26	Э4
5.14	СЗИ от НСД SN AB: настройка контроля целостности /Лаб/	9	2	ПК-14, ПК-26	Э4
5.15	СЗИ от НСД SN AB: регистрация событий /Лаб/	9	3	ПК-14, ПК-26	Э4
5.16	СЗИ от НСД SN AB: работа с электронным идентификатором; затирание данных /Лаб/	9	2	ПК-14, ПК-26	Э4
5.17	Проработка лекционного материала, подготовка к семинарским занятиям и лабораторным работам /Ср/	9	14	ПК-14, ПК-26	Э4, Э5, Э9
	Раздел 6. Средства антивирусной защиты информации				
6.1	Угрозы применения вредоносного ПО. Технологии антивирусной защиты информации /Лек/	9	2	ПК-14, ПК-26	Л1.2, Э8
6.2	Эксплуатация средств антивирусной защиты 360 Total Security; Dr. Web cureit; Dr_Web; Касперский_IS /Лаб/	9	3	ПК-14, ПК-26	Л1.3-Л.1.4, Л2.1, Л2.3
6.3	Проработка лекционного материала, подготовка к семинарским занятиям и лабораторным работам /Ср/	9	10	ПК-14, ПК-26	Л1.2, Л4.1, Э8
	Раздел 7. Технологии анализа защищенности АС				
7.1	Цели и задачи проведения мероприятий по оценке уровня защищенности АС /Лек/	9	2	ПК-14, ПК-26	Л2.1-Л2.5
7.2	Средство анализа защищенности АС «Агент инвентаризации (ОС Windows)»; средство фиксации и контроля исходного состояния программного комплекса "ФИКС"; средство создания модели системы разграничения доступа "Ревизор 1 XP"; средство контроля защищенности от НСД "Ревизор 2 XP" /Лек/	9	2	ПК-14, ПК-26	Л2.1-Л2.5
7.3	Сканер-ВС, сканеры MaxPatrol и "Ревизор сети" /Пр/	9	3	ПК-14, ПК-26	Л2.1-Л2.5
7.4	Работа со сканерами безопасности Сканер-ВС и MaxPatrol /Лаб/	9	2	ПК-14, ПК-26	Л2.1-Л2.5
7.5	Проработка лекционного материала, подготовка к семинарским занятиям и лабораторным работам /Ср/	9	10	ПК-14, ПК-26	Л2.1-Л2.5
	Раздел 8. Программно-аппаратные средства защиты информации в сетях передачи данных				
8.1	Технологии построения частных виртуальных сетей (VPN). Построение VPN на примере систем линейки АПКШ «Континент» /Лек /	9	2	ПК-14, ПК-26	Л.1.2-Л1.4; Л2.1-Л2.4, Л4.1; Э4, Э7
8.2	Построение VPN на примере систем линейки VipNet /Пр /	9	3	ПК-14, ПК-26	Э7
8.3	Проработка лекционного материала, подготовка к семинарским занятиям /Ср/	9	10	ПК-14, ПК-26	Л.1.2-Л1.4; Л2.1-Л2.4,

					Л4.1; Э4, Э7
	Раздел 9. Задачи и технологии сертификации программно-аппаратных средств на соответствие требованиям ИБ				
9.1	Понятие сертификации ПАСЗИ. Порядок проведения сертификации программно-аппаратных средств обеспечения ИБ /Лек/	9	2	ПК-14, ПК-26	Э1, Э2
9.2	Сравнительная характеристика российских комплексов программно-аппаратных средств. Достоинства и недостатки /Пр/	9	3	ПК-14, ПК-26	Л1.1-Л1.4; Л2.1-2.5, Л3.1; Л4.1
9.3	Проработка лекционного материала, подготовка к семинарским занятиям /Ср/	9	10	ПК-14, ПК-26	Э1, Э2,
	Раздел 10. Аттестация				
10.1	Подготовка к экзамену /Экзамен/	9	36	ПК-14, ПК-26	Л1.1-Л1.4; Л2.1-2.5, Л3.1; Л4.1; Э1-Э8

5 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

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

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

6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1 Основная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/100% онлайн
Л1.1	Афанасьев А.А., Веденьев Л.Т., Воронцов А.А.	Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам; http://e.lanbook.com/books/element.php?pl1_id=5114: для ВПО	Горячая линия-Телеком, 2012	100 % онлайн
Л1.2	Бирюков А.А.	Информационная безопасность: защита и нападение; http://e.lanbook.com/books/element.php?pl1_id=39990: Учебник	М: ДМК Пресс, 2012	100 % онлайн
Л1.3	М.А. Борисов, И.В. Заводцев, И.В. Чижов	Основы программно-аппаратной защиты информации; http://elibrary.ru/item.asp?id=19865165	М.: Либроком, 2012	100 % онлайн
Л1.4	М.О. Таньгин	Программно-аппаратные системы защиты информации; http://elibrary.ru/item.asp?id=19599479	Курск: Юго-западный гос. ун-т, 2013	100 % онлайн

6.1.2 Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/100% онлайн
Л2.1	Анин Б.Ю.	Защита компьютерной информации: Учебник	СПб.: БХВ, 2000	23
Л2.2	Платонов В.В.	Программно-аппаратные средства обеспечения	М.: Академия,	1

		информационной безопасности вычислительных сетей: Учебное пособие	2006	
Л2.3	Шаньгин В.Ф.	Защита компьютерной информации. Эффективные методы и средства: Учебное пособие	М.: ДМК, 2008	1
Л2.4	Ададуров С.Е., Глухов А.П., Корниенко А.А., Диасамидзе С.В., Корниенко А.А.	Информационная безопасность и защита информации на железнодорожном транспорте: Учебное пособие для ВО	М.: УМЦ по образованию на ж.-д. трансп., 2014	30
Л2.5	Никитин И. А. , Цулая М. Т.	Процессы анализа и управления рисками в области ИТ; Учебная литература для ВУЗов; http://biblioclub.ru/index.php?page=book_red&id=429089:	М.: Национальный Открытый Университет «ИНТУИТ», 2016	100 % онлайн
6.1.3 Методические разработки				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/100% онлайн
Л3.1	Бутин А.А.	Методы и средства защиты информации от несанкционированного доступа. Программно-аппаратный уровень: Учебное пособие	Иркутск: ИрГУПС, 2015	43
6.1.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/100% онлайн
Л4.1	Завгородний В.И.	«Комплексная защита информации в компьютерных системах»; http://www.proklondike.com/books/defence/zavgorodniy_complex_defence.html; http://bezopasnik.org/article/book/zavgorodniy_-_Complex_Defend.pdf		100% онлайн

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»		
Э1	Сайт ФСТЭК РФ	http://fstec.ru/
Э2	Сайт ФСБ РФ	http://www.fsb.ru/
Э3	Сайт призводителя ruToken	http://www.rutoken.ru/
Э4	Сайт "Код безопасности"	http://www.securitycode.ru
Э5	Сайт производителя Dallas Lock	https://www.dallaslock.ru/
Э6	Сайт производителя СЗИ "Аккорд"	http://www.accord.ru/
Э7	Сайт производителя линейки "ViPNet"	http://www.infotecs.ru/
Э8	Материалы «Комплексная защита информации в компьютерных системах»	http://padaread.com/
Э9	Сайт производителя СЗИ СтражNT	http://guardnt.ru

6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)	
6.3.1 Перечень базового программного обеспечения	
6.3.1.1	ОС Microsoft Windows XP Professional with Service Pack 2, лицензия Open License; количество – 427;
6.3.1.2	ОС Microsoft Windows 7;
6.3.1.3	Офисный пакет Microsoft Office 2010, OpenLicense; количество – 155;
6.3.2 Перечень специализированных средств и программного обеспечения	
6.3.2.1	Сканер MBSA (бесплатное программное обеспечение (ПО));
6.3.2.2	«Сканер-ВС» (бесплатное ПО для вузов);
6.3.2.3	Персональные идентификаторы ruToken;
6.3.2.4	VirtualBox (бесплатное ПО);
6.3.2.5	СЗИ Dallas Lock 8.0-C ОС Windows (бесплатная лицензия для вузов по Договору с производите-

	лем);
6.3.2.6	СЗИ Dallas Lock 8.0 ОС Linux (бесплатная лицензия для вузов по Договору с производителем);
6.3.2.7	СЗИ Secret Net 6.0 К (лицензия);
6.3.2.8	Электронный замок «Соболь-PCI»;
6.3.2.9	Средство антивирусной защиты 360 Total Security;
6.3.2.10	Средство антивирусной защиты Dr. Web cureit;
6.3.2.11	Средство антивирусной защиты Dr_Web (demo);
6.3.2.12	Средство антивирусной защиты Касперский_IS (demo);
6.3.2.13	Средство криптографической защиты информации «КриптоАРМ» (demo);
6.3.2.14	Учебная программа Rohos (demo);
6.3.2.15	Учебная программа Криптосейф (demo);
6.3.2.16	Учебная программа Криптоофис (demo);
6.3.2.17	MaxPatrol-8 (бесплатная лицензия для вузов);
6.3.2.18	XSpider (бесплатная лицензия для вузов).
6.3.3 Перечень информационных справочных систем	
6.3.3.1	Информационно-справочная система КонсультантПлюс http://www.consultant.ru

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

1	Учебные аудитории для проведения занятий лекционного типа, 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.
2	Учебная лаборатория «Средства и методы защиты информации», Д-523. Оснащена компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечена доступом в электронную информационно-образовательную среду ИрГУПС. Перечень установленных программных средств: MicrosoftOffice 2010, OpenOffice 3.0.1, 7-zip, BorlandDelphi 7, AbodeReaderXI, MicrosoftSecurityEssentials, а также специализированное ПО.
3	Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Помещения для самостоятельной работы обучающихся: – читальные залы; – учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507.

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на лабораторной работе.
Практические (семинарские) занятия	Обобщение, расширение и углубление пройденного материала на лекции. 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. Контроль качества усвоения пройденного материала.
Лабораторная работа	Один из видов практической работы, проводимой с целью углубления и закрепления теоретических знаний, развития навыков самостоятельной деятельности. Включает подготовку необходимых программно-аппаратных средств, составление плана работы, ее проведение и написание отчета.
Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным	

рабочей программой дисциплины, размещен в электронной информационно-образовательной среде Ир-ГУПС, доступной обучающемуся через его личный кабинет.

Приложение 1 к рабочей программе по дисциплине
Б1.Б.1.28 Программно-аппаратные средства
обеспечения информационной безопасности

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине
Б1.Б.1.28 «Программно-аппаратные средства обеспечения информационной безопасности»

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

Дисциплина «**Программно-аппаратные средства обеспечения информационной безопасности**» участвует в формировании компетенций:

ПК-14: способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации;
ПК-26: способность администрировать подсистему информационной безопасности автоматизированной системы.

Таблица траекторий формирования у обучающихся компетенций ПК-14, ПК-26 при освоении образовательной программы

Код компетенции	Наименование компетенции	Индекс и наименование дисциплин/ практик, участвующих в формировании компетенции	Семестр изучения дисциплины	Этапы формирования компетенции
ПК-14	способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Б1.Б.1.25 Техническая защита информации	6	1
		Б1.Б.1.23 Криптографические методы защиты информации	7	2
		Б1.Б.1.28 Программно-аппаратные средства обеспечения информационной безопасности	8, 9	3
		Б2.Б.05(П) Производственная - технологическая	А	4
ПК-26	способность администрировать подсистему информационной безопасности автоматизированной системы	Б1.Б.1.19 Безопасность операционных систем	5, 6	1
		Б2.Б.02(П) Производственная - по получению профессиональных умений и опыта профессиональной деятельности	6	1
		Б1.Б.1.20 Безопасность сетей ЭВМ	6, 7	2
		Б1.Б.1.21 Безопасность систем баз данных	7, 8	2
		Б2.Б.03(П) Производственная - эксплуатационная	8	3
		Б1.Б.1.28 Программно-аппаратные средства обеспечения информационной безопасности	8, 9	4

Таблица соответствия уровней освоения компетенций ПК-14, ПК-26

планируемым результатам обучения

Код компетенции	Наименование компетенции	Наименования разделов дисциплины	Уровни освоения компетенций	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции)
ПК-14	способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических	Раздел 1. Основные категории требований к программно-аппаратной реализации средств обеспечения ИБ. Раздел 2. Базовые	Минимальный уровень	Знать методики проведения проверки эффективности работы программно-аппаратных средств защиты информации (ПАСЗИ);
				Уметь организовать проверки эффективности работы ПАСЗИ;

	и технических средств защиты информации	принципы применения ПАСЗИ, основные классы ПАСЗИ. Раздел 3. Программно-аппара-ные средства, реализующие отдельные функциональные требования по защите, их технологические особенности, взаимодействие с общесистемными компонентами АС. Раздел 4. Аппаратные средства аутентификации; методы и средства хранения ключевой информации. Раздел 5. Методы и средства разграничения доступа к компонентам АС; технологии защиты от несанкционированного доступа (НСД) к информации. Раздел 6. Средства антивирусной защиты информации. Раздел 7. Технологии анализа защищенности АС. Раздел 8. Программно-аппа-ратные средства защиты информации в сетях передачи данных. Раздел 9. Задачи и технологии сертификации программно-аппаратных средств на соответствие требованиям ИБ.		Владеть навыками тестирования работоспособности ПАСЗИ;
			Базовый уровень	Знать способы устранения нештатных ситуаций в процессе функционирования ПАСЗИ;
				Уметь проводить проверки эффективности работы ПАСЗИ;
				Владеть навыками анализа работы ПАСЗИ и выявления наличия нештатных ситуаций.
			Высокий уровень	Знать методики проведения проверки эффективности работы и способы устранения нештатных ситуаций;
				Уметь проводить проверки эффективности работы ПАСЗИ и устранять нештатные ситуации;
				Владеть навыками тестирования работоспособности ПАСЗИ и анализа его результатов.
ПК-26	способность администрировать подсистему информационной безопасности автоматизированной системы	Раздел 1. Основные категории требований к программно-аппаратной реализации средств обеспечения ИБ**.** Раздел 2. Базовые принципы применения ПАСЗИ, основные классы ПАСЗИ. Раздел 3. Программно-аппара-ные средства, реализующие отдельные функциональные требования по защите, их технологические особенности, взаимодействие с общесистемными компонентами АС.	Минимальный уровень	Знать основные классы штатных и добавочных ПАСЗИ;
				Уметь устанавливать добавочные программно-аппаратные средства обеспечения ИБ;
				Владеть навыками администрирования отдельных защитных механизмов ПАСЗИ.
			Базовый уровень	Знать базовые сервисы безопасности ПАСЗИ;
				Уметь настраивать основные механизмы в соответствии с политикой ИБ;
				Владеть навыками анализа рынка современных ПАСЗИ.
			Высокий уровень	Знать функциональные возможности представителей классов ПАСЗИ;
				Уметь в полной мере адми-

		Раздел 4. Аппаратные средства аутентификации; методы и средства хранения ключевой информации. Раздел 5. Методы и средства разграничения доступа к компонентам АС; технологии защиты от несанкционированного доступа (НСД) к информации. Раздел 6. Средства антивирусной защиты информации. Раздел 7. Технологии анализа защищенности АС. Раздел 8. Программно-аппа-ратные средства защиты информации в сетях передачи данных. Раздел 9. Задачи и технологии сертификации программно-аппаратных средств на соответствие требованиям ИБ.		нистрировать механизмы безопасности ПАСЗИ; Владеть навыками администрирования комплексной системы ПАСЗИ.

Программа контрольно-оценочных мероприятий за период изучения дисциплины

№	Неделя	Наименование контрольно-оценочного мероприятия	Объект контроля (понятия, тема / раздел дисциплины, компетенция, и т.д.)		Наименование оценочного средства (форма проведения)
8 семестр					
1	1	Текущий контроль	Работа с пакетом «КриптоАРМ»	ПК-14, ПК-26	Защита лабораторной работы
2	3	Текущий контроль	Работа с пакетом «Криптосейф»	ПК-14, ПК-26	Защита лабораторной работы
3	7	Текущий контроль	Работа с пакетом «Криптоофис»	ПК-14, ПК-26	Защита лабораторной работы
4	11	Текущий контроль	Использование ключевого носителя ruToken (на базе пакета Rohos)	ПК-14, ПК-26	Защита лабораторной работы
5	15	Текущий контроль	ЭЗ Соболь-PCI. Настройка и эксплуатация. Управление пользователями. Диагностика устройства. Настройка контроля целостности. Регистрация событий	ПК-14, ПК-26	Защита лабораторной работы
6	18	Текущий контроль	СЗИ НСД DL: установка средства, настройка параметров входа в систему; реализация дискреционного разграничения доступа	ПК-14, ПК-26	Защита лабораторной работы
10	1-18	Текущий контроль	Индивидуальное выступление с докладом на семинарском занятии по теме в соответствии с РПД по данной дисциплине	ПК-14, ПК-26	Сообщение, доклад (устно); наличие презентации

11	18	Промежуточная аттестация – зачет	Разделы 1 – 5.3 РПД	ПК-14, ПК-26	Собеседование (устно)
9 семестр					
1	2	Текущий контроль	СЗИ НСД DL: реализация мандатного разграничения доступа; механизм замкнутой программной среды	ПК-14, ПК-26	Защита лабораторной работы
2	4	Текущий контроль	СЗИ НСД DL: протоколирование событий; настройка механизма контроля целостности; администрирование системы защиты	ПК-14, ПК-26	Защита лабораторной работы
3	6	Текущий контроль	ЗИ от НСД SN AB: установка средства, дискреционное разграничение доступа	ПК-14, ПК-26	Защита лабораторной работы
4	8	Текущий контроль	СЗИ от НСД SN AB: настройка контроля целостности	ПК-14, ПК-26	Защита лабораторной работы
5	10	Текущий контроль	СЗИ от НСД SN AB: регистрация событий	ПК-14, ПК-26	Защита лабораторной работы
6	12	Текущий контроль	СЗИ от НСД SN AB: работа с электронным идентификатором; затирание данных	ПК-14, ПК-26	Защита лабораторной работы
7	14	Текущий контроль	Эксплуатация средств антивирусной защиты 360 Total Security; Dr. Web cureit; Dr_Web; Касперский_IS	ПК-14, ПК-26	Защита лабораторной работы
8	16	Текущий контроль	Работа со сканерами безопасности Сканер-ВС и MaxPatrol	ПК-14, ПК-26	Защита лабораторной работы
9	18	Текущий контроль	Работа со сканерами безопасности Сканер-ВС и MaxPatrol	ПК-14, ПК-26	Защита лабораторной работы
10	1-18	Текущий контроль	Индивидуальное выступление с докладом на семинарском занятии по теме в соответствии с РПД по данной дисциплине	ПК-14, ПК-26	Сообщение, доклад (устно); наличие презентации
11	18	Тест	Разделы 1 –9 РПД	ПК-14, ПК-26	Перечень тестовых заданий
12	18	Промежуточная аттестация – экзамен	Разделы 1 – 9 РПД	ПК-14, ПК-26	Собеседование (устно)

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

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

Текущий контроль успеваемости – основной вид систематической проверки знаний, умений, навыков обучающихся. Задача текущего контроля – оперативное и регулярное управление учебной деятельностью обучающихся на основе обратной связи и корректировки. Результаты оценивания учитываются в виде средней оценки при проведении промежуточной аттестации.

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

Перечень оценочных средств, используемых для оценивания компетенций на различных этапах их формирования, а так же краткая характеристика этих средств приведены в таблице

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Защита лабораторной работы	Средство, позволяющее оценить умение обучающегося письменно излагать суть поставленной задачи, самостоятельно применять стандартные методы решения поставленной задачи с использованием имеющейся лабораторной базы, проводить анализ полученного результата работы. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся	Темы лабораторных работ и требования к их защите
2	Сообщение, доклад	Продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Темы докладов, сообщений
3	Тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий
4	Зачет	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень теоретических вопросов и практических заданий (билетов) к зачету
5	Экзамен	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень теоретических вопросов и практических заданий (билетов) к экзамену

Критерии и шкалы оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета и экзамена, а также шкала для оценивания уровня освоения компетенций

Шкалы оценивания	Критерии оценивания	Уровень освоения компетенций
«зачтено»	Обучающийся правильно ответил на теоретические вопросы. Показал отличные знания в рамках учебного материала. Правильно выполнил практические задания. Показал отличные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на все дополнительные вопросы	Высокий
	Обучающийся с небольшими неточностями ответил на теоретические вопросы. Показал хорошие знания в рамках учебного материала. С небольшими неточностями выполнил практические задания. Показал хорошие умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на большинство дополнительных вопросов	Базовый
	Обучающийся с существенными неточностями ответил на теоретические вопросы. Показал удовлетворительные знания в рамках учебного материала. С существенными неточ-	Минимальный

	ностями 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	
«не зачтено»	Обучающийся при ответе на теоретические вопросы и при выполнении практических заданий продемонстрировал недостаточный уровень знаний и умений при решении задач в рамках учебного материала. При ответах на дополнительные вопросы было допущено множество неправильных ответов	Компетенции не сформированы

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Доклад, сообщение

Шкала оценивания	Критерии оценивания
«отлично»	Доклад создан с использованием компьютерных технологий (презентация PowerPoint,Flash–презентация, видео-презентация и др.) Использованы дополнительные источники информации. Содержание заданной темы раскрыто в полном объеме. Отражена структура доклада (вступление, основная часть, заключение, присутствуют выводы и примеры). Оформление работы. Оригинальность выполнения (работа сделана самостоятельно, представлена впервые)
«хорошо»	Доклад создан с использованием компьютерных технологий (презентация PowerPoint,Flash–презентация, видео-презентация и др.) Содержание доклада включает в себя информацию из основных источников (методическое пособие), дополнительные источники информации не использовались. Содержание заданной темы раскрыто не в полном объеме. Структура доклада сохранена (вступление, основная часть, заключение, присутствуют выводы и примеры)
«удовлетворительно»	Доклад сделан устно, без использования компьютерных технологий. Содержание доклада ограничено информацией только из методического пособия. Содержание заданной темы раскрыто не в полном объеме. Отсутствуют выводы и примеры. Оригинальность выполнения низкая
«неудовлетворительно»	Доклад сделан устно, без использования компьютерных технологий и других наглядных материалов. Содержание ограничено информацией только из методического пособия. Заданная тема доклада не раскрыта, основная мысль сообщения не передана

Тест (структура теста по компетенциям)

Проверяемый уровень освоения компетенции компетенций (части компетенций, элементов компетенций)	Минимальное количество тестовых заданий на один раздел программы	Рекомендуемые формы тестовых заданий	Количество баллов за одно тестовое задание
Минимальный уровень освоения компетенции	19	Тестовые задания с выбором одного правильного ответа из нескольких	1
		Тестовые задания с выбором нескольких правильных ответов из множества ответов	
		Тестовые задания на установление соответствия	
		Тестовые задания на установление правильной последовательности	
Базовый уровень освоения компетенции	8	Тестовые задания с закрытым конструируемым ответом (ввод одного или нескольких слов, цифры)	4
Высокий уровень освоения компетенции	6	Тестовые задания со свободно конструируемым ответом (интервью, эс-	7

		се) Структурированный тест Кейсы	

Тест (шкала и критерии оценивания, уровни освоения)

Шкалы оценивания		Критерии оценивания	Уровень освоения компетенции
«отлично»	«зачтено»	Обучающийся при тестировании набрал 86-93 баллов	Высокий
«хорошо»		Обучающийся при тестировании набрал 69-85 баллов	Базовый
«удовлетворительно»		Обучающийся при тестировании набрал 53-68 баллов	Минимальный
«неудовлетворительно»	«не зачтено»	Обучающийся при тестировании набрал 0-52 баллов	Компетенция не сформирована

Защита лабораторной работы

Шкала оценивания	Критерии оценивания
«отлично»	Лабораторная работа выполнена в обозначенный преподавателем срок, письменный отчет без замечаний. Лабораторная работа выполнена обучающимся в полном объеме с соблюдением необходимой последовательности. Обучающийся работал полностью самостоятельно; показал необходимые для проведения работы теоретические знания, практические умения и навыки. Работа (отчет) оформлена аккуратно, в наиболее оптимальной для фиксации результатов форме
«хорошо»	Лабораторная работа выполнена в обозначенный преподавателем срок, письменный отчет с небольшими недочетами. Лабораторная работа выполнена обучающимся в полном объеме и самостоятельно. Допущены отклонения от необходимой последовательности выполнения, не влияющие на правильность конечного результата. Работа показывает знание обучающимся основного теоретического материала и овладение умениями, необходимыми для самостоятельного выполнения работы. Допущены неточности и небрежность в оформлении результатов работы (отчета)
«удовлетворительно»	Лабораторная работа выполнена с задержкой, письменный отчет с недочетами. Лабораторная работа выполняется и оформляется обучающимся при посторонней помощи. На выполнение работы затрачивается много времени. Обучающийся показывает знания теоретического материала, но испытывает затруднение при самостоятельной работе с источниками знаний или приборами
«неудовлетворительно»	Лабораторная работа не выполнена, письменный отчет не представлен. Результаты, полученные обучающимся не позволяют сделать правильных выводов и полностью расходятся с поставленной целью. Показывается плохое знание теоретического материала и отсутствие необходимых умений. Лабораторная работа не выполнена, у учащегося отсутствуют необходимые для проведения работы теоретические знания, практические умения и навыки

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

3.1 Перечень типовых тем докладов, сообщений

1. Комплекс национальных стандартов Российской Федерации ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»;
2. Биометрические методы идентификации и аутентификации. Процедуры биометрического опознания. Устройства биометрической идентификации и аутентификации для автоматизированных систем и виды контроля;
3. Линейка СЗИ Acronis;
4. АПК Аргус;
5. Микропроцессорные или интеллектуальные карточки. Бесконтактные карточки. Среда использования смарт-карт в персональных компьютерах;
6.Электронные идентификаторы eToken;
7. Программно-аппаратный комплекс защиты информации от НСД “Аккорд”;
8. СЗИ Device Lock;
9. DLP-система Info Watch Traffic Monitor Enterprise Edition;
10. СЗИ Secret Net Studio;
11. СЗИ vGate for VMvare Infrastructure;
12. Сканер-ВС, сканеры MaxPatrol и "Ревизор сети";
13. Построение VPN на примере систем линейки VipNet;
14. Сравнительная характеристика российских комплексов программно-аппаратных средств. Достоинства и недостатки.

3.2. Тест

1. Выберите правильное определение термина «обладатель информации»:
   а) лицо, самостоятельно создавшее информацию;
   б) лицо, получившее на основании закона или договора право разрешать или ограничивать доступ к информации;
   в) лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
   г) лицо, самостоятельно создавшее информацию либо получившее право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.
2. Выберите правильное определение термина «предоставление информации»:
   а) действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;
   б) действия, направленные на распространение сведений в средствах массовой информации;
   в) действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;
   г) действия, направленные на получение информации как определённым, так и неопределённым кругом лиц или передачу информации как определенному, так и неопределённому кругу лиц.
3. Выберите правильное определение термина «контролируемая зона»:
   а) пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств;
   б) часть здания, в котором исключено неконтролируемое пребывание посторонних лиц, транспортных, технических и иных материальных средств;
   в) пространство (территория, здание, часть здания, помещение), в котором действует особый режим наблюдения за всеми сотрудниками организации;

г) помещение, в котором постоянно, независимо от окружающих факторов ведётся систематический контроль и надзор за действиями пользователей.

4. К рекомендуемым методам и способам защиты информации в информационных системах относятся (выберите все верные варианты ответов):

а) методы и способы защиты информации от несанкционированного доступа;

б) методы и способы сокрытия информации от внутренних нарушителей;

в) методы и способы устранения конкурентов;

г) методы и способы защиты информации от утечки по техническим каналам;

5. Средствами защиты информации, подлежащими сертификации, являются (выберите все верные варианты ответов):

а) строительные материалы, используемые для отделки помещений, в которых размещаются отдельные элементы АС;

б) детали интерьера, используемые для размещения АИС;

в) средства контроля эффективности применения средств защиты информации;

г) средства контроля эффективности прочности ограждений;

д) средства защиты информации (технические, программные, программно-аппаратные) от НСД, блокировки доступа и нарушения целостности.

6. «Несанкционированный доступ к информации» - это:

а) доступ, реализующий возможности совокупности физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;

б) доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств;

в) доступ с использованием совокупности средств технической разведки и прочих средств, которыми добывается защищаемая информация;

г) доступ к информации, реализуемый путём уничтожения технических средств информационной системы.

7. «Персональный идентификатор» — это

а) устройство для хранения зашифрованной информации пользователя;

б) устройство для хранения информации, необходимой при идентификации и аутентификации пользователя;

в) устройство для хранения журнала аудита.

8. Механизм контроля целостности СЗИ Secret Net предназначен для:

а) формирования цифровых отпечатков данных;

б) контроля информационных потоков;

в) слежения за неизменностью содержимого ресурсов компьютера.

9. Механизм замкнутой программной среды СЗИ Secret Net и Dallas Lock предназначен для

а) ограничения использования программного обеспечения на компьютере;

б) установки ограниченного количества программ;

в) сбора сведений об используемых приложениях.

10. В СЗИ Secret Net пользователю с уровнем допуска "конфиденциально" разрешается выполнять чтение файлов с категориями

а) «конфиденциально»;

б) «секретно»;

в) «строго конфиденциально»,

г) «неконфиденциально».

11. Межсетевой экран служит для:

а) разграничения доступа в помещения АИС;

б) фильтрации трафика при передачи данных;

в) защиты от утечек информации путем экранирования поверхности стен;

г) контроля целостности программного обеспечения.

12. ПСКЗИ ШИПКА – это:
    а) средство контроля целостности;
    б) средство проведения аудита АИС;
    в) средство хранения ключевой информации;
    г) средство шифрования информации;
    д) средство для идентификации и аутентификации пользователей.
13. ЭЗ «Соболь»предназначен для:
    а) разграничения доступа к ресурсам АИС;
    б) защиты от утечки информации по техническим каналам;
    г) доверенной загрузки штатной операционной системы.
14. СЗИ SecretNet имеет контуры _____ управления:
    а) оперативного;
    б) централизованного;
    в) локального.
    г) защищенного.
15. СЗИ Dallas Lock имеет в своем составе следующие подсистемы:
    а) разграничения доступа;
    б) идентификации и аутентификации;
    в) защиты от утечки по виброакустическому каналу.
16. Механизмы защиты СЗИ SecretNet входят в состав:
    а) агента сервера безопасности (СБ);
    б) клиента СБ.
17. Задача оперативного реагирования в СЗИ SecretNet принадлежит
    а) программе «Монитор»;
    б) программе «Журналы».
18. Механизм контроля целостности реализован в следующих средствах защиты информации:
    а) СЗИ Dallas Lock;
    б) СЗИ SecretNet;
    в) ПАК Аккорд;
    д) СЗИ Страж NT.
19. Основные функции СБ СЗИ SecretNet:
    а) взаимодействие с клиентами СБ;
    б) взаимодействие с агентами СБ;
    в) обеспечение защиты клиентов СБ;
    г) непосредственное обеспечение защиты информационных ресурсов АИС.
20. Максимально возможное количество категорий конфиденциальности в СЗИ Secret Net 7.x равно _____ (16).
21. В СЗИ Secret Net категорию конфиденциальности можно назначить для следующих ресурсов: каталоги и файлы на дисках с файловой системой _____ (NTFS).
22. Эффективным средством защиты от утечки информации из АИС показали себя _____ (DLP) – системы.
23. АПКШ «Континент» является средством построения частных _____ (виртуальных) сетей.
24. Сканер-ВС, сканеры MaxPatrol и "Ревизор сети" представляют собой средства контроля _____ (защищенности) компьютерной сети.
25. Dr. Web является сертифицированным средством защиты от _____ (вредоносного) программного обеспечения.
26. Info Watch Traffic Monitor Enterprise Edition – это система защиты от _____ (утечки) инсайдерской информации.
27. АМДЗ «Аккорд» является средством _____ (доверенной) загрузки штатной операционной системы.

28. Как в СЗИ Secret Net происходит включение режима хранения пароля в идентификаторе?
    (Основной тезис: происходит добавление в базу данных Secret Net сведений о включении для пользователя режима хранения пароля в идентификаторе. Одновременно с этой операцией выполняется запись пароля в идентификатор. После включения режима пароль пользователя при входе в систему не вводится с клавиатуры, а считывается из идентификатора).
29. Каким образом в СЗИ Secret Net происходит присвоение пользователю персонального идентификатора?
    (Основной тезис: происходит добавление в базу данных Secret Net сведений о том, что пользователю принадлежит персональный идентификатор данного типа с уникальным серийным номером).
30. Каким образом в СЗИ Secret Net реализуется затирание файлов?
    (Основной тезис: при действии механизма затирания в область диска, где физически было расположено содержимое удаленного файла, записывается последовательность случайных чисел).
31. СЗИ SecretNet: опишите функции сервера безопасности (СБ).
32. СЗИ SecretNet: опишите функции агента СБ.
33. СЗИ SecretNet: опишите функции программ «Монитор» и «Журналы».

3.3. Перечень теоретических вопросов к зачету

1. Руководящие и методические документы Гостехкомиссии и ФСТЭК РФ.
2. Профили защиты средств защиты информации.
3. Обоснование необходимости применения добавочных ПАСЗИ, принципы использования.
4. Основные классы добавочных программно-аппаратных средств, обеспечивающих повышенный уровень защиты.
5. Характеристика, основные сервисы и механизмы добавочных ПАСЗИ.
6. Типы технологий усиленной идентификации и аутентификации, разграничения доступа к информации.
7. Общие сведения о методах аутентификации. Магнитные диски. Магнитные и интеллектуальные карты.
8. Устройство хранения ключей типа Touch Memory (iButton).
9. Электронные идентификаторы ruToken; ПСКЗИ ШИПКА.
10. Электронный замок (ЭЗ) «Соболь»: назначение, варианты применения, требования к оборудованию и ПО, комплектация.
11. ЭЗ «Соболь»: основные принципы функционирования.
12. ЭЗ «Соболь»: настройка и эксплуатация устройства.
13. СЗИ от НСД «Dallas Lock» (DL): назначение и состав системы защиты.
14. DL: общие принципы организации защиты ресурсов.
15. DL: механизмы управления доступом и защиты объектов.

3.4. Перечень типовых простых практических заданий к зачету

Формируется на основании требований к выполнению лабораторных работ и результатов их защиты.

3.5. Перечень типовых практических заданий к зачету

Формируется на основании требований к выполнению лабораторных работ и результатов их защиты.

3.6. Перечень теоретических вопросов к экзамену

1. Руководящие и методические документы Гостехкомиссии и ФСТЭК РФ.
2. Профили защиты средств защиты информации.
3. Обоснование необходимости применения добавочных ПАСЗИ, принципы использования.
4. Основные классы добавочных программно-аппаратных средств, обеспечивающих повышенный уровень защиты.
5. Характеристика, основные сервисы и механизмы добавочных ПАСЗИ.
6. Типы технологий усиленной идентификации и аутентификации, разграничения доступа к информации.
7. Общие сведения о методах аутентификации. Магнитные диски. Магнитные и интеллектуальные карты.
8. Устройство хранения ключей типа Touch Memory (iButton).
9. Электронные идентификаторы ruToken. ПСКЗИ ШИПКА.
10. Электронный замок (ЭЗ) «Соболь»: назначение, варианты применения, требования к оборудованию и ПО, комплектация.
11. ЭЗ «Соболь»: основные принципы функционирования.
12. ЭЗ «Соболь»: настройка и эксплуатация устройства.
13. СЗИ от НСД «Dallas Lock» (DL): назначение и состав системы защиты.
14. DL: общие принципы организации защиты ресурсов.
15. DL: механизмы управления доступом и защиты объектов.
16. СЗИ SecretNet ОС Windows (автономный вариант) (SN AB): архитектура и компоненты системы.
17. SN AB: защитные механизмы.
18. SN (сетевой вариант) (SN CB): назначение и варианты применения системы.
19. SN CB: общая архитектура и компоненты.
20. SN CB: управление доступом пользователей к ресурсам.
21. SN CB: средства централизованного и оперативного управления.
22. СЗИ Страж NT.
23. Программно-аппаратный комплекс защиты информации от НСД “Аккорд”.
24. СЗИ Device Lock.
25. DLP-система Info Watch Traffic Monitor Enterprise Edition.
26. СЗИ Secret Net Studio.
27. СЗИ vGate for VMvare Infrastructure.
28. Технологии антивирусной защиты информации.
29. Цели и задачи проведения мероприятий по оценке уровня защищенности АС.
30. Средство анализа защищенности АС «Агент инвентаризации (ОС Windows)».
31. Средство фиксации и контроля исходного состояния программного комплекса "ФИКС".
32. Средство создания модели системы разграничения доступа "Ревизор 1 XP".
33. Средство контроля защищенности от НСД "Ревизор 2 XP".
34. Построение VPN на примере систем линейки АПКШ «Континент».
35. Построение VPN на примере систем линейки VipNet.
36. Порядок проведения сертификации программно-аппаратных средств обеспечения ИБ.

3.7. Перечень типовых простых практических заданий к экзамену

Формируется на основании требований к выполнению лабораторных работ и результатов их защиты.

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

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

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Сообщение, доклад	Обучаемый получает тему от преподавателя изучает литературу (не менее 3-4 источников, включая самостоятельный поиск в интернете), готовит доклад (сообщение), объемом до 10 стр. текста размером 12 пунктов, интервал 1,2; предоставляет доклад (сообщение) преподавателю, отвечает на его вопросы. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.
Тест	Обучаемый самостоятельно отвечает на вопросы теста в письменной форме. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.
Защита лабораторной работы	Обучаемый самостоятельно, под руководством преподавателя выполняет лабораторную работу на заданную тему. Тема (задание) предлагается в конкретном виде. Методы и инструменты для ее разработки предлагаются преподавателем. После выполнения задания обучаемый готовит пояснительную записку, предоставляет ее преподавателю, отвечает на его вопросы в ходе собеседования (защиты). Оценка ставится по представленным результатам и результатам собеседования. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.

Для организации и проведения промежуточной аттестации (в форме зачета/экзамена) составляются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы:

– перечень теоретических вопросов к зачету/экзамену для оценки знаний;

– перечень типовых простых практических заданий к зачету/экзамену для оценки умений;

– перечень типовых практических заданий к зачету/экзамену для оценки навыков и (или) опыта деятельности.

Перечень теоретических вопросов и перечни типовых практических заданий разного уровня сложности к зачету/экзамену обучающиеся получают в начале семестра через электронную информационно-образовательную среду ИрГУПС (личный кабинет обучающегося).

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

При проведении промежуточной аттестации в форме зачета преподаватель может воспользоваться результатами текущего контроля успеваемости в течение семестра. 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»

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

Промежуточная аттестация в форме экзамена проводится путем устного собеседования по билетам. Билеты составлены таким образом, что в каждый из них включал в себя теоретические вопросы и практические задания.

Билет содержит: два теоретических вопроса для оценки знаний. Теоретические вопросы выбираются из перечня вопросов к экзамену; три практических задания: два из них для оценки умений (выбираются из перечня типовых простых практических заданий к экзамену); третье практическое задание для оценки навыков и (или) опыта деятельности (выбираются из перечня типовых практических заданий к экзамену).

Распределение теоретических вопросов и практических заданий по экзаменационным билетам находится в закрытом для обучающихся доступе. Разработанный комплект билетов (25-30 билетов) не выставляется в электронную информационно-образовательную среду ИрГУПС, а хранится на кафедре-разработчике ФОС на бумажном носителе в составе ФОС по дисциплине.

На экзамене обучающийся берет билет, для подготовки ответа на экзаменационный билет обучающемуся отводится время в пределах 45 минут. В процессе ответа обучающегося на вопросы и задания билета, преподаватель может задавать дополнительные вопросы.

Каждый вопрос/задание билета оценивается по четырехбалльной системе, а далее вычисляется среднее арифметическое оценок, полученных за каждый вопрос/задание. Среднее арифметическое оценок округляется до целого по правилам округления.

Образец экзаменационного билета

ИРГУПС 20__-20__ учебный год	**Экзаменационный билет № 1** **по дисциплине «_____»** **__ ____ семестр**	Утверждаю: Заведующий кафедрой «_____» ИрГУПС _____
1. …… 2. …… 3. …….. 4. …….. 5 ……..……. Варианты размеров билета: Билет формата А5 – 148*210мм Билет формата А4 – 210*297мм		

В разделе «Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы» приведены типовые контрольные задания, для оценки результатов освоения образовательной программы. Задания, по которым проводятся контрольно-оценочные мероприятия, оформляются в соответствии с формами оформления оценочных средств, приведенными ниже, и не выставляются в электронную информационно-образовательную среду ИрГУПС, а хранятся на кафедре-разработчике ФОС на бумажном носителе в составе ФОС по дисциплине.