ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Иркутский государственный университет путей сообщения»
(ФГБОУ ВО ИрГУПС)
Забайкальский институт железнодорожного транспорта –
филиал Федерального государственного бюджетного образовательного учреждения высшего образования «Иркутский государственный университет путей сообщения»
(ЗабИЖТ ИрГУПС)

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

Б1.О.51 Основы информационной безопасности

рабочая программа дисциплины

Специальность – 38.05.02 Таможенное дело
Профиль – Таможенное дело
Квалификация выпускника – специалист таможенного дела
Форма и срок обучения – очная форма, 5 лет обучения; заочная форма, 6 лет обучения
Кафедра-разработчик программы – Техносферная безопасность

Общая трудоемкость в з.е. – 2
Часов по учебному плану (УП) – 72

Формы промежуточной аттестации в семестрах, курсах
очная форма обучения: зачет 4 семестр
заочная форма обучения: зачет 3 курс

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

Семестр	4	**Итого**
Число недель в семестре	17	
Вид занятий	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий	**34**	**34**
– лекции	17	17
– практические	17	17
– лабораторные		
Самостоятельная работа	**38**	**38**
Зачет		
Итого	**72**	**72**

Заочная форма обучения **Распределение часов дисциплины по курсам**

Курс	3	**Итого**
Вид занятий	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий	**8**	**8**
– лекции	4	4
– практические		
– лабораторные	4	4
Зачет	**60**	**60**
Экзамен	**4**	**4**
Итого	**72**	**72**

ЧИТА

Рабочая программа дисциплины разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования – специалитет по специальности 38.05.02 Таможенное дело, утверждённым приказом Министерства науки и высшего образования РФ от 25.11.2020 г. № 1453.

Программу составил:

к.п.н., доцент, зав. кафедрой Л.В. Виноградова

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «Техносферная безопасность», протокол от «23» апреля 2024 г. № 7.

Зав. кафедрой, к.п.н., доцент Л.В. Виноградова

СОГЛАСОВАНО

Кафедра «Управление процессами перевозок», протокол от «24» апреля 2024 г. № 10.

Зав. кафедрой, к.т.н., доцент М.И. Коновалова

1 ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ	
1.1 Цели преподавания дисциплины	
1	формирование знаний и представлений о смысле, целях и задачах информационной защиты, характерных свойствах защищаемой информации, основных информационных угрозах, существующих (действующих) направлениях защиты и возможностях построения моделей, стратегий, методов и правил информационной защиты
1.2 Задачи дисциплины	
1	изучение основных методов и принципов обеспечения конфиденциальности, целостности и доступности информации в информационных системах
2	изучение типовых угроз безопасности информации при её обработке в информационных системах
3	изучение основных принципов обеспечения информационной безопасности
4	изучение основ построения модели угроз и политики безопасности
5	изучение основных моделей доступа
6	изучение основы информационной безопасности в системе национальной безопасности РФ
1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины	
Профессионально-трудовое воспитание обучающихся	
Цель профессионально-трудового воспитания – формирование у обучающихся осознанной профессиональной ориентации, понимания общественного смысла труда и значимости его для себя лично, ответственного, сознательного и творческого отношения к будущей деятельности, профессиональной этики, способности предвидеть изменения, которые могут возникнуть в профессиональной деятельности, и умению работать в изменённых, вновь созданных условиях труда. Цель достигается по мере решения в единстве следующих задач: – формирование сознательного отношения к выбранной профессии; – воспитание чести, гордости, любви к профессии, сознательного отношения к профессиональному долгу, понимаемому как личная ответственность и обязанность; – формирование психологии профессионала; – формирование профессиональной культуры, этики профессионального общения; – формирование социальной компетентности и другие задачи, связанные с имиджем профессии и авторитетом транспортной отрасли	

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
Блок/часть ОПОП	Блок 1.Дисциплины / Обязательная часть
2.1 Требования к предварительной подготовке обучающегося	
1	Б1.О.22 Математика в экономике
2	ФТД.02 Основы научных исследований
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б1.О.32 Таможенная статистика
2	Б2.О.04(Н) Производственная - научно-исследовательская работа
3	Б2.О.05(Пд) Производственная - преддипломная практика
4	Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы
5	Б3.02(Д) Защита выпускной квалификационной работы

3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ТРЕБОВАНИЯМИ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ		
Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения**
ОПК-2 Способен осуществлять сбор, обработку, анализ данных для решения профессиональных задач, информирования органов государственной власти и общества на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-2.6. Умеет работать с файлами и документами, содержащими персональные данные и информацию ограниченного доступа	**Знать:** основные понятия в области информационной безопасности; виды и источники опасностей и угроз в сфере информационных процессов и систем; нормативно-правовые акты по обработке персональных данных и информации ограниченного доступа
		Уметь: работать с файлами и документами, содержащими персональные данные и информацию ограниченного доступа
		Владеть: навыками работы с файлами и документами, содержащими персональные

		данные и информацию ограниченного доступа

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работы	Очная форма					Заочная форма					*Код индикатора достижения компетенции
		Семестр	Часы				Курс/ сессия	Часы				
			Лек	Пр	Лаб	СР		Лек	Пр	Лаб	СР	
1.0	**Раздел 1. Теоретические основы информационной безопасности**	**4**	**4**	**4**		**8**	**3/ зимняя**	**2**	**2**		**8**	**ОПК-2.6**
1.1	Тема 1. Значение информационной безопасности и ее место в системе национальной безопасности, современная Доктрина информационной безопасности РФ	4	2	2		4	3/ зимняя	2	2		4	ОПК-2.6
1.2	Тема 2. Теоретические и концептуальные основы защиты информации. Современные факторы, влияющие на защиту информации	4	2	2		4	3/ зимняя				4	ОПК-2.6
2	**Раздел 2. Информация: виды, методы и средства обеспечения безопасности**	**4**	**10**	**10**		**22**	**3/ зимняя**	**2**	**2**		**24**	**ОПК-2.6**
2.1	Тема 3. Критерии, условия и принципы отнесения информации к защищаемой. Носители защищаемой информации: состав, классификация	4	2	2		4	3/ зимняя				4	ОПК-2.6
2.2	Тема 4. Классификации информации по видам тайн и степеням конфиденциальности, по собственникам и владельцам	4	2	2		4	3/ зимняя				8	ОПК-2.6
2.3	Тема 5. Понятие и структура угроз защищаемой информации. Источники, виды, условия и способы дестабилизирующего воздействия на защищаемую информацию	4	2	2		5	3/ зимняя				6	ОПК-2.6
2.4	Тема 6. Каналы и методы несанкционированного доступа к конфиденциальной информации. Направления, виды и особенности деятельности разведывательных служб по несанкционированному доступу к конфиденциальной информации.	4	2	2		5	3/ зимняя	2	2		6	ОПК-2.6
2.5	Объекты защиты информации. Вирусное заражение информации. Классификация антивирусных программ	4	2	2		4	3/ зимняя				4	ОПК-2.6
3	**Раздел 3. Организационно-правовое обеспечение информационной безопасности**	**4**	**3**	**3**		**8**	**3/ зимняя**				**10**	**ОПК-2.6**
3.1	Тема 7. Кадровое, ресурсное и технологическое обеспечение защиты информации	4	2	2		5	3/ зимняя				4	ОПК-2.6
3.2	Тема 8. Назначение и структура систем защиты информации	4	1	1		3	3/ зимняя				6	ОПК-2.6
4	Выполнение контрольной работы						3/ зимняя				18	ОПК-2.6
5	**Форма промежуточной аттестации - зачет**	**4**	**-**				**3/ зимняя**	**4**				**ОПК-2.6**

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

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

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

6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ		
6.1 Учебная литература		
6.1.1 Основная литература		
	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.1.1	Афонин, П. Н. Информационная безопасность в таможенном деле: учебник / П. Н. Афонин, Д. Н. Афонин, А. И. Краснова. – Санкт-Петербург: Троицкий мост, 2016. – 512 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=445283 . – Библиогр. в кн. – ISBN 978-5-4377-0039-6. – Текст: электронный (дата обращения: 23.04.2024)	онлайн
6.1.1.2	Швечкова, О. Г. Информационная безопасность: учебник / О. Г. Швечкова, С. И. Бабаев. – Москва: Курс, 2023. – Часть 1. Теоретические основы. – 145 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=708265 – Библиогр. в кн. – ISBN 978-5-907352-37-7. – Текст: электронный (дата обращения: 23.04.2024)	онлайн
6.1.1.3	Швечкова, О. Г. Информационная безопасность: учебник / О. Г. Швечкова, С. И. Бабаев. – Москва: Курс, 2023. – Часть 2. Стандарты и документы. – 145 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=708266 – Библиогр. в кн. – ISBN 978-5-907352-68-1. – Текст: электронный (дата обращения: 23.04.2024)	онлайн
6.1.2 Дополнительная литература		
	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.2.1	Аверченков, В. И. Защита персональных данных в организации / В. И. Аверченков, М. Ю. Рытов, Т. Р. Гайнулин. – 4-е изд., стер. – Москва: ФЛИНТА, 2021. – 124 с: табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=93260 – Библиогр.: с. 107-109. – ISBN 978-5-9765-1273-3. – Текст: электронный. (дата обращения: 23.04.2024)	онлайн
6.1.2.2	Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика: учебное пособие: [16+] / В. Я. Ищейнов. – Москва; Берлин: Директ-Медиа, 2020. – 271 с.: схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=571485 (– Библиогр. в кн. – ISBN 978-5-4499-0496-6. – DOI 10.23681/571485. – Текст: электронный (дата обращения: 23.04.2024)	онлайн
6.1.2.3	Порядина, О. В. Управление информационными ресурсами: учебно-методическое пособие: [16+] / О. В. Порядина; Поволжский государственный технологический университет. – Йошкар-Ола: Поволжский государственный технологический университет, 2015. – 52 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=439328 – Библиогр. в кн. – ISBN 978-5-8158-1536-0. – Текст: электронный (дата обращения: 23.04.2024)	онлайн
6.1.2.4	Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях : практическое пособие: [16+] / В. Ф. Шаньгин. – 2-е изд. – Москва : ДМК Пресс, 2023. – 594 с.: ил., табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=703712 – Библиогр.: с. 576-580. – ISBN 978-5-89818-506-0. – Текст: электронный (дата обращения: 23.04.2024)	онлайн
6.1.3 Учебно-методические разработки (в т. ч. для самостоятельной работы обучающихся)		
	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн/ЭИОС

6.1.3.1	Виноградова Л.В. Основы информационной безопасности: практикум: Учебно-методическое пособие на практические занятия для студентов специальности 3805.02 «Таможенное дело» - Чита: ЗабИЖТ, 2016. – 78 с. [Электронный ресурс]: http://zabizht.ru/cgi-bin/viewer.pl?book_id=32350.pdf (дата обращения: 23.04.2024)	онлайн/ ЭИОС
6.1.3.2	Виноградова Л.В. Основы информационной безопасности: Учебно-методическое пособие для выполнения контрольной и самостоятельной работы для студентов специальности 3805.02 «Таможенное дело» - Чита: ЗабИЖТ, 2016. – 54 с. [Электронный ресурс]: http://zabizht.ru/cgi-bin/viewer.pl?book_id=32349.pdf (дата обращения: 23.04.2024)	онлайн/ ЭИОС
6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»		
6.2.1	АСУ Библиотека ЗабИЖТ http://zabizht.ru	
6.2.2	ЭБС «Университетская библиотека Online» http://biblioclub.ru/	
6.3 Программное обеспечение и информационные справочные системы		
6.3.1 Базовое программное обеспечение		
6.3.1.1	Microsoft Windows 7 Professional, лицензия № 49156201, государственный контракт от 03.10.2011 г. № 139/53-ОАЭ-11	
6.3.1.2	Microsoft Office 2007 Standard, лицензия № 45777622, государственный контракт от 10.08.2009 г. №64/17-ОА-09; Microsoft Office 2007 Standard, лицензия № 44718393, государственный контракт от 18.10.2008 г. № 92/32А-08	
6.3.1.3	Яндекс. Браузер. Прикладное программное обеспечение общего назначения, Офисные приложения, лицензия – свободно распространяемое программное обеспечение по лицензии BSD License	
6.3.1.4	АСУ «Библиотека», свидетельство о государственной регистрации программы для ЭВМ № 2009611107, зарегистрировано в Реестре программ для ЭВМ 19.02.2009	
6.3.1.5	БД АСУ «Библиотека», свидетельство о государственной регистрации программы для ЭВМ № 2009620102, зарегистрировано в Реестре программ для ЭВМ 27.02.2009	
6.3.2 Специализированное программное обеспечение		
6.3.2.1	Не предусмотрено	
6.3.3 Информационные справочные системы		
6.3.3.1	Информационно-справочная система «Гарант»	
6.4 Правовые и нормативные документы		
6.3.4.1	Конституция Российской Федерации	
6.3.4.2	Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»	
6.3.4.3	Указ Президента РФ от17.03.2008 № 351 (ред. от 22.05.2015) «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»	
6.3.4.4	Указ Президента Российской Федерации от 02.07.2021 № 400 «О стратегии национальной безопасности Российской Федерации»	
6.3.4.5	Федеральный закон от 30.12.2001 № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях»	
6.3.4.6	Федеральный закон от 13.06.1996 № 63-ФЗ «Уголовный кодекс Российской Федерации»	
6.3.4.7	Федеральный закон от 18.12.2006 № 230-ФЗ «Гражданский кодекс Российской Федерации (часть четвертая)»	
6.3.4.8	Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	
6.3.4.9	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»	
6.3.4.10	Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»	
6.3.4.11	Закон РФ «О государственной тайне» от 21.07.1993 № 5485-1	
6.3.4.12	Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности»	
6.3.4.13	Закон РФ от 05.03.1992 № 2446-1 «О безопасности»	

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

1	Учебный и лабораторный корпуса ЗабИЖТ ИрГУПС находятся по адресу: 672040, Забайкальский край, город Чита, улица Магистральная, дом 11

2	Учебная аудитория 418 для проведения лекционных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованная специализированной мебелью и техническими средствами обучения (ноутбук (переносной), мультимедиапроектор, экран), служащими для представления учебной информации большой аудитории. Для проведения занятий имеются учебно-наглядные пособия (презентации), обеспечивающие тематические иллюстрации содержания дисциплины
3	Учебная аудитория 403 для проведения лекционных и практических занятий, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации, укомплектованная специализированной мебелью и техническими средствами обучения (ноутбук (переносной), мультимедиапроектор, экран), служащими для представления учебной информации большой аудитории. Для проведения занятий имеются учебно-наглядные пособия (презентации), обеспечивающие тематические иллюстрации содержания дисциплины
4	Помещения для самостоятельной работы обучающихся оснащены специализированной мебелью и компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ЗабИЖТ. Помещения для самостоятельной работы обучающихся: – читальный зал; – 3.24, 4.15
5	Помещение 3.25 для хранения и профилактического обслуживания учебного оборудования. Оснащенность: компьютеры, ручной слесарный инструмент, электротехнический инструмент, принадлежности для пайки, мебель, учебно-наглядные пособия

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	На лекциях обучающиеся получают самые необходимые данные, во многом дополняющие и корректирующие учебники. Умение сосредоточенно слушать лекции, активно, творчески воспринимать излагаемые сведения является непременным условием их глубокого и прочного усвоения, а также развития умственных способностей. Слушание и запись лекций – сложные виды работы. Внимательное слушание и конспектирование лекций предполагает интенсивную умственную деятельность обучающегося. Слушая лекции, надо отвлечься при этом от посторонних мыслей и думать только о том, что излагает преподаватель. Краткие записи лекций, конспектирование их помогает усвоить материал. Внимание человека неустойчиво. Требуются волевые усилия, чтобы оно было сосредоточенным. Конспект является полезным тогда, когда записано самое существенное, основное. Это должно быть сделано самим обучающимся. Не надо стремиться записать дословно всю лекцию. Такое "конспектирование" приносит больше вреда, чем пользы. Некоторые обучающиеся просят иногда лектора "читать помедленнее". Но лекция не может превратиться в лекцию-диктовку. Это очень вредная тенденция, ибо в этом случае обучающийся механически записывает большое количество услышанных сведений, не размышляя над ними. Запись лекций рекомендуется вести по возможности собственными формулировками. Желательно запись осуществлять на одной странице, а следующую оставлять для проработки учебного материала самостоятельно в домашних условиях. Конспект лучше подразделять на пункты, параграфы, соблюдая красную строку. Принципиальные места, определения, формулы следует сопровождать замечаниями: «важно», «особо важно» и т.п. Целесообразно разработать собственную «маркографию» (значки, символы), сокращения слов. Работая над конспектом лекций, нужно использовать не только учебник, но и рекомендованную дополнительную литературу. Именно такая серьезная, кропотливая работа с лекционным материалом позволит глубоко овладеть знаниями. Функция обучающегося – не только переработать информацию, но и активно включиться в открытие неизвестного для себя знания. Общие и утвердившиеся в практике правила, и приемы конспектирования лекций: Конспектирование лекций ведется в специально отведенной для этого тетради, каждый лист, которой должен иметь поля, на которых делаются пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. Необходимо записывать тему и план лекций, рекомендуемую литературу к теме. Записи разделов лекции должны иметь заголовки, подзаголовки, красные строки. Для выделения разделов, выводов, определений, основных идей можно использовать цветные

	карандаши и фломастеры. Названные в лекции ссылки на первоисточники надо пометить на полях, чтобы при самостоятельной работе найти и вписать их. В конспекте дословно записываются определения понятий, категорий и законов. Остальное должно быть записано своими словами. Каждому обучающемуся необходимо выработать и использовать допустимые сокращения наиболее распространенных терминов и понятий. В конспект следует заносить всё, что преподаватель пишет на доске, а также рекомендуемые схемы, таблицы, диаграммы и т.д. 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 лабораторном занятии
Практическое занятие	Практическое занятие – вид аудиторных учебных занятий, целенаправленная форма организации учебного процесса, при реализации которой обучающиеся по заданию и под руководством преподавателя выполняют практические задания. Практические задания направлены на углубление научно-теоретических знаний и овладение определенными методами работы, в процессе которых вырабатываются умения и навыки выполнения тех или иных учебных действий в данной сфере науки. Практические занятия развивают научное мышление и речь, позволяют проверить знания обучающихся, выступают как средства оперативной обратной связи; цель практических занятий – углублять, расширять, детализировать знания, полученные на лекции, в обобщенной форме и содействовать выработке навыков профессиональной деятельности. На практических занятиях подробно рассматриваются основные вопросы дисциплины, разбираются основные типы задач. К каждому практическому занятию следует заранее самостоятельно выполнить домашнее задание и выучить лекционный материал к следующей теме. Систематическое выполнение домашних заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины.
Самостоятельная работа	Обучение по дисциплине предусматривает активную самостоятельную работу обучающегося. В разделе 4 рабочей программы, который называется «Структура и содержание дисциплины», все часы самостоятельной работы расписаны по темам и вопросам. Обучающийся изучает учебный материал и если, несмотря на изученный материал, задания выполнить не удается, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия и/или консультацию лектора. Самостоятельная работа обучающегося является основным средством овладения учебным материалом во время, свободное от обязательных учебных занятий. Самостоятельная работа обучающегося над усвоением учебного материала может выполняться в библиотеке, аудиториях для самостоятельной работы, а также в домашних условиях. Учебный материал дисциплины, предусмотренный учебным планом, для усвоения обучающимся в процессе самостоятельной работы, выносится на промежуточную аттестацию наряду с учебным материалом, который разрабатывался при проведении учебных занятий. Содержание самостоятельной работы обучающегося определяется учебной программой дисциплины, методическими материалами, заданиями и указаниями преподавателя. Самостоятельная работа обучающихся осуществляется в аудиторной и внеаудиторной формах
Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины, размещен в электронной информационно-образовательной среде ЗабИЖТ ИрГУПС, доступной обучающемуся через его личный кабинет	

Приложение № 1 к рабочей программе

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации

1 Общие положения

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

Фонды оценочных средств предназначены для использования обучающимися, преподавателями, администрацией Института, а также 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. С учетом действующего в Институте 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 включаются оценочные средства для проведения текущего контроля успеваемости обучающихся.

Задачами ФОС являются:

– оценка достижений обучающихся в процессе изучения дисциплины;

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

– самоподготовка и самоконтроль обучающихся в процессе обучения.

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

Для оценки уровня сформированности компетенций используется трехуровневая система:

– минимальный уровень освоения, обязательный для всех обучающихся по завершению освоения 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 «Основы информационной безопасности» участвует в формировании компетенции:

ОПК-2 Способен осуществлять сбор, обработку, анализ данных для решения профессиональных задач, информирования органов государственной власти и общества на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Программа контрольно-оценочных мероприятий очная форма обучения

№	Наименование контрольно-оценочного мероприятия	Объект контроля (раздел/тема дисциплины)	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
4 семестр				
1	Текущий контроль	Раздел 1. Теоретические основы информационной безопасности. Раздел 2. Информация: виды, методы и средства обеспечения безопасности. Раздел 3. Организационно-правовое обеспечение информационной безопасности	ОПК-2.6	Конспект (письменно), доклад (устно), разноуровневые задания (письменно, устно), тестирование (компьютерные технологии)
2	Промежуточная аттестация	Раздел 1. Теоретические основы информационной безопасности. Раздел 2. Информация: виды, методы и средства обеспечения безопасности. Раздел 3. Организационно-правовое обеспечение информационной безопасности	ОПК-2.6	Зачет (собеседование), зачет – тестирование (компьютерные технологии)

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

Программа контрольно-оценочных мероприятий заочная форма обучения

№	Наименование контрольно-оценочного мероприятия	Объект контроля (раздел/тема дисциплины)	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
Курс 3, сессия зимняя				
1	Текущий контроль	Раздел 1. Теоретические основы информационной безопасности. Раздел 2. Информация: виды, методы и средства обеспечения безопасности. Раздел 3. Организационно-правовое обеспечение информационной безопасности	ОПК-2.6	Конспект (письменно), доклад (устно), разноуровневые задания (письменно, устно), контрольная работа (письменно), тестирование (компьютерные технологии)
2	Промежуточная аттестация	Раздел 1. Теоретические основы информационной безопасности. Раздел 2. Информация: виды, методы и средства обеспечения безопасности. Раздел 3. Организационно-правовое обеспечение информационной безопасности	ОПК-2.6	Зачет (собеседование), зачет – тестирование (компьютерные технологии)

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

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

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

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

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Конспект	Особый вид текста, в основе которого лежит аналитико-синтетическая переработка информации первоисточника (исходного текста). Цель этой деятельности — выявление, систематизация и обобщение (с возможной критической оценкой) наиболее ценной (для конспектирующего) информации. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Темы конспектов
2	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
3	Тестирование (компьютерные технологии)	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	Контрольная работа	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу. Может быть использовано для оценки знаний и умений обучающихся	Типовое задание для выполнения контрольной работы
5	Разноуровневые задания	Различают задания: – репродуктивного уровня, позволяющие оценивать и диагностировать знание фактического материала (базовые понятия, алгоритмы, факты) и умение правильно использовать специальные термины и понятия, узнавание объектов изучения в рамках определенного раздела дисциплины; может быть использовано для оценки знаний и умений обучающихся; – реконструктивного уровня, позволяющие оценивать и диагностировать умения синтезировать, анализировать, обобщать фактический и теоретический материал с	Типовые разноуровневые задания

		формулированием конкретных выводов, установлением причинно-следственных связей; может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся; – творческого уровня, позволяющие оценивать и диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения; может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	
6	Тест – промежуточная аттестация в форме зачета	Система автоматизированного контроля освоения компетенций (части компетенций) обучающимся по дисциплине с использованием информационно-коммуникационных технологий. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий
7	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

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

Шкалы оценивания	Критерии оценивания	Уровень освоения 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 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
«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

Тестирование – промежуточная аттестация в форме зачета:

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

«не зачтено»	Обучающийся верно ответил на 69 % и менее тестовых заданий при прохождении тестирования

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Конспект

Шкала оценивания	Критерии оценивания
«зачтено»	Конспект полный. В конспектируемом материале даны основные понятия и определения, полностью раскрыты поставленные вопросы. В конспекте обучающегося отражены основные концепции и теории по данному вопросу, проведен их критический анализ и сопоставление, описанные теоретические положения иллюстрируются практическими примерами и экспериментальными данными, обучающимся формулируется собственная точка зрения на конспектируемый материал. Обучающийся использовал несколько источников литературы
	Конспект полный. В конспекте обучающегося описываются и сравниваются основные вопросы, описанные теоретические положения иллюстрируются практическими примерами, обучающимся формулируется собственная точка зрения на заявленные проблемы, однако он испытывает затруднения в ее аргументации. Обучающийся использовал несколько источников литературы
	Конспект не полный. В конспекте обучающегося отражены лишь некоторые вопросы, их анализ и сопоставление не проводится. Обучающийся испытывает значительные затруднения при иллюстрации теоретических положений практическими примерами. У обучающегося отсутствует собственная точка зрения на заявленные проблемы. Обучающийся использовал несколько источников литературы
«не зачтено»	Конспект обучающегося не раскрывает тему по данному вопросу. Обучающийся не может привести практических примеров. Материал излагается «житейским» языком, не используются понятия и термины соответствующей научной области. Обучающийся использовал недостаточное количество источников литературы. Обучающимся не представлен конспект

Доклад

Шкала оценивания	Критерии оценивания
«зачтено»	Доклад создан с использованием компьютерных технологий (презентация Power Point, 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)
	Доклад создан с использованием компьютерных технологий (презентация Power Point, 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)
	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
«не зачтено»	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

Контрольная работа

Шкала оценивания	Критерии оценивания
«зачтено»	Обучающийся полностью и правильно выполнил задания контрольной работы. Показал отличные знания и умения в рамках усвоенного учебного материала. Контрольная работа оформлена аккуратно и в соответствии с предъявляемыми требованиями
	Обучающийся выполнил задания контрольной работы с небольшими неточностями. Показал хорошие знания и умения в рамках усвоенного учебного материала. Есть недостатки в оформлении контрольной работы

	Обучающийся выполнил задания контрольной работы с существенными неточностями. Показал удовлетворительные знания и умения в рамках усвоенного учебного материала. Качество оформления контрольной работы имеет недостаточный уровень
«не зачтено»	Обучающийся не полностью выполнил задания контрольной работы, при этом проявил недостаточный уровень знаний и умений

Разноуровневые задания

Шкала оценивания	Критерии оценивания
«зачтено»	Демонстрирует очень высокий/высокий уровень знаний, умений, навыков в соответствии с критериями оценивания. Все требования, предъявляемые к заданию, выполнены
	Демонстрирует достаточно высокий/выше среднего уровень знаний, умений, навыков в соответствии с критериями оценивания. Все требования, предъявляемые к заданию, выполнены
	Демонстрирует средний уровень знаний, умений, навыков в соответствии с критериями оценивания. Большинство требований, предъявляемых к заданию, выполнены. Демонстрирует низкий/ниже среднего уровень знаний, умений, навыков в соответствии с критериями оценивания. Многие требования, предъявляемые к заданию, не выполнены
«не зачтено»	Демонстрирует очень низкий уровень знаний, умений, навыков в соответствии с критериями оценивания. Нет ответа. Не было попытки выполнить задание

Тестирование – текущий контроль:

Шкала оценивания	Критерии оценивания
«зачтено»	Обучающийся верно ответил на 70 – 100 % тестовых заданий при прохождении тестирования
«не зачтено»	Обучающийся верно ответил на 69 % и менее тестовых заданий при прохождении тестирования

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 конспектов

Темы конспектов выложены в электронной информационно-образовательной среде ЗабИЖТ ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведены темы конспектов, предусмотренные рабочей программой дисциплины.

Темы конспектов:

Раздел 1. Теоретические основы защиты информации

1.1 Виды ответственности за нарушение требований в области информационной безопасности.

Раздел 2. Информация: виды, методы и средства обеспечения безопасности.

2.1 Методы и средства борьбы с компьютерными вирусами.

Раздел 3. Организационно-правовое обеспечение информационной безопасности.

3.1 Электронная подпись: виды, назначение, защита файлов.

3.2 Темы докладов

Темы докладов выложены в электронной информационно-образовательной среде ЗабИЖТ ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведены темы докладов, предусмотренные рабочей программой дисциплины.

Темы докладов

Раздел 1. Теоретические основы защиты информации

1.1. Современные факторы, влияющие на защиту информации

Раздел 2. Информация: виды, методы и средства обеспечения безопасности

2.1. Государственная тайна, грифы секретности, сведения, составляющие государственную тайну, носители государственной тайны, доступ к государственной тайне.

2.2. Персональные данные. Нормативно-правовые документы, регламентирующие обеспечение прав и свобод граждан при обработке его персональных данных.

2.3. Процессуальные тайны. Сведения, составляющие тайну следствия и судопроизводства.

2.4. Служебная тайна.

2.5. Профессиональная тайна. Врачебная тайна. Нотариальная тайна. Адвокатская тайна. Тайна усыновления. Тайна страхования. Тайна исповеди. Банковская тайна

2.6. Коммерческая тайна, отнесение сведений к коммерческой тайне.

2.7. Личная тайна. Семейная тайна.

2.8. Защита интеллектуальной собственности. Авторское право. Международное право в сфере защиты информации. Защита авторских и смежных прав в законодательстве РФ. Объекты и субъекты авторского права. Права обладателей авторских прав.

2.9. Тайна сведений, содержащихся в личных делах осужденных.

2.10. Организация доступа персонала предприятия к конфиденциальной информации.

2.11. Информационные войны

Раздел 3. Организационно-правовое обеспечение информационной безопасности

3.1. Идентификация и аутентификация.

3.2. Криптография.

3.3. Построение системы защиты от угрозы нарушения целостности информации и отказа доступа.

3.4. Электронная подпись.

3.5. Дезинформация и методы борьбы с ней.

3.6. Контроль целостности потока сообщений.

3.7. Политика безопасности и аксиомы политики безопасности.

3.3 Типовые контрольные задания для проведения тестирования

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

Структура фонда тестовых заданий по дисциплине

Индикатор достижения компетенции	Тема в соответствии с РПД	Характеристика ТЗ	Количество тестовых заданий, типы ТЗ
ОПК-2.6 Умеет работать с файлами и документами, содержащими персональные данные и информацию ограниченного доступа	Тема 1. Значение информационной безопасности и ее место в системе национальной безопасности, современная Доктрина информационной безопасности РФ	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Действие	1 – ОТЗ 1 – ЗТЗ
	Тема 2. Теоретические и концептуальные основы защиты информации Современные факторы, влияющие на защиту информации	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Действие	1 – ОТЗ 1 – ЗТЗ
	Тема 3. Критерии, условия и принципы отнесения информации к защищаемой. Носители защищаемой информации: состав, классификация	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Действие	1 – ОТЗ 1 – ЗТЗ
	Тема 4. Классификации информации по видам тайн и степеням конфиденциальности, по собственникам и владельцам	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Действие	1 – ОТЗ 1 – ЗТЗ
	Тема 5. Понятие и структура угроз защищаемой информации. Источники, виды, условия и способы дестабилизирующего воздействия на защищаемую информацию	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Действие	1 – ОТЗ 1 – ЗТЗ
	Тема 6. Каналы и методы несанкционированного доступа к конфиденциальной информации. Направления, виды и особенности деятельности разведывательных служб по несанкционированному доступу к конфиденциальной информации	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Действие	1 – ОТЗ 1 – ЗТЗ
	Тема 7. Объекты защиты информации. Вирусное заражение информации. Классификация	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	1 – ОТЗ

	антивирусных программ		1 – ЗТЗ
		Действие	1 – ОТЗ 1 – ЗТЗ
	Тема 8. Кадровое, ресурсное и технологическое обеспечение защиты информации	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Действие	1 – ОТЗ 1 – ЗТЗ
	Тема 9. Назначение и структура систем защиты информации	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Действие	1 – ОТЗ 1 – ЗТЗ
		Итого	∑60 30 – ОТЗ 30 – ЗТЗ

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

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

Образец типового варианта итогового теста,
предусмотренного рабочей программой дисциплины

1. Сведения (сообщения, данные) независимо от формы их представления – это <:**информация**:>.

2. Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов:

а) Информация.
б) **Информационные технологии.**
в) Информационная система.
г) Информационно-телекоммуникационная сеть.
д) Обладатель информации.

3. Закон РФ «О государственной тайне» был принят в следующем <:**1993**:> году.

4. Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации

а) Источник информации.
б) Потребитель информации.
в) Уничтожитель информации.
г) Носитель информации.
д) **Обладатель информации.**

5. Информация, переданная или полученная пользователем информационно-телекоммуникационной сети:

а) **Электронное сообщение.**
б) Информационное сообщение.
в) Текстовое сообщение.
г) Визуальное сообщение.

д) SMS-сообщение.

6. Защита информации от утечки это деятельность по предотвращению:

а) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;

б) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

в) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;

г) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;

д) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

7. Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации – это

а) **государственная тайна;**

б) защищаемая информация;

в) сведения, составляющие тайну следствия и судопроизводства;

г) коммерческая тайна

8. Какие сведения **не** относятся к государственной тайне:

а) о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства;

б) о методах и средствах защиты секретной информации;

в) о мерах по обеспечению безопасности критической информационной инфраструктуры Российской Федерации и о состоянии ее защищенности от компьютерных атак;

г) о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях.

9. Действия с персональными данными, включая сбор, систематизацию, накопление, хранение, использование, распространение и т.д. – это <:**обработка**:> персональных данных.

10. Процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации - <:**аутентификация**:>

11. Процесс, а также результат проверки некоторых обязательных параметров пользователя и, при успешности, предоставление ему определенных полномочий на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом - <:**авторизация**:>

12. На рисунке изображена вербальная система обеспечения безопасности: <:**видеокамера**:>

13. Информацией, составляющей государственную тайну, владеет <:**государство**:>

14. Для защиты от вредоносных программ на ПЭВМ необходимо использовать <:**антивирусные программы**:>.

15. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

а) чтобы убедиться, что проводится справедливая оценка;

б) это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ;

в) поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа;

г) поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку.

16. Все компоненты информационной системы предприятия, в котором накапливаются и обрабатываются персональные данные

а) **Информационная система персональных данных.**

б) База данных.

в) Централизованное хранилище данных.

г) Система Статэкспресс.

д) Сервер.

17. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

а) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования.

б) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации.

в) Улучшить контроль за безопасностью этой информации.

г) Снизить уровень классификации этой информации.

18. Информация, которую следует защищать (по нормативам, правилам сети, системы) называется <:**защищаемой**:>.

3.4. Типовые разноуровневые задания

Разноуровневые задания выложены в электронной информационно-образовательной среде ЗабИЖТ ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец разноуровневого задания по теме, предусмотренной рабочей программой дисциплины.

Образец разноуровневого задания
по теме «Значение информационной безопасности и ее место в системе национальной безопасности, современная Доктрина информационной безопасности РФ»

Задание 1. Составить блок-схему нормативно-правовых актов по обеспечению информационной безопасности.

Задание 2. Заполнить таблицу анализа нормативно-правовых актов по обеспечению информационной безопасности, пользуясь информационно-справочными системами Internet

Нормативно-правовой акт	Что устанавливает/определяет?

В таблицу внести нормативно правовые акты согласно их классификации (по уровням), а также краткую характеристику документа (область применения, что устанавливает или определяет).

3.5 Типовое задание для выполнения контрольной работы

Варианты заданий для выполнения контрольной работы выложены в электронной информационно-образовательной среде ЗабИЖТ ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типового задания для выполнения контрольной работы по темам дисциплины, предусмотренными рабочей программой дисциплины.

Контрольная работа содержит три теоретических вопроса по каждому разделу дисциплины, тестовые задания.

Вариант контрольной работы соответствует последней цифре шифра обучающегося. Например, номер зачетной книжки заканчивается цифрами 897340, то номер варианта 10, если шифр 56983, то номер варианта - 3.

Номера теоретических заданий контрольной работы выбираются из каждого раздела и номер вопроса соответствует номеру варианта. Дать развернутые ответы на теоретические вопросы

Тестовые задания представлены в четвертом задании. Необходимо ответить на 10 тестовых заданий, соответствующих Вашему варианту (например, если вариант 5, то необходимо ответить на тестовые задания под номером 5, 15, 25, 35 и т.д). Ответы на тестовые задания представляются в виде «Вопрос-ответ», вопросы полностью копируются из пособия, ответ записывается только правильный (если тест с выбором ответа, но кроме правильного ответа необходимо указать его номер).

Образец типового варианта задания для выполнения контрольной работы

Задание 1. Теоретические основы защиты информации

1. Сформулируйте основные положения Доктрины информационной безопасности РФ.

2. Каковы основные цели защиты информации? Каковы основные задачи в области информационной безопасности?

3. Виды ответственности за нарушение законодательство в области обеспечения информационной безопасности. Кто несет ответственность за нарушение режима защиты информации?

4. Концептуальные основы защиты информации.

5. Какие факторы влияют на защиту информации?

6. Каково место информационной безопасности в системе национальной безопасности Российской Федерации?

7. Концепция комплексной защиты информации.

8. Исторические предпосылки развития теории комплексной безопасности.

9. Дать понятие информации, информационной безопасности, защиты информации (сравнить из разных источников)

10. Какова структура государственной системы защиты информации?

Задание 2. Информация: виды, методы и средства обеспечения безопасности

1. Перечислить и охарактеризовать особенности информации как объекта защиты. Классифицировать информацию по различным признакам.

2. Назовите уровни представления информации. Вещественные и энергетические носители информации. Каковы основные свойства защищаемой информации.

3. Государственная тайна, грифы секретности, сведения, составляющие государственную тайну, носители государственной тайны, доступ к государственной тайне.

4. Персональные данные. Нормативно-правовые документы, регламентирующие обеспечение прав и свобод граждан при обработке его персональных данных.

5. Процессуальные тайны. Сведения, составляющие тайну следствия и судопроизводства.

6. Служебная тайна.

7. Профессиональная тайна. Врачебная тайна. Нотариальная тайна. Адвокатская тайна. Тайна усыновления. Тайна страхования. Тайна исповеди. Банковская тайна

8. Коммерческая тайна, отнесение сведений к коммерческой тайне.

9. Анализ уязвимости системы. Классификация угроз информационной безопасности.

10. Компьютерные вирусы и защита от них.

Задание 3. Организационно-правовое обеспечение информационной безопасности

1. Основные направления защиты информации. В чем заключается организационно-правовая защита информации? Основные принципы организационной защиты информации.

2. Структура органов защиты информации и их основные функции.

3. Идентификация и аутентификация.

4. Криптография.

5. Электронная подпись.

6. Контроль целостности потока сообщений

7. Политика безопасности и аксиомы политики безопасности.

8. Дезинформация и методы борьбы с ней. Фейки.

9. Понятие система защиты информации. Структура защиты информации. Требования к системе защиты информации.

10. Организационные, технические и программные средства защиты информации.

Задание 4. Тестовые задания

1. Кто является основным ответственным за определение уровня классификации информации?

Варианты ответа:

а) Руководитель среднего звена

б) Высшее руководство

в) Владелец

г) Пользователь

2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

Варианты ответа:

а) Сотрудники

б) Хакеры

в) Атакующие

г) Контрагенты (лица, работающие по договору)

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

Варианты ответа:

а) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования

б) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

в) Улучшить контроль за безопасностью этой информации

г) Снизить уровень классификации этой информации

4. Что самое главное должно продумать руководство при классификации данных?

Варианты ответа:

а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным

б) Необходимый уровень доступности, целостности и конфиденциальности

в) Оценить уровень риска и отменить контрмеры

г) Управление доступом, которое должно защищать данные

5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

Варианты ответа:

а) Владельцы данных

б) Пользователи

в) Администраторы

г) Руководство

6. Что такое процедура?

Варианты ответа:

а) Правила использования программного и аппаратного обеспечения в компании

б) Пошаговая инструкция по выполнению задачи

в) Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

г) Обязательные действия

7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

Варианты ответа:

а) Поддержка высшего руководства

б) Эффективные защитные меры и методы их внедрения

в) Актуальные и адекватные политики и процедуры безопасности

г) Проведение тренингов по безопасности для всех сотрудников

8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

Варианты ответа:

а) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски

б) Когда риски не могут быть приняты во внимание по политическим соображениям

в) Когда необходимые защитные меры слишком сложны

г) Когда стоимость контрмер превышает ценность актива и потенциальные потери

9. Что такое политики безопасности?

Варианты ответа:

а) Пошаговые инструкции по выполнению задач безопасности

б) Общие руководящие требования по достижению определенного уровня безопасности

в) Широкие, высокоуровневые заявления руководства

г) Детализированные документы по обработке инцидентов безопасности

10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

Варианты ответа:

а) Анализ рисков

б) Анализ затрат / выгоды

в) Результаты ALE

г) Выявление уязвимостей и угроз, являющихся причиной риска

3.6 Перечень теоретических вопросов к зачету

(для оценки знаний)

Раздел 1. Теоретические основы защиты информации

1.1. Современные факторы, влияющие на защиту информации

1.2. Понятие национальной безопасности, виды безопасности. Информационная безопасность Российской Федерации.

1.3. Национальные интересы Российской Федерации в информационной сфере.

1.4. Приоритетные направления в области защиты информации в Российской Федерации.

1.5. Тенденции развития информационной политики государств и ведомств.

1.6. Терминологические основы информационной безопасности. Основные понятия и определения.

1.7. Понятие информации и смежных с ним: информационная безопасность, информационная война, информационная агрессия, информационное оружие, информационные процессы, информационная система, информационная сфера.

Раздел 2. Информация: виды, методы и средства обеспечения безопасности

2.1 Защита информации, тайна, средства защиты информации, угрозы — определения, сопоставление

2.2. Государственная тайна. Правовое обеспечение защиты информации.

2.3. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене.

2.4. Государственная тайна, грифы секретности, сведения, составляющие государственную тайну, носители государственной тайны, доступ к государственной тайне.

2.5. Персональные данные. Нормативно-правовые документы, регламентирующие обеспечение прав и свобод граждан при обработке его персональных данных.

2.6. Процессуальные тайны. Сведения, составляющие тайну следствия и судопроизводства.

2.7. Служебная тайна.

2.8. Профессиональная тайна. Врачебная тайна. Нотариальная тайна. Адвокатская тайна. Тайна усыновления. Тайна страхования. Тайна исповеди. Банковская тайна

2.9. Коммерческая тайна, отнесение сведений к коммерческой тайне.

2.10. Личная тайна. Семейная тайна.

2.11. Защита интеллектуальной собственности. Авторское право.

2.12. Тайна сведений, содержащихся в личных делах осужденных.

2.13. Организация доступа персонала предприятия к конфиденциальной информации.

2.14. Общеметодологические принципы теории информационной безопасности.

2.15. Комплексность. Этапы развития информационной безопасности: 1. Системы безопасности ресурса; 2. Этап развитой защиты (Постепенное осознание необходимости комплексирования целей защиты, Расширение арсенала используемых средств защиты, стали объединяться в функциональные самостоятельные системы защиты); 3. Этап комплексной защиты.

2.16. Требования к системе защиты информации.

2.17. Показатели информации: важность, полнота, адекватность, релевантность, толерантность.

2.18. Комплексность: целевая, инструментальная, структурная, функциональная, временная.

2.19. Угрозы. Классификация и анализ угроз информационной безопасности.

2.20. Понятие угрозы. Виды угроз. Три наиболее выраженные угрозы: 1) подверженность физическому искажению или уничтожению; 2) возможность несанкционированной (случайной или злоумышленной) модификации; 3) опасность несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена.

2.21. Характер происхождения угроз: умышленные факторы, естественные факторы. Источники угроз. Предпосылки появления угроз: объективные, субъективные.

2.22. Методы нарушения конфиденциальности, целостности и доступности информации.

2.23. Классы каналов несанкционированного получения информации: 1) непосредственно с объекта; 2) с каналов отображения информации; 3) получение по внешним каналам; 4) подключение к каналам получения информации.

2.24. Причины нарушения целостности информации: субъективные преднамеренные, субъективные непреднамеренные, объективные непреднамеренные.

2.25. Потенциально возможные злоумышленные действий в автоматизированных системах обработки данных.

2.26. Функции защиты информации: 4 функции.

2.27. Причины, виды, каналы утечки и искажения информации.

Раздел 3. Организационно-правовое обеспечение информационной безопасности

3.1. Архитектура систем защиты информации.

3.2. Органы, обеспечивающие национальную безопасность Российской федерации, цели, задачи.

3.3. Идентификация и аутентификация.

3.4. Криптография.

3.5. Построение системы защиты от угрозы нарушения целостности информации и отказа доступа.

3.6. Электронная подпись.

3.7. Дезинформация и методы борьбы с ней.

3.8. Контроль целостности потока сообщений.

3.9. Политика безопасности и аксиомы политики безопасности.

3.10. Последовательность решения задачи защиты информации.

3.11. Регулирование использования элементов системы и защищаемой информации.

3.12. Защита от информационного воздействия на технические средства обработки. Защита от информационного воздействия на общество. Защита от информационного воздействия на психику человека

3.7 Типовые практические задания к зачету
(для оценки умений)

Распределение практических заданий к зачету находится в закрытом для обучающихся доступе. Разработанный комплект типовых практических заданий к зачету не выставляется в электронную информационно-образовательную среду ЗабИЖТ ИрГУПС, а хранится на кафедре-разработчике в составе ФОС по дисциплине.

Ниже приведен образец типовых практических заданий к зачету.

Образец типовых практических заданий к зачету

Задание 1. Составить перечень органов, обеспечивающих информационную безопасность и защиту информации, их функции и задачи, заполнив таблицу

Органы государственной власти, обеспечивающие в рамках своих полномочий информационную безопасность и защиту информации	Нормативно, правовые акты, регламентирующие их деятельность	Основные функции в области информационной безопасности и защиты информации	Основные задачи в области информационной безопасности и защиты информации

Задание 2. Описать основные критерии отнесения информации к защищаемой.

Задание 3. Пользуясь различными источниками информации, классифицировать основные угрозы защищаемой информации.

3.8 Типовые практические задания к зачету
(для оценки навыков и (или) опыта деятельности)

Распределение практических заданий к экзамену находится в закрытом для обучающихся доступе. Разработанный комплект типовых практических заданий к зачету не выставляется в электронную информационно-образовательную среду ЗабИЖТ ИрГУПС, а хранится на кафедре-разработчике в составе ФОС по дисциплине.

Ниже приведен образец типовых практических заданий к зачету.

Образец типовых практических заданий к зачету

1. Провести анализ уязвимости объекта с точки зрения обеспечения информационной безопасности, описав в виде таблицы и/или структуру организации/предприятия, установив обмен информационными потоками (организацию/предприятие задает преподаватель или выбирается самостоятельно).
2. Опишите виды работ от НСД в заданном предприятии.
3. Сравните виды антивирусных программ, их достоинства или недостатки.

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
Конспект	Защита конспектов, предусмотренных рабочей программой дисциплины, проводится во время практических занятий. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся: тему конспектов и требования, предъявляемые к их выполнению и защите
Доклад	Защита докладов, предусмотренных рабочей программой дисциплины, проводится во время практических занятий. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся: тему докладов и требования, предъявляемые к их выполнению и защите
Разноуровневые задания	Выполнение разноуровневых заданий, предусмотренных рабочей программой дисциплины, проводятся во время практических занятий. Во время выполнения заданий разрешается пользоваться учебниками, справочниками, конспектами лекций, тетрадями для практических занятий
Контрольная работа	Преподаватель на установочном занятии доводит до обучающихся: темы, количество заданий в контрольной работе. Контрольная работа должна быть выполнена в установленный срок и в соответствии с правилами к оформлению (текстовой и графической частей), сформулированными в Положении «Требования к оформлению текстовой и графической документации. Нормоконтроль» в последней редакции. Выполненная контрольная работа передается для проверки преподавателю в установленные сроки. Если контрольная работа выполнена не в соответствии с указаниями или не в полном объеме, она возвращается на доработку
Тестирование (компьютерные технологии)	Тестирование проводится по результатам освоения тем или разделов дисциплины или по окончанию ее изучения во время практических занятий. Во время проведения тестирования пользоваться учебниками, справочниками, конспектами лекций, тетрадями для практических занятий не разрешено. Преподаватель на практическом занятии, предшествующем занятию проведения теста, доводит до обучающихся: темы, количество заданий в тесте, время выполнения. Результаты тестирования видны обучающемуся на компьютере сразу после прохождения теста

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

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

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

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

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

Средняя оценка уровня сформированности компетенций по результатам текущего контроля	Шкала оценивания
Оценка не менее 3,0 и нет ни одной неудовлетворительной оценки по текущему контролю	«зачтено»
Оценка менее 3,0 или получена хотя бы одна неудовлетворительная оценка по текущему контролю	«не зачтено»

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

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