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.В.ДВ.16.01 Кибербезопасность

рабочая программа дисциплины

Направление подготовки – 38.03.01 Экономика
Профиль – Цифровая экономика
Квалификация выпускника – бакалавр
Форма и срок обучения – 4 года очная форма
Кафедра-разработчик программы – Прикладная механика и математика

Общая трудоемкость в з.е. – 3
Часов по учебному плану (УП) – 108
В том числе в форме практической подготовки (ПП) – 4

Формы промежуточной аттестации в семестрах
очная форма обучения: экзамен 7 семестр

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

Семестр	7	**Итого**
Число недель в семестре	14	
Вид занятий	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/в т.ч. в форме ПП	**42/4**	**42/4**
– лекции	14	14
– практические	28/4	28/4
– лабораторные работы		
Самостоятельная работа	**30**	**30**
Экзамен	**36**	**36**
Итого	**108/4**	**108/4**

ЧИТА

Рабочая программа дисциплины разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования – бакалавриат по направлению 38.03.01 Экономика, утвержденным приказом Министерства образования и науки Российской Федерации от 12.08.2020 г. № 954

Программу составили:
к.ф-м.н., доцент Л. Г. Гомбоев
к.э.н., доцент кафедры О.Л. Быстрова

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «Прикладная механика и математика», протокол от «23» апреля 2024 г. № 10.

Зав. кафедрой, к.ф.-м.н., доцент Н.В. Пешков

СОГЛАСОВАНО

Кафедра «Экономика и управление», протокол от «29» апреля 2024 г. № 9.

Зав. кафедрой, к.э.н., доцент О.Л. Быстрова

1 ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1 Цели преподавания дисциплины

1	формирование у обучающихся необходимых знаний, умений и навыков в области кибербезопасности

1.2 Задачи дисциплины

1	изучение теоретических, методологических и практических проблем в области кибербезопасности
2	приобретение практических навыков работы с нормативно-правовыми документами в области кибербезопасности

1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины

Научно-образовательное воспитание обучающихся

Цель научно-образовательного воспитания – создание условий для реализации научно-образовательного потенциала обучающихся в форме наставничества, тьюторства, научного творчества.

Цель достигается по мере решения в единстве следующих задач:
– формирование системного и критического мышления, мотивации к обучению, развитие интереса к творческой научной деятельности;
– создание в студенческой среде атмосферы взаимной требовательности к овладению знаниями, умениями и навыками;
– популяризация научных знаний среди обучающихся;
– содействие повышению привлекательности науки, поддержка научно-технического творчества;
– создание условий для получения обучающимися достоверной информации о передовых достижениях и открытиях мировой и отечественной науки, повышения заинтересованности в научных познаниях об устройстве мира и общества;
– совершенствование организации и планирования самостоятельной работы обучающихся как образовательной технологии формирования будущего специалиста путем индивидуальной познавательной и исследовательской деятельности

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 / Часть, формируемая участниками образовательных отношений

2.1 Требования к предварительной подготовке обучающегося

1	Б1.В.ДВ.02.01 Электронная торговля
2	Б1.В.ДВ.02.02 Коммерция в цифровой экономике
3	Б1.В.ДВ.05.01 Операции с ценными бумагами
4	Б1.В.ДВ.05.02 Профессиональная деятельность на рынке ценных бумаг
5	Б1.В.ДВ.06.01 Финансовый менеджмент
6	Б1.В.ДВ.06.02 Инструменты финансового управления
7	Б1.В.ДВ.07.01 Анализ данных и прикладное программное обеспечение
8	Б1.В.ДВ.07.02 Цифровые сервисы
9	Б1.В.ДВ.11.01 Цифровые технологии налоговой системы
10	Б1.В.ДВ.11.02 Налогообложение в цифровой экономике
11	Б1.В.ДВ.12.01 Введение в цифровую экономику
12	Б1.В.ДВ.12.02 Основы цифровых технологий
13	Б2.О.02(Н) Учебная - научно-исследовательская работа (получение первичных навыков научно-исследовательской работы)

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

1	Б1.В.ДВ.08.01 Проектирование информационных систем в экономике
2	Б1.В.ДВ.08.02 Управление информационными ресурсами
3	Б1.В.ДВ.09.01 Цифровые финансы и платежные системы
4	Б1.В.ДВ.09.02 Цифровые услуги финансовых рынков и платежных систем
5	Б1.В.ДВ.14.01 Автоматизация бизнес-решений
6	Б1.В.ДВ.14.02 Бизнес-планирование в цифровой экономике
7	Б2.О.04(Пд) Производственная - преддипломная практика
8	Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы
9	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**
ПК.6.2 Способен на основе типовых методик и действующей нормативно-правовой базы рассчитать необходимые для составления экономических разделов планов показатели для принятия обоснованных экономических решений в области цифровых финансов и платежей	ПК-6.2.1 Разрабатывает бизнес-план развития финансовых организаций и платежных систем с учетом защиты систем, сетей и программ от цифровых атак	**Знать:** объекты компьютерных технологий, используемые в обеспечении кибербезопасности; понятийный аппарат в области бизнес-планирования; нормативно-правовые акты, нормативные и методические документы, регламентирующие деятельность по составления экономических разделов планов показатели для принятия обоснованных экономических решений в области цифровых финансов и платежей
		Уметь: анализировать угрозы, уязвимости, риски в области безопасности информации; применять знания о нормативных и методических документов, регламентирующих деятельность по защите информации в решении поставленных задач; применять знания по информационной безопасности в современном обществе
		Владеть: знаниями о современных технологиях, применяемых в области кибербезопасности; навыками составления документов с учетом требований нормативно-правовой документации; навыками оформления документов по организации защиты информации
ПК.6.4 Способен организовывать и сопровождать процессы в платежной системе	ПК-6.4.1 Сопровождает процессы организации и регистрации платежной системы, в т.ч. с использованием методов и моделей обеспечения информационной безопасности	**Знать:** основные термины и понятия организации и регистрации платежной системы; особенности информационные технологии, используемые в автоматизированных системах; тенденций развития информационных технологий, средств защиты информации
		Уметь: ставить цели, формулировать задачи, связанные с обеспечением информационной безопасности; анализировать тенденции развития систем обеспечения кибербезопасности; применять знания по расчетам финансово-экономических показателей функционирования цифровых финансов и платежей при решении поставленных задач
		Владеть: методами проведения анализа профессиональной деятельности для решения задач защиты информации; навыками работы с процессом организации и регистрации платежной системы; алгоритмами обработки информации, в сфере информационной безопасности

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ							
Код	**Наименование разделов, тем и видов работы**	**Очная форма**					***Код индикатора достижения компетенции**
		Семестр	**Часы**				
			Лек	**Пр**	**Лаб**	**СР**	
1.0	**Раздел 1 Основы кибербезопасности**	**7**	**6**	**12**		**14**	**ПК-6.2.1**
1.1	Тема 1. Задачи кибербезопасности и структура системы кибербезопасности	7	2			2	ПК-6.2.1
1.2	Практическое занятие № 1. Системы кибербезопасности в разных странах	7		2		2	ПК-6.2.1
1.3	Практическое занятие № 2. Основные понятия информационной безопасности: угрозы, уязвимость, атаки	7		2		2	ПК-6.2.1
1.4	Тема 2. Понятие информации и информатизации, свойства информации как объекта защиты от киберугроз	7	2				ПК-6.2.1
1.5	Практическое занятие № 3. Особенности современных киберсистем и кибератак	7		2		2	ПК-6.2.1
1.6	Практическое занятие № 4. Особенности защиты кибернетических систем: Internet-вещей, АСУТП, smart things	7		2		2	ПК-6.2.1
1.7	Тема 3. Антивирусы и защита электронного документооборота от не санкционированного доступа	7	2				ПК-6.2.1
1.8	Практическое занятие № 5. Характеристика и особенности современных антивирусных систем	7		2		2	ПК-6.2.1
1.9	Практическое занятие № 6. Общая характеристика сетей и протоколов передачи данных	7		2		2	ПК-6.2.1
2.0	**Раздел 2. Принципы построения системы кибербезопасности**	**7**	**4**	**8/2**		**8**	**ПК-6.4.1**
2.1	Тема 4. Общие требования к паролям симметричное и асимметричное шифрование	7	2				ПК-6.4.1
2.2	Практическое занятие № 7. Методы защиты информации на основе криптографических преобразований	7		2/2		2	ПК-6.4.1
2.3	Практическое занятие № 8. Методы проверки подлинности	7		2		2	ПК-6.4.1
2.4	Тема 5. Хэш-функция и электронная подпись и протоколы электронных данных	7	2				ПК-6.4.1
2.5	Практическое занятие № 9. Хэш-функция и электронная подпись	7		2		2	ПК-6.4.1
2.6	Практическое занятие № 10. Защищенные каналы данных облачные технологии и защищённый документооборота	7		2		2	ПК-6.4.1
3.0	**Раздел 3. Киберпреступность и способы её предотвращения**	**7**	**4**	**8/2**		**8**	**ПК-6.2.1**
3.1	Тема 6. Нормативно-правовые акты и стандарты по кибербезопасности	7	2				ПК-6.2.1
3.2	Практическое занятие № 11. Стандарты в области обеспечения информационной безопасности	7		2		2	ПК-6.2.1
3.3	Практическое занятие № 12. Безопасносное восстановление информационных систем	7		2		2	ПК-6.2.1
3.4	Тема 7. Преступления в сфере информационных технологий	7	2				ПК-6.2.1

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работы	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
3.5	Практическое занятие № 13. Системы обнаружения вторжений	7		2		2	ПК-6.2.1
3.6	Практическое занятие № 14. Киберпреступность в современном мире	7		2/2		2	ПК-6.2.1
	Форма промежуточной аттестации - экзамен	7	36				ПК-6.2.1, ПК-6.4.1

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 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	Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами: монография / А. И. Белоус, В. А. Солодуха. - Москва; Вологда: Инфра-Инженерия, 2020. - 692 с. - ISBN 978-5-9729-0486-0. - Текст: электронный. - URL: https://znanium.ru/catalog/product/1167736 – Режим доступа: по подписке (дата обращения: 23.04.2024)	онлайн
6.1.1.2	Велигура, А. Н. Комбинаторика и теория графов для кибербезопасности : учебное пособие / А. Н. Велигура. — Москва: НИЯУ МИФИ, 2021. — 200 с. — ISBN 978-5-7262-2836-5. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/284441 — Режим доступа: для авториз. пользователей (дата обращения: 23.04.2024)	онлайн
	Кибербезопасность в условиях электронного банкинга: практическое пособие: [16+] / А. А. Бердюгин, А. Б. Дудка, С. В. Конявская [и др.]; под ред. П. В. Ревенкова. – Москва: Прометей, 2020. – 522 с.: ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=610688 – Библиогр. в кн. – ISBN 978-5-907244-61-0. – 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		онлайн
6.1.2.2	Компьютерные сети: учебник : [12+] / А. Н. Алексахин, С. А. Алексахина, А. В. Батищев [и др.] ; под общ. ред. А. М. Нечаева. – Москва: Университет Синергия, 2023. – 313 с. : ил., табл., схем. – (Университетская серия). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=699933 – Библиогр. в кн. – ISBN 978-5-4257-0558-7. – DOI 10.37791/978-5-4257-0558-7-2023-1-312. – Текст: электронный. (дата обращения: 23.04.2024)	онлайн

6.1.2.3	Яковлев, В.В. Технологии виртуализации и консолидации информационных ресурсов: учебное пособие / В. В. Яковлев. — Москва: ФГБОУ «Учебно-методический центр по образованию на железнодорожном транспорте», 2015. — 156 с. — 978-5-89035-837-0. — Текст: электронный // УМЦ ЖДТ: электронная библиотека. — URL: https://umczdt.ru/books/1210/30049/ — Режим доступа: по подписке (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	Быстрова О.Л. Пешков Н.В. Кибербезопасность Учебное методическое пособие для практических и самостоятельных работ для студентов всех форм обучения направления подготовки «Экономика» профиль Цифровая экономика	рукопись
6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»		
6.2.1	АСУ Библиотека ЗабИЖТ http://zabizht.ru	
6.2.2	ЭБС "Издательство "Лань" https://e.lanbook.com/	
6.2.3	Электронная библиотечная система Знаниум https://znanium.ru	
6.2.4	Электронная библиотека Учебно-методического центра по образованию на железнодорожном транспорте https://umczdt.ru/books/	
6.2.5	Электронная библиотека Университетская библиотека http://biblioclub.ru	
6.3 Программное обеспечение и информационные справочные системы		
6.3.1 Базовое программное обеспечение		
6.3.1.1	MicrosoftWindows 7 Professional, лицензия № 49156201, государственный контракт от 03.10.2011 г. № 139/53-ОАЭ-11	
6.3.1.2	MicrosoftOffice 2007 Standard, лицензия № 45777622, государственный контракт от 10.08.2009 г. №64/17-ОА-09; MicrosoftOffice 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		
6.4.1	Не предусмотрено	

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 416 для проведения лекционных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованная специализированной мебелью и техническими средствами обучения (интерактивная доска, компьютер), служащими для представления учебной информации большой аудитории. Для проведения занятий лекционного типа имеются учебно-наглядные пособия (презентации), обеспечивающие тематические иллюстрации содержания дисциплины
3	Учебная аудитория 211 для проведения лабораторных работ, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованная специализированной мебелью и техническими средствами обучения (компьютеры с подключением к сети Интернет, обеспечивающие доступ в электронную информационно-образовательную среду ЗабИЖТ ИрГУПС, интерактивная доска). Для проведения занятий имеются учебно-наглядные пособия (презентации, плакаты, таблицы), обеспечивающие тематические иллюстрации содержания дисциплины
4	Учебная аудитория 212 для проведения лабораторных работ, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованная специализированной

	мебелью и техническими средствами обучения (компьютеры с подключением к сети Интернет, обеспечивающие доступ в электронную информационно-образовательную среду ЗабИЖТ ИрГУПС). Для проведения занятий имеются учебно-наглядные пособия (презентации, плакаты), обеспечивающие тематические иллюстрации содержания дисциплины
5	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 ИрГУПС. Помещения для самостоятельной работы обучающихся: – читальный зал; –4.15, 3.24
6	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. Лекция (от латинского «lection» – чтение) – вид аудиторных учебных занятий. Лекция: закладывает основы научных знаний в систематизированной, последовательной, обобщенной форме; раскрывает состояние и перспективы развития соответствующей области науки и техники; концентрирует внимание обучающихся на наиболее сложных, узловых вопросах; стимулирует познавательную активность обучающихся. Во время лекционных занятий обучающийся должен уметь сконцентрировать внимание на изучаемых проблемах и включить в работу все виды памяти: словесную, образную и моторно-двигательную. Для этого весь материал, излагаемый преподавателем, обучающемуся необходимо конспектировать. В конспект рекомендуется выписывать определения, формулировки и т.п. На полях конспекта следует помечать вопросы, выделенные обучающимся для консультации с преподавателем. Полезно составить краткий справочник, содержащий определения важнейших понятий дисциплины. К каждой лекции следует разобрать материал предыдущей лекции. Изучая материал по учебнику или конспекту лекций, следует переходить к следующему вопросу только в том случае, когда хорошо усвоен предыдущий вопрос. При этом необходимо воспроизводить на бумаге все рассуждения, как имеющиеся в учебнике или конспекте. Ряд вопросов дисциплины может быть вынесен на самостоятельное изучение. Такое задание требует оперативного выполнения. В конспекте лекций необходимо оставить место для освещения упомянутых вопросов. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии
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, ситуации. 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. Особое внимание следует обращать на определение основных понятий дисциплины. Обучающийся должен подробно разбирать примеры, которые поясняют

	понятия. Практическая подготовка, включаемая в практические занятия, предполагает выполнение обучающимся отдельных элементов работ, связанных с будущей профессиональной деятельностью и направленных на формирование умений и практических навыков
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 учебной 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 (ФОС) 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 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 «Кибербезопасность» участвует в формировании компетенций:

ПК-6.2 – способен на основе типовых методик и действующей нормативно-правовой базы рассчитать необходимые для составления экономических разделов планов показатели для принятия обоснованных экономических решений в области цифровых финансов и платежей;

ПК-6.4 – способен организовывать и сопровождать процессы в платежной системе.

Программа контрольно-оценочных мероприятий очная форма обучения

№	Наименование контрольно-оценочного мероприятия	Объект контроля (тема/раздел дисциплины)	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
7 семестр				
1	Текущий контроль	Раздел 1 Основы кибербезопасности	ПК-6.2.1	Индивидуальное творческое задание (письменно), доклад (устно), разноуровневые задания (письменно), тестирование (компьютерные технологии)
2	Текущий контроль	Раздел 2 Принципы построения системы кибербезопасности	ПК-6.4.1	Индивидуальное творческое задание (письменно), доклад (устно), разноуровневые задания (письменно), тестирование (компьютерные технологии). В рамках ПП**: индивидуальное творческое задание (письменно)
3	Текущий контроль	Раздел 3 Киберпреступность и способы её предотвращения	ПК-6.2.1	Индивидуальное творческое задание (письменно), доклад (устно), тестирование (компьютерные технологии). В рамках ПП**: разноуровневые задания (письменно)
4	Промежуточная аттестация	Раздел 1 Основы кибербезопасности. Раздел 2 Принципы построения системы кибербезопасности. Раздел 3 Киберпреступность и способы её предотвращения	ПК-6.2.1, ПК-6.4.1	Экзамен (собеседование), экзамен – 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 заносятся преподавателем в журнал и учитываются в виде средней оценки при проведении промежуточной аттестации

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

Перечень оценочных средств сформированности компетенций представлен в нижеследующей таблице

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Творческое задание	Частично регламентированное задание, имеющее нестандартное решение и позволяющее диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения. Может выполняться в индивидуальном порядке или группой обучающихся. Может быть использовано для оценки знаний, навыков и (или) опыта деятельности обучающихся	Образец индивидуальных творческих заданий
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, навыков и (или) опыта деятельности обучающихся	Темы докладов
3	Разноуровневые задания	Различают задачи и 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 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	Типовые разноуровневые задания
4	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
5	Экзамен	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень теоретических вопросов и типовые практические задания к экзамену (образец экзаменационного билета)
6	Тест – промежуточная аттестация в форме экзамена	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

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

Тест – промежуточная аттестация в форме экзамена:

Шкала оценивания	Критерии оценивания
«отлично»	Обучающийся верно ответил на 90 – 100 % тестовых заданий при прохождении тестирования
«хорошо»	Обучающийся верно ответил на 80 – 89 % тестовых заданий при прохождении тестирования
«удовлетворительно»	Обучающийся верно ответил на 70 – 79 % тестовых заданий при прохождении тестирования
«неудовлетворительно»	Обучающийся верно ответил на 69 % и менее тестовых заданий при прохождении тестирования

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Творческое задание

Шкала оценивания	Критерии оценивания
«отлично»	Представленная работа демонстрирует точное понимание задания и полное ему соответствие. В работе приводятся конкретные факты и примеры. Материал изложен логично. Работа и форма её представления является авторской, выполнена самостоятельно и содержит большое число оригинальных, изобретательных примеров. Эффективное использование изображений, видео, аудио и других мультимедийных возможностей, чтобы представить свою тему и вызвать интерес. Презентация имеет все необходимые разделы, данные об авторе, ссылки на источники, оформлена в

	одном стиле. Текст не избыточен на слайде, не имеет орфографических и речевых ошибок
«хорошо»	Представленная работа демонстрирует понимание задания. В работу включаются как материалы, имеющие как непосредственное отношение к теме, так и материалы, не имеющие отношения к ней. Содержание работы соответствует заданию, но не все аспекты задания раскрыты. В работе есть элементы творчества. Используются однотипные мультимедийные возможности, или некоторые из них отвлекают внимание от темы презентации. Основные требования к презентации соблюдены, но отсутствует выполнение требований либо к оформлению, либо к содержанию. Текст на слайде не избыточен, но плохо читается, несколько неудачных речевых выражений.
«удовлетворительно»	В работу включена собранная обучающимся информация, но она не анализируется и не оценивается. Нарушение логики в изложении материала. Обычная, стандартная работа, элементы творчества отсутствуют. Не используются изображения, видео, аудио и другие мультимедийные возможности, или их использование отвлекает внимание. Не соблюдены требования к оформлению презентации. Слишком много текста, или две и более орфографических ошибок, или речевые и орфографические ошибки
«неудовлетворительно»	Включены материалы, не имеющие непосредственного отношения к теме работы, содержание работы не относится в рассматриваемой проблеме. Отсутствует логики в изложении материала. Не используются изображения, видео, аудио и другие мультимедийные возможности, или их использование отвлекает внимание. Не соблюдены требования к оформлению презентации

Доклад

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

Разноуровневые задания

Шкала оценивания	Критерии оценивания
«отлично»	Демонстрирует очень высокий/высокий уровень знаний, умений, навыков в соответствии с критериями оценивания. Все требования, предъявляемые к заданию, выполнены
«хорошо»	Демонстрирует достаточно высокий/выше среднего уровень знаний, умений, навыков в соответствии с критериями оценивания. Все требования, предъявляемые к заданию, выполнены
«удовлетворительно»	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

«неудовлетворительно»	Демонстрирует очень низкий уровень знаний, умений, навыков в соответствии с критериями оценивания. Не ответа. Не было попытки решить задачу

Тестирование – текущий контроль:

Шкала оценивания	Критерии оценивания
«отлично»	Обучающийся верно ответил на 90 – 100 % тестовых заданий при прохождении тестирования
«хорошо»	Обучающийся верно ответил на 80 – 89 % тестовых заданий при прохождении тестирования
«удовлетворительно»	Обучающийся верно ответил на 70 – 79 % тестовых заданий при прохождении тестирования
«неудовлетворительно»	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

3.1 Образец индивидуальных творческих заданий

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

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

Образец индивидуального творческого задания

Задание. Каждому обучающемуся выбрать любую страну и рассмотреть существующую систему кибербезопасности в этой стране. Всей группе заполнить таблицу по всем перечисленным странам:

Страна	Рейтинг кибербезопасности	Цели кибербезопасности	Описание системы	Угрозы (примеры)

Образец индивидуального творческого задания, выполняемого в рамках практической подготовки

Задание.

1. Изучить предлагаемый теоретический материал по персональной кибербезопасности.
2. Оценить экономический эффект применения инструментов персональной кибербезопасности. Рассмотреть защиту персонального компьютера, ноутбука и смартфона
3. Составить таблицу сравнительного анализа экономического эффекта применения инструментов персональной кибербезопасности. Оценить соотношение цена/качество.

Таблица - Перечень объектов защиты

№	Объект защиты	Область защиты
1	Студент университета	Ноутбук, смартфон, средства связи
2	IT-специалист на удаленном доступе	Персональный компьютер, ноутбук, смартфон, средства связи
3	Модератор информационного ресурса	Персональный компьютер, ноутбук, смартфон, средства связи
4	Спич-райтер	Ноутбук, смартфон, средства связи
5	Блогер	Ноутбук, смартфон, средства связи
6	Школьник	Ноутбук, смартфон, средства связи
7	Менеджер среднего звена на удаленном доступе	Персональный компьютер, ноутбук, смартфон, средства связи
8	Специалист по анализу данных на удаленном доступе	Персональный компьютер, ноутбук, смартфон, средства связи
9	Разработчик сайтов на удаленном доступе	Персональный компьютер, ноутбук, смартфон, средства связи
10	Программист на удаленном доступе	Персональный компьютер, ноутбук, смартфон, средства связи

Контрольные вопросы

1. Оценка средств криптозащиты.
2. Экономическое обоснование расходов на обеспечение персональной кибербезопасности.
3. Обоснованный выбор мер и средств обеспечения персональной кибербезопасности.
4. Преимущества и недостатки существующих методов обоснования инвестиций в средства обеспечения персональной кибербезопасности.

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

1. Методы борьбы с фишинговыми атаками.
2. Законодательство о персональных данных.
3. Защита авторских прав.
4. Назначение, функции и типы систем видеозащиты.
5. Как подписывать с помощью ЭЦП электронные документы различных форматов.
6. Обзор угроз и технологий защиты Wi-Fi-сетей.
7. Проблемы внедрения дискового шифрования.
8. Борьба со спамом: основные подходы, классификация, примеры, прогнозы на будущее.
9. Особенности процессов аутентификации в корпоративной среде.
10. Квантовая криптография.
11. Утечки информации: как избежать. Безопасность смартфонов.
12. Безопасность применения пластиковых карт - законодательство и практика.
13. Защита CD- и DVD-дисков от копирования.
14. Современные угрозы и защита электронной почты.
15. Программные средства анализа локальных сетей на предмет уязвимостей.
16. Безопасность применения платежных систем - законодательство и практика.
17. Аудит программного кода по требованиям безопасности.
18. Антишпионское ПО (antispyware).
19. Обеспечение безопасности Web-сервисов.
20. Защита от внутренних угроз.
21. Технологии RFID.
22. Уничтожение информации на магнитных носителях.
23. Ботнеты - плацдарм современных кибератак.
24. Цифровые водяные знаки в изображениях.
25. Электронный документооборот. Модели нарушителя.
26. Идентификация по голосу. Скрытые возможности.
27. Безопасность океанских портов.
28. Безопасность связи.
29. Безопасность розничной торговли.
30. Банковская безопасность.
31. Информатизация управления транспортной безопасностью.
32. Биопаспорт.
33. Обзор современных платформ архивации данных.
34. Что такое консалтинг в области ИБ.
35. Бухгалтерская отчетность как источник рассекречивания информации.
36. Управление рисками: обзор употребительных подходов.

37. Категорирование информации и информационных систем. Обеспечение базового уровня информационной безопасности.

38. Распределенные атаки на распределенные системы.

39. Оценка безопасности автоматизированных систем.

40. Windows и Linux: что безопаснее?

41. Функциональная безопасность программных средств.

42. Технологические процессы и стандарты обеспечения функциональной безопасности в жизненном цикле программных средств.

43. Информационная безопасность: экономические аспекты.

44. Преступления против конфиденциальности, целостности и доступности компьютерных данных или систем.

45. Правонарушения, связанные с использованием компьютерных средств.

46. Компьютерное мошенничество или подлог.

47. Компьютерные преступления, связанные с использованием персональных данных, и спам.

48. Компьютерные преступления, касающиеся авторских прав или товарных знаков.

49. Деяния, предполагающие использование компьютера в целях причинения личного вреда.

50. Завлечение детей или «груминг».

51. Правонарушения, связанные с содержанием компьютерных данных.

3.3 Типовые разноуровневые задания

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

Ниже приведен образец разноуровневых заданий по темам, предусмотренным рабочей программой дисциплины.

Образец разноуровневого задания

Задание. Тематическое исследование: к какому типу киберпреступности относится это преступление? Контролер компании Scoular.co, занимающейся торговлей сырьевыми товарами, предположительно получил электронные письма от имени генерального директора компании Чака Элси (Chuck Elsea) и базирующейся в штате Небраска аудиторской фирмы, которая сотрудничает с компанией, с просьбой об осуществлении трех банковских переводов в китайский банк на общую сумму около 17 миллионов долларов (Reuters, 2015). В электронных письмах содержалась просьба о сохранении конфиденциальности, поскольку деньги предназначались для приобретения китайской компании. Контролер выполнил требования, полагая, что письма отправил генеральный директор, хотя использованный адрес электронной почты не был официальным адресом электронной почты компании. К какому типу киберпреступности относится это преступление? Пожалуйста, объясните свой ответ.

Образец разноуровневого задания,
выполняемого в рамках практической подготовки

Задание. Случаи совершения киберпреступлений

До начала занятия обучающихся следует в произвольном порядке распределить по группам, чтобы они могли выполнить задание до того, как все группы соберутся в аудитории. Каждой группе в произвольном порядке должна быть определена одна из следующих категорий киберпреступности:

- преступления против конфиденциальности, целостности и доступности компьютерных данных или систем;

- правонарушения, связанные с использованием компьютерных средств;
- правонарушения, связанные с содержанием компьютерных данных.

Необходимо провести исследование, отыскать случай совершения киберпреступления и прийти подготовленными к обсуждению этого случая

Обучающиеся могут поискать случаи совершения киберпреступлений в базе данных судебных дел УНП ООН SHERLOC: https://www.unodc.org/cld/v3/sherloc/

3.4 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 тестовых материалов по дисциплине «Кибербезопасность»

Индикатор достижения компетенции	Тема в соответствии с РПД	Характеристика ТЗ	Количество тестовых заданий, типы ТЗ
ПК-6.2.1 Разрабатывает бизнес-план развития финансовых организаций и платежных систем с учетом защиты систем, сетей и программ от цифровых атак	Задачи кибербезопасности и структура системы кибербезопасности	Знание	3 – ОТЗ 3 – ЗТЗ
		Умение	3 – ОТЗ 3 – ЗТЗ
		Действие	3 – ОТЗ 3 – ЗТЗ
	Понятие информации и информатизации, свойства информации как объекта защиты от киберугроз	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Действие	2 – ОТЗ 2 – ЗТЗ
	Антивирусы и защита электронного документооборота от не санкционированного доступа	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Действие	2 – ОТЗ 2 – ЗТЗ
	Нормативно-правовые акты и стандарты по кибербезопасности	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Действие	2 – ОТЗ 2 – ЗТЗ
	Преступления в сфере информационных технологий	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Действие	2 – ОТЗ 2 – ЗТЗ
ПК-6.4.1 Сопровождает процессы организации и регистрации платежной системы, в т.ч. с использованием методов и моделей обеспечения информационной безопасности	Общие требования к паролям симметричное и асимметричное шифрование	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Действие	2 – ОТЗ 2 – ЗТЗ
	Хэш-функция и электронная подпись и протоколы электронных данных	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ

		Действие	2 – ОТЗ 2 – ЗТЗ
		Итого	45 – ОТЗ 45 – 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. Детализированные документы по обработке инцидентов безопасности <…….>.

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

а) Анализ рисков.

б) Анализ затрат / выгоды.

в) Результаты ALE.

г) Выявление уязвимостей и угроз, являющихся причиной риска.

3. Цель расчета ALE? <…….>

4. Тактическое планирование – это <…….> планирование

5. Что является определением воздействия (exposure) на безопасность?

а) Нечто, приводящее к ущербу от угрозы.

б) Любая потенциальная опасность для информации или систем.

в) Любой недостаток или отсутствие информационной безопасности.

г) Потенциальные потери от угрозы.

6. Эффективная программа безопасности требует сбалансированного применения

а) Технических и нетехнических методов;

б) Контрмер и защитных механизмов;

в) Физической безопасности и технических средств защиты;

г) Процедур безопасности и шифрования.

7 Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

а) Внедрение управления механизмами безопасности.

б) Классификацию данных после внедрения механизмов безопасности.

в) Уровень доверия, обеспечиваемый механизмом безопасности.

г) Соотношение затрат / выгод.

8. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?

а) Только военные имеют настоящую безопасность.

б) Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности.

в) Военным требуется больший уровень безопасности, т.к. их риски существенно выше.

г) Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности.

9. Как рассчитать остаточный риск? <…….>

10. Что из перечисленного не является целью проведения анализа рисков?

а) Делегирование полномочий.

б) Количественная оценка воздействия потенциальных угроз.

в) Выявление рисков.

г) Определение баланса между воздействием риска и стоимостью необходимых контрмер.

11. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

а) Поддержка.

б) Выполнение анализа рисков.

в) Определение цели и границ.

г) Делегирование полномочий.

12. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод: <…….>.

13. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод: <…….>.

14. Деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё <…….>.

15. Естественные угрозы безопасности информации вызваны: <…….>.

16. Во сколько раз теоретически вырастет производительность при подсчёте числа слов в тексте при работе MapReduce при переходе от одного узла к двум? (Введите число.) <…….> .

17. Установить правильную последовательность этапов проекта аналитики в соответствии с CRISP-DM

(1) понимание бизнеса (Business understanding)

(2) понимание данных (Data Understanding)

(3) подготовка данных (Data Preparation)

(4) моделирование (Modeling)

(5) оценка (Evaluation)

(6) внедрение (Deployment)

18 Найдите соответствие определений антивирусов

детектор	Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы
доктор	Антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние
ревизор	Антивирус запоминает исходное состояние программ, каталогов и системных областей диска когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным
сторож	Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов

3.5 Перечень теоретических вопросов к экзамену
(для оценки знаний)

1. Основные понятия информационной безопасности.
2. Информационные технологии и необходимость ИБ.
3. Система защиты информации и ее структуры.
4. Экономическая информация как товар и объект безопасности.
5. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.
6. Персональные данные и их защита.
7. Информационные угрозы, их виды и причины возникновения.
8. Информационные угрозы для государства.
9. Информационные угрозы для компании.
10. Информационные угрозы для личности (физического лица).
11. Действия и события, нарушающие информационную безопасность.
12. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.
13. Способы воздействия информационных угроз на объекты.
14. Внешние и внутренние субъекты информационных угроз.
15. Компьютерные преступления и их классификация.
16. Исторические аспекты компьютерных преступлений и современность.
17. Субъекты и причины совершения компьютерных преступлений.
18. Вредоносные программы, их виды.
19. История компьютерных вирусов и современность.
20. Деятельность международных организаций в сфере информационной безопасности.
21. Государственное регулирование информационной безопасности в РФ.
22. Задачи ИБ в программе « цифровая экономика».
23. Доктрина информационной безопасности России.
24. Федеральные законы в сфере информатизации и информационной безопасности в РФ.
25. Уголовно-правовой контроль над компьютерной преступностью в РФ.
26. Политика безопасности и ее принципы.
27. Фрагментарный и системный подход к защите информации.
28. Методы и средства защиты информации.
29. Организационное обеспечение ИБ.
30. Организация конфиденциального делопроизводства.
31. Организационно-экономическое обеспечение ИБ.
32. Инженерно-техническое обеспечение компьютерной безопасности.
33. Организационно-правовой статус службы безопасности.
34. Защита информации в Интернете.
35. Электронная почта и ее защита.
36. Защита от компьютерных вирусов.
37. «Больные» мобильники и их «лечение».
38. Популярные антивирусные программы и их классификация.
39. Этапы и освоение защиты информации экономических объектов.
40. Криптографические методы защиты информации.
41. Оценка эффективности инвестиций в информационную безопасность.
42. Российские компании в сфере ИБ.
43. Фирмы, оценивающие работу персонала в компании.
44. Менеджмент и аудит ИБ на уровне предприятия.
45. Аудит ИБ автоматизированных банковских систем.
46. Аудит ИБ электронной коммерции.
47. Информационная безопасность предпринимательской деятельности.

3.6 Типовые практические задания к экзамену

(для оценки умений, навыков и (или) опыта деятельности)

Распределение практических заданий к экзамену находится в закрытом для обучающихся доступе. Разработанный комплект типовых практических заданий к экзамену 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 экзамену.

Образец типовых практических заданий к экзамену

1. Проанализировать свои действия в Интернете, которые могут скомпрометировать вашу безопасность или конфиденциальность.
2. Что такое кибервойна? Приведите примеры кибератак за последние 2 года.
3. Разработать многокритериальные классификационные схемы, позволяющие идентифицировать:

- криптосистему - с учетом особенностей ее реализации;
- потенциального взломщика - с учетом его мотивации, возможностей и квалификации;
- криптоаналитическую атаку - с учетом применимости к различным криптосистемам и необходимых для ее осуществления ресурсов.

4. На основе разработанных классификаций создать параметрические модели криптосистем, атак и злоумышленников.
5. Установить зависимость возможных сценариев взлома от характеристик злоумышленников и от особенностей реализации исследуемой криптосистемы.

4 Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности

В таблице дано описание процедур проведения контрольно-оценочных мероприятий, соответствующих рабочей программе дисциплины, и процедур оценивания результатов обучения с помощью спланированных оценочных средств.

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Творческое задание	Индивидуальные творческие задания выдаются на практических занятиях, предшествующих изучению предлагаемой темы. Задания выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет. Индивидуальные задания должны быть выполнены в установленный преподавателем срок и в соответствии с требованиями к оформлению (текстовой и графической частей), сформулированными в Положении «Требования к оформлению текстовой и графической документации. «Нормоконтроль» в последней редакции. Выполненные задания в назначенный срок сдаются на проверку
Доклад	Защита докладов предусмотренные 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 заданий репродуктивного уровня, предусмотренные рабочей программой дисциплины, проводятся во время практических занятий. Вариантов заданий по теме не менее пяти. Во время выполнения заданий пользоваться учебниками, справочниками, конспектами лекций, тетрадями для практических занятий не разрешено. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся: тему, количество заданий и время выполнения заданий
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 экзамена и оценивания результатов обучения

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

Билет содержит три задания: два теоретических вопроса для оценки знаний одно практическое задание оценки умений, навыков и (или) опыта деятельности. 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

(25-30 билетов) не выставляется в электронную информационно-образовательную среду ЗабИЖТ ИрГУПС, а хранится на кафедре-разработчике ФОС на бумажном носителе в составе ФОС по дисциплине.

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

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

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.

Образец экзаменационного билета для обучающихся

ЗабИЖТ ИрГУПС 20__ /20__ учебный год	Экзаменационный билет № 1 по дисциплине «Кибербезопасность»	УТВЕРЖДАЮ Заведующий кафедрой «ПМиМ» ЗабИЖТ _____ Н.В.Пешков
1. Информационные угрозы, их виды и причины возникновения		
2. Аудит ИБ автоматизированных банковских систем		
3. Разработать многокритериальные классификационные схемы, позволяющие идентифицировать: криптосистему - с учетом особенностей ее реализации; потенциального взломщика - с учетом его мотивации, возможностей и квалификации		
Составил:		