ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

УТВЕРЖДЕНА
приказом ректора
от «07» июня 2021 г. № 78

Б1.О.39 Программно-аппаратные средства защиты информации

рабочая программа дисциплины

Специальность – 10.05.03 Информационная безопасность автоматизированных систем
Специализация – № 5 Безопасность открытых информационных систем
Квалификация выпускника – Специалист по защите информации
Форма и срок обучения – 5 лет 6 месяцев, очная форма
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 5
Часов по учебному плану (УП) – 180

Формы промежуточной аттестации в семестрах:
экзамен 9

Распределение часов дисциплины по семестрам

Семестр	9	**Итого**
Число недель в семестре	17	
Вид занятий	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*	**102**	**102**
– лекции	34	34
– лабораторные	34	34
– практические (семинарские)	34	34
Самостоятельная работа	**42**	**42**
Экзамен	**36**	**36**
Итого	**180**	**180**

* В форме ПП – в форме практической подготовки.

ИРКУТСК

Рабочая программа дисциплины разработана в соответствии с федеральным государственным образовательным стандартом высшего образования – специалитет по специальности 10.05.03«Информационная безопасность автоматизированных систем», утверждённым приказом Минобрнауки России от 26.11.2020 г. № 1457.

Программу составил:
к.ф.-м.н., доцент _____А.А. Бутин

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «Информационные системы и защита информации», протокол от «04» июня 2021 г. № 11/2

И.о. зав. кафедрой, к.э.н, доцент _____ Т.К. Кириллова

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1 Цели преподавания дисциплины

1	обучение 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 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

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

Освоение дисциплин и практик Б1.О.13 «Информатика;

Б1.О.24 «Аттестация объектов информатизации»;

Б1.О.30 «Безопасность операционных систем»;

Б1.О.31 «Безопасность сетей ЭВМ»;

Б1.О.42 «Открытые информационные системы»;

Б1.О.51 «Кибербезопасность».

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

1	Б1.О.40 «Разработка и эксплуатация автоматизированных систем в защищенном исполнении»;
2	Б1.О.44 «Информационная безопасность открытых систем»;
3	Б1.О.46 «Аудит информационных технологий и систем обеспечения информационной безопасности»;
4	Б1.О.55 «Защита объектов критической информационной инфраструктуры»;
5	Б1.О.57 «Методы принятия организационно-технических решений»;
6	Б1.О.59 «Проектирования систем защиты объектов информатизации»;
7	Б1.О.60 «Защита информации от несанкционированного доступа»;
8	Б2.В.03(П) «Производственная - проектно-технологическая»;
9	Б2.В.04(Н) «Производственная - научно-исследовательская работа»;
10	Б2.В.05 (Пд) «Производственная - преддипломная»

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

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-2. Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности	ОПК-2.1. Применяет современные программные средства системного и прикладного назначений, в том числе отечественного производства, при решении задач профессиональной деятельности ОПК-2.2. Знает основы программных средств системного и прикладного значения, в том числе отечественного производства	**Знать:** – методические основы использования программных средств обеспечения информационной безопасности (ИБ) АС; – условия эксплуатации программных средств обеспечения ИБ АС. **Уметь:** – администрировать программные средства; – проводить проверки работоспособности и устранять нештатные ситуации. **Владеть:** – практическими навыками использования программных средств обеспечения ИБ.
ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ОПК-9.1. Проводит анализ профессиональной деятельности для решения задач защиты информации, сетей и систем передачи данных ОПК-9.2. Знает основные информационные технологии, используемые в автоматизированных системах, их состояние и тенденции развития	**Знать:** – основные тенденции развития современного рынка ПАСЗИ. **Уметь:** – экономически эффективно использовать программно-аппаратные средства обеспечения ИБ в профессиональной деятельности; – проводить выбор ПАСЗИ для использования их в составе АС с целью обеспечения требуемого уровня защищенности. **Владеть:** – практическими навыками использования программно-аппаратных средств обеспечения ИБ АС (на основе программно-технических и программных образцов).
ОПК-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1. Знает средства криптографической и технической защиты информации для решения задач профессиональной деятельности	**Знать:** – методические основы использования криптографических средств обеспечения информационной безопасности (ИБ) АС; – условия эксплуатации криптографических средств обеспечения ИБ АС. **Уметь:** – администрировать криптографические средства защиты информации. – проводить проверки работоспособности и устранять нештатные ситуации. **Владеть:** – практическими навыками использования криптографических средств обеспечения ИБ.
ОПК-11. Способен разрабатывать компоненты систем защиты информации автоматизированных систем	ОПК-11.1. Знает программно-аппаратные средства, используемые в качестве компонентов систем защиты информации в программном обеспечении автоматизированных систем	**Знать:** – принципы функционирования ПАСЗИ; – функциональные возможности представителей основных классов ПАСЗИ; – условия эксплуатации программно-аппаратных средств обеспечения ИБ АС; – способы устранения нештатных ситуаций в процессе функционирования ПАСЗИ. **Уметь:** – администрировать ПАСЗИ; – создавать необходимые условия использования ПАСЗИ для обеспечения ИБ; – проводить проверки работоспособности ПАСЗИ и устранять нештатные ситуации. **Владеть:** – практическими навыками использования программно-аппаратных средств обеспечения ИБ АС (на основе программно-технических

		и программных образцов).

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работы	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Лаб	Пр	СР	
1.0	**Базовые принципы применения и основные классы ПАСЗИ. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, технологические особенности. Аппаратные средства аутентификации; методы и средства хранения ключевой информации**	7	6	8	22	14	ОПК-2.1; ОПК-2.2; ОПК-9.1; ОПК-9.2; ОПК-10.1; ОПК-11.1
1.1	Обоснование необходимости применения добавочных ПАСЗИ. Основные классы добавочных программно-аппаратных средств, обеспечивающих повышенный уровень защиты. Характеристика, основные сервисы и механизмы добавочных ПАСЗИ		4				
1.2	Работа с пакетом «Криптосейф»			2			
1.3	Работа с пакетом «Криптоофис»			2			
1.4	Работа с пакетом «КриптоАРМ»			2			
1.5	Профили защиты средств защиты информации ФСТЭК				8	10	
1.6	ГОСТ Р ИСО/МЭК 15408				4		
1.7	Биометрические методы идентификации и аутентификации. Процедуры биометрического опознания. Устройства биометрической идентификации и аутентификации для автоматизированных систем и виды контроля				2		
1.8	Линейка СЗИ Acronis				2		
1.9	Общие сведения о методах аутентификации. Магнитные и интеллектуальные карты. Устройство хранения ключей типа Touch Memory (iButton). Электронные идентификаторы ruToken. ПСКЗИ ШИПКА		2				
1.10	Электронные идентификаторы eToken				2		
1.11	Использование ключевого носителя ruToken (на базе пакета Rohos)			2			
1.12	Идентификационные карточки с магнитной полосой. Карточки с интегральной микросхемой и металлическими контактами. Карточки с незащищенной памятью				4	4	
2.0	**Методы и средства разграничения доступа к компонентам АС; технологии защиты от несанкционированного доступа (НСД) к информации. Средства антивирусной защиты информации. Технологии анализа защищен-**	7	28	26	12	28	ОПК-2.1; ОПК-2.2; ОПК-9.1; ОПК-9.2; ОПК-10.1; ОПК-11.1

	ности АС. Программно-аппаратные средства защиты информации в сетях передачи данных. Задачи и технологии сертификации ПАСЗИ на соответствие требованиям ИБ						
2.1	Электронный замок (ЭЗ) «Соболь»: назначение, варианты применения, требования к оборудованию и ПО, комплектация. ЭЗ «Соболь»: основные принципы функционирования. ЭЗ «Соболь»: настройка и эксплуатация устройства		2				
2.2	СЗИ от НСД «Dallas Lock» (DL): назначение и состав системы защиты; общие принципы организации защиты ресурсов; механизмы управления доступом и защиты объектов		6			8	
2.3	СЗИ SecretNet: архитектура и компоненты системы; защитные механизмы; назначение и варианты применения системы; управление доступом пользователей к ресурсам; средства централизованного и оперативного управления		6			6	
2.4	Программно-аппаратный комплекс защиты информации от НСД “Аккорд”		4		2		
2.5	DLP-система Info Watch Traffic Monitor Enterprise Edition. СЗИ Device Lock		2		2	2	
2.6	ЭЗ Соболь-PCI. Настройка и эксплуатация. Управление пользователями. Диагностика устройства. Настройка контроля целостности. Регистрация событий			2			
2.7	СЗИ НСД DL: установка средства, настройка параметров входа в систему; реализация дискреционного разграничения доступа			2			
2.8	СЗИ НСД DL: реализация мандатного разграничения доступа; механизм замкнутой программной среды			4			
2.9	СЗИ от НСД SN: дискреционное разграничение доступа, мандатное разграничение доступа, замкнутая программная среда			8			
2.10	СЗИ от НСД SN: настройка контроля целостности			2			
2.11	СЗИ от НСД SN: регистрация событий			4			
2.12	СЗИ от НСД SN: работа с электронным идентификатором; затирание данных			2			
2.13	Угрозы применения вредоносного ПО. Технологии антивирусной защиты информации		2			6	
2.14	Эксплуатация средства антивирусной защиты			2			
2.15	Сканеры безопасности				6		
2.16	Технологии построения частных		4		2	4	

	виртуальных сетей (VPN). Построение VPN на примере систем линеек АПКШ «Континент» и VipNet						
2.17	Понятие сертификации ПАСЗИ. Порядок проведения сертификации		2			2	
3.0	**Экзамен**					36	ОПК-2.1; ОПК-2.2; ОПК-9.1; ОПК-9.2; ОПК-10.1; ОПК-11.1

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

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

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1 Основная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/100% онлайн
6.1.1.1	Казарин О. В. Забабурин А. С.	Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов. 312 с. https://urait.ru/bcode/491249	Юрайт, 2022	100 % онлайн
6.1.1.2	Мифтахова Л. Х., Касимова А. Р., Красильников В. Н. [и др.].	Программно-аппаратные средства защиты информации : учебное пособие . 408 с. https://e.lanbook.com/book/103200	Лань, 2018	100 % онлайн

6.1.2 Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/100% онлайн
6.1.2.1	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
6.1.2.2	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

6.1.3 Методические разработки

	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/100% онлайн

6.1.3.1	Фомин Д. В.	Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : методические указания. 240 с. https://e.lanbook.com/book/156494	Лань, 2017	100 % онлайн
6.1.3.2	Булычев Г. Г.	Программно-аппаратные средства обеспечения информационной безопасности : методические рекомендации . Часть 1. 23 с. https://e.lanbook.com/book/163932	Лань, 2020	100 % онлайн
6.1.3.3	Булычев Г. Г	Программно-аппаратные средства обеспечения информационной безопасности : методические указания. Часть 2. 46 с. https://e.lanbook.com/book/163812	Лань, 2020	100 % онлайн

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»		
6.2.1	Сайт ФСТЭК РФ	http://fstec.ru/
6.2.2	Сайт ФСБ РФ	http://www.fsb.ru/
6.2.3	Сайт производителя ruToken	http://www.rutoken.ru/
6.2.4	Сайт "Код безопасности"	http://www.securitycode.ru
6.2.5	Сайт производителя Dallas Lock	https://www.dallaslock.ru/
6.2.6	Сайт производителя СЗИ "Аккорд"	http://www.accord.ru/
6.2.7	Сайт производителя линейки "ViPNet"	http://www.infotecs.ru/
6.2.8	Материалы «Комплексная защита информации в компьютерных системах»	http://padaread.com/
6.2.9	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;
6.3.1.2	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
6.3.1.3	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 Перечень специализированных средств и программного обеспечения	
6.3.2.1	Сканер MBSA (бесплатное ПО);
6.3.2.2	«Сканер-ВС» (бесплатное ПО для вузов);
6.3.2.3	Персональные идентификаторы ruToken (инвентарный номер 101042001242);
6.3.2.4	VirtualBox (бесплатное ПО);
6.3.2.5	СЗИ Dallas Lock 8.0 ОС Windows (бесплатная лицензия для вузов по Договору с производителем);
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 (лицензия);
6.3.2.8	Электронный замок «Соболь-PCI» (инвентарный номер 101042001241);
6.3.2.9	Средство антивирусной защиты 360 Total Security (бесплатное ПО);
6.3.2.10	Средство антивирусной защиты Dr_Web (demo);
6.3.2.11	Средство защиты Антивирус Касперского (лицензия)
6.3.2.12	Средство криптографической защиты информации «КриптоАРМ» (demo);
6.3.2.13	Учебная программа Rohos (demo);
6.3.2.14	Учебная программа Криптосейф (demo);
6.3.2.15	Учебная программа Криптоофис (demo);
6.3.2.16	MaxPatrol-8 (бесплатная лицензия для вузов);
6.3.2.17	ПО Acronis (лицензия)
6.3.3 Перечень информационных справочных систем	

6.3.3.1	КонсультантПлюс – студенческая версия (Онлайн–версия КонсультантПлюс: Студент, https://student2.consultant.ru/cgi/online.cgi?req=home;rnd=0.8160556428138959)

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.
Самостоятельная работа	Обучение по дисциплине «Безопасность операционных систем» предусматривает активную самостоятельную работу обучающегося. На самостоятельную работу отводится 82 часа по очной форме обучения. В разделе 4 рабочей программы, который называется «Структура и содержание дисциплины», все часы самостоятельной работы расписаны по темам и вопросам, а так же указана необходимая учебная литература: обучающийся изучает учебный материал, разбирает примеры и решает разноуровневые задачи в рамках выполнения домашних заданий. Если этого будет недостаточно для выполнения всей работы можно дополнительно воспользоваться учебными пособиями, приведенными в разделе 6.1 «Учебная литература». Если, несмотря на изученный материал, задание выполнить не удается, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия, и/или консультацию лектора.

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.

Лист регистрации дополнений и изменений рабочей программы дисциплины

№ п/п	Часть текста, подлежавшего изменению в документе			Общее количество страниц		Основание для внесения изменения, № документа	Подпись отв. исп.	Дата
	№ раздела	№ пункта	№ подпункта	до внесения изменений	после внесения изменений			

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.39 Программно-аппаратные средства защиты информации

Приложение 1 к рабочей программе

Специальность – 10.05.03 Информационная безопасность автоматизированных систем;
Специализация – № 5 "Безопасность открытых информационных систем"

ИРКУТСК

Общие положения

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

Фонды оценочных средств предназначены для использования обучающимися, преподавателями, администрацией Университета, а так же сторонними образовательными организациями для оценивания качества освоения образовательной программы и уровня сформированности компетенций у обучающихся.

В соответствии с требованиями действующего законодательства в сфере образования, оценочные средства представляются в виде ФОС для проведения промежуточной аттестации обучающихся по дисциплине (модулю), практике. С учетом действующего в Университете Положения о формах, периодичности и порядке текущего контроля успеваемости и промежуточной аттестации обучающихся (высшее образование – бакалавриат, специалитет, магистратура), в состав ФОС для проведения промежуточной аттестации по дисциплине (модулю), практике включаются оценочные средства для проведения текущего контроля успеваемости обучающихся.

Задачами ФОС являются:

– оценка достижений обучающихся в процессе изучения дисциплины (модуля) или прохождения практики;

– 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 ОПОП; 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 с указанием этапов их формирования. Показатели оценивания компетенций, критерии оценки

Дисциплина «Программно-аппаратные средства защиты информации» участвует в формировании компетенции:

ОПК-2. Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.

ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации.

ОПК-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности.

ОПК-11. Способен разрабатывать компоненты систем защиты информации автоматизированных систем.

Программа контрольно-оценочных мероприятий

№	Неделя	Наименование контрольно-оценочного мероприятия	Объект контроля (понятие/тем/раздел и т.д. дисциплины)	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
9 семестр					
1	1-17	Текущий контроль	Лабораторные работы (см. п.4 РПД, разделы 1,2)	ОПК-2.1,ОПК - 2.2; ОПК-9.1, ОПК-9.2; ОПК-10.1; ОПК-11.1	Защита лабораторной работы (устно)
2	1-17	Текущий контроль	Индивидуальное выступление с докладом на семинарском занятии по теме в соответствии с п.4 РПД , разделы 1,2	ОПК-2.1,ОПК - 2.2; ОПК-9.1, ОПК-9.2; ОПК-10.1; ОПК-11.1	Сообщение, доклад (устно); наличие презентации;
3	17	Тест	Разделы 1,2 РПД	ОПК-2.1,ОПК - 2.2; ОПК-9.1, ОПК-9.2; ОПК-10.1; ОПК-11.1	Фонд тестовых заданий (письменно)
4		Промежуточная аттестация – экзамен	Разделы 1,2 РПД	ОПК-2.1,ОПК - 2.2; ОПК-9.1, ОПК-9.2; ОПК-10.1; ОПК-11.1	Экзамен (устно)

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

Описание показателей и критериев оценивания компетенций на различных этапах их формирования. 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 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	Сообщение, доклад	Продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полу-	Темы докладов, сообщений

		ченных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	
2	Тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Может быть использован для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий
3	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
4	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 билетов к экзамену

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

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

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

Оценочное средство «Тест»

Тестирование с применением компьютерных технологий проводится по окончании 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 итогового теста по дисциплине и типовые примеры тестов приведены в разделе 3 данного документа.

Результаты тестирования могут быть использованы при проведении промежуточной аттестации в форме экзамена.

Промежуточная аттестация в форме экзамена – результаты тестирования могут являться допуском к экзамену:

Критерии оценивания	Шкала оценивания
Обучающийся набрал при тестировании более 69 баллов	Обучающийся к экзамену допущен
Обучающийся набрал при тестирован менее 69 баллов	Обучающийся к экзамену не допущен

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, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

3.1. Темы докладов, сообщений

См. п. 4 РПД

3.2 Перечень теоретических вопросов к экзамену

Раздел 1

1.1. Обоснование необходимости применения добавочных ПАСЗИ.

1.2.Основные классы добавочных программно-аппаратных средств, обеспечивающих повышенный уровень защиты.

1.3.Характеристика, основные сервисы и механизмы добавочных ПАСЗИ;

1.4. Общие сведения о методах аутентификации. Магнитные и интеллектуальные карты.

1.5. Устройство хранения ключей типа Touch Memory (iButton). Электронные идентификаторы ruToken.

1.6. ПСКЗИ ШИПКА;

Раздел 2

2.1. Электронный замок (ЭЗ) «Соболь»: назначение, варианты применения, требования к оборудованию и ПО, комплектация.

2.2. ЭЗ «Соболь»: основные принципы функционирования.

2.3.ЭЗ «Соболь»: настройка и эксплуатация устройства;

2.4. ЭЗ «Соболь»: администрирование;

2.5. СЗИ от НСД «Dallas Lock» (DL): назначение и состав системы защиты;

2.6. СЗИ от НСД «Dallas Lock» (DL): общие принципы организации защиты ресурсов;

2.7. СЗИ от НСД «Dallas Lock» (DL): механизмы управления доступом и защиты объектов;

2.8. СЗИ SecretNet: архитектура и компоненты системы;

2.9. СЗИ SecretNet: защитные механизмы; назначение и варианты применения системы;
2.10. СЗИ SecretNet: управление доступом пользователей к ресурсам;
2.11. СЗИ SecretNet: средства централизованного и оперативного управления;
2.12. СЗИ от НСД Страж NT
2.13. Программно-аппаратный комплекс защиты информации от НСД “Аккорд”;
2.14. DLP-система Info Watch Traffic Monitor Enterprise Edition;
2.15.СЗИ Device Lock;
2.16. Технологии антивирусной защиты информации.
2.17. Цели и задачи проведения мероприятий по оценке уровня защищенности АС.
2.18. Построение VPN на примере систем линейки АПКШ «Континент».
2.19. Порядок проведения сертификации программно-аппаратных средств обеспечения ИБ

3.3 Тестирование по дисциплине

3.3.1 Структура фонда тестовых заданий по дисциплине

Структура фонда тестовых заданий по дисциплине Программно-аппаратные средства защиты информации

Раздел дисциплины	Тема раздела	Количество тестовых заданий (ТЗ), типы ТЗ
1. Базовые принципы применения и основные классы ПАСЗИ. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, технологические особенности. Аппаратные средства аутентификации; методы и средства хранения ключевой информации	Обоснование необходимости применения добавочных ПАСЗИ. Основные классы добавочных программно-аппаратных средств, обеспечивающих повышенный уровень защиты. Характеристика, основные сервисы и механизмы добавочных ПАСЗИ. Общие сведения о методах аутентификации. Магнитные и интеллектуальные карты. Устройство хранения ключей типа Touch Memory (iButton). Электронные идентификаторы ruToken. ПСКЗИ ШИПКА.	23 – тип A 1 – тип B 1 – тип D
Итого по разделу		**∑ 25** **23– тип A** **1- тип B** **1- тип D**

2. Методы и средства разграничения доступа к компонентам АС; технологии защиты от несанкционированного доступа (НСД) к информации. Средства антивирусной защиты информации. Технологии анализа защищенности АС. Программно-аппаратные средства защиты информации в сетях передачи данных. Задачи и технологии сертификации ПАСЗИ на соответствие требованиям ИБ	Электронный замок (ЭЗ) «Соболь»: назначение, варианты применения, требования к оборудованию и ПО, комплектация. ЭЗ «Соболь»: основные принципы функционирования. ЭЗ «Соболь»: настройка и эксплуатация устройства. СЗИ от НСД «Dallas Lock» (DL): назначение и состав системы защиты; общие принципы организации защиты ресурсов; механизмы управления доступом и защиты объектов. СЗИ SecretNet: архитектура и компоненты системы; защитные механизмы; назначение и варианты применения системы; управление доступом пользователей к ресурсам; средства централизованного и оперативного управления. Программно-аппаратный комплекс защиты информации от НСД “Аккорд”. DLP-система Info Watch Traffic Monitor Enterprise Edition. СЗИ Device Lock. Угрозы применения вредоносного ПО. Технологии антивирусной защиты информации. Технологии построения частных виртуальных сетей (VPN). Построение VPN на примере систем линеек АПКШ «Континент» и VipNet.. Понятие сертификации ПАСЗИ. Порядок проведения сертификации	47 – тип А
Итого по разделу		**∑ 47** **47 – тип А**
Итого по дисциплине		**∑ 72** **70 – тип А** **1 – тип В** **1 – тип D**

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 D: тестовое задание на установление правильной последовательности.

3.3.2 Структура и образец итогового теста по дисциплине за весь период ее освоения

Структура типового итогового теста по дисциплине за весь период ее освоения

Раздел дисциплины	Тема раздела	Количество тестовых заданий (ТЗ), типы ТЗ

1. Базовые принципы применения и основные классы ПАСЗИ. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, технологические особенности. Аппаратные средства аутентификации; методы и средства хранения ключевой информации	Обоснование необходимости применения добавочных ПАСЗИ. Основные классы добавочных программно-аппаратных средств, обеспечивающих повышенный уровень защиты. Характеристика, основные сервисы и механизмы добавочных ПАСЗИ. Общие сведения о методах аутентификации. Магнитные и интеллектуальные карты. Устройство хранения ключей типа Touch Memory (iButton). Электронные идентификаторы ruToken. ПСКЗИ ШИПКА.	6 – тип А 1 – тип В 1 – тип D
Итого по разделу		**∑ 8** **6– тип А** **1- тип В** **1- тип D**
2. Методы и средства разграничения доступа к компонентам АС; технологии защиты от несанкционированного доступа (НСД) к информации. Средства антивирусной защиты информации. Технологии анализа защищенности АС. Программно-аппаратные средства защиты информации в сетях передачи данных. Задачи и технологии сертификации ПАСЗИ на соответствие требованиям ИБ	Электронный замок (ЭЗ) «Соболь»: назначение, варианты применения, требования к оборудованию и ПО, комплектация. ЭЗ «Соболь»: основные принципы функционирования. ЭЗ «Соболь»: настройка и эксплуатация устройства. СЗИ от НСД «Dallas Lock» (DL): назначение и состав системы защиты; общие принципы организации защиты ресурсов; механизмы управления доступом и защиты объектов. СЗИ SecretNet: архитектура и компоненты системы; защитные механизмы; назначение и варианты применения системы; управление доступом пользователей к ресурсам; средства централизованного и оперативного управления. Программно-аппаратный комплекс защиты информации от НСД “Аккорд”. DLP-система Info Watch Traffic Monitor Enterprise Edition. СЗИ Device Lock. Угрозы применения вредоносного ПО. Технологии антивирусной защиты информации. Технологии построения частных виртуальных сетей (VPN). Построение VPN на примере систем линеек АПКШ «Континент» и VipNet.. Понятие сертификации ПАСЗИ. Порядок проведения сертификации	17 – тип А
Итого по разделу		**∑ 17** **17 – тип А**
Итого по дисциплине		**∑ 25** **23 – тип А** **1 – тип В** **1 – тип D**

Образец типового теста за 9 семестр по дисциплине

3.3.4 Фонд тестовых заданий

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 АС;
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 равно _____ .
21. В СЗИ Secret Net категорию конфиденциальности можно назначить для следующих ресурсов: каталоги и файлы на дисках с файловой системой _____.
22. Эффективным средством защиты от утечки информации из АИС показали себя _____ – системы.
23. АПКШ «Континент» является средством построения частных _____ сетей.
24. Сканер-ВС, сканеры MaxPatrol и "Ревизор сети" представляют собой средства контроля _____ компьютерной сети.
25. Dr. Web является сертифицированным средством защиты от _____ программного обеспечения.
26. Info Watch Traffic Monitor Enterprise Edition – это система защиты от _____ инсайдерской информации.
27. АМДЗ «Аккорд» является средством _____ загрузки штатной операционной системы.
28. Как в СЗИ Secret Net происходит включение режима хранения пароля в идентифика- торе?
29. СЗИ SecretNet: опишите функции сервера безопасности (СБ).
30. СЗИ SecretNet: опишите функции агента СБ.

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 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 экзамена и оценивания результатов обучения

Промежуточная аттестация в форме экзамена проводится путем устного собеседования по билетам.

Билет содержит: два теоретических вопроса для оценки знаний. Теоретические вопросы выбираются из перечня вопросов к экзамену.

Распределение теоретических вопросов и практических заданий по экзаменационным билетам находится в закрытом для обучающихся доступе. Разработанный комплект 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 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 2021-2022 учебный год	**Экзаменационный билет № 1** **по дисциплине «__ПАСЗИ__»** **__** **__9__ семестр**	Утверждаю: Заведующий кафедрой ИСиЗИ ИрГУПС _____
1. Общие сведения о методах аутентификации. Магнитные и интеллектуальные карты; 2. ЭЗ «Соболь»: основные принципы функционирования. Билет формата А5 – 148*210мм		