Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

ИНСТИТУТ ЭКОНОМИКИ, МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И АНАЛИЗА ДАННЫХ
Кафедра системного анализа и информатики

УТВЕРЖДЕНА

решением кафедры системного анализа и информатики

Протокол от № 01 от «03» сентября 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.О.10.05 Информационная безопасность

направление подготовки
09.03.03 Прикладная информатика

направленность (профиль)
«Веб-разработка»

квалификация
бакалавр

очная форма обучения

Год набора – 2021

Москва, 2020 г.

Автор–составитель:

к.т.н.. доцент кафедры системного анализа и информатики Каширская Е.Н.

Зав. кафедрой

Системного анализа и информатики Маруев С.А.

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Дисциплина «Информационная безопасность» обеспечивает овладение следующими компетенциями:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
УК ОС-2	Способен разработать проект на основе оценки ресурсов и ограничений	УК ОС -2.1	Способен применять необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы принятия управленческого решения.
		УК ОС-2.2	Способен анализировать альтернативные варианты решений для достижения намеченных результатов; разрабатывать план, определять целевые этапы и основные направления работ.
		УК ОС-2.3	Владеет методиками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах.
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1	ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
		ОПК-3.2	ОПК-3.2. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с

			применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
		ОПК-3.3	ОПК-3.3. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.
ОПК-4	Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.1	ОПК-4.1. Знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.
		ОПК-4.2	ОПК-4.2. Способен применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.
		ОПК-4.3	ОПК-4.3. Способен составлять техническую документацию на различных этапах жизненного цикла информационной системы.
УК ОС-10	Способен демонстрировать и формировать нетерпимое отношение к коррупционному поведению	УК ОС-10.1. УК ОС-10.2. УК ОС-10.3.	УК ОС-10.1. Способен применять необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы защиты информации и противодействия коррупции. УК ОС-10.2. Способен анализировать альтернативные варианты решений для обеспечения защиты информации и противодействия коррупции. УК ОС-10.3. Владеет методиками разработки

			цели и задач проекта; методами обеспечения защиты информации и противодействия коррупции.

В результате освоения дисциплины у студентов должны быть сформированы:

ОТФ/ТФ (при наличии профстандарта)/ профессиональные действия	Код этапа освоения компетенции	Результаты обучения
	УК ОС-2.1 УК ОС-2.2 УК ОС-2.3	УК-2.1.1 Знает необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы принятия управленческого решения. УК-2.1.2 Умеет использовать методологические основы принятия управленческого решения в профессиональной области УК-2.2.1 Знает методы анализа альтернативных решений для достижения намеченных результатов УК-2.2.2 Умеет разрабатывать план, определять целевые этапы и основные направления работ УК-2.3.1 Знает методики разработки цели и задач проекта УК-2.3.2 Владеет методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах.
	ОПК-3.1 ОПК-3.2 ОПК-3.3	ОПК-3.1.1 Знает основные принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры ОПК-3.1.2 Умеет применять информационно-коммуникационные технологии для решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности. ОПК-3.2.1 Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры ОПК-3.2.2

		Умеет решать стандартные задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. ОПК-3.3.1 Умеет выполнять анализ и формировать его результаты в виде докладов, презентаций, научных публикаций с использованием библиографии по научно-исследовательской работе с учетом требований информационной безопасности. ОПК-3.3.2 Владеет навыками научно-исследовательской работы с учетом требований информационной безопасности.
	ОПК-4.1 ОПК-4.2 ОПК-4.3	ОПК-4.1.1 Знает особенности всех этапов жизненного цикла информационной системы ОПК-4.1.2 Знает основные стандарты оформления технической документации для информационной системы ОПК-4.2.1 Умеет применять стандарты оформления технической документации на ИС ОПК-4.2.2 Владеет навыками оформления технической документации для информационной системы. ОПК-4.3.1 Знает перечень стандартной технической документации для каждого этапа жизненного цикла информационной системы. ОПК-4.3.2 Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы в соответствии с действующими стандартами
	УК ОС-10.1. УК ОС-10.2. УК ОС-10.3.	УК-10.1.1 Знает необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы защиты информации и противодействия коррупции. УК-10.1.2 Умеет использовать методологические основы

		принятия управленческого решения для обеспечения защиты информации и противодействия коррупции. УК-10.2.1 Знает методы анализа альтернативных решений для достижения намеченных результатов для обеспечения защиты информации и противодействия коррупции. УК-10.2.2 Умеет разрабатывать план, определять целевые этапы и основные направления работ для обеспечения защиты информации и противодействия коррупции. УК-10.3.1 Знает методики разработки цели и задач проекта для обеспечения защиты информации и противодействия коррупции. УК-10.3.2 Владеет методиками разработки цели и задач проекта; методами обеспечения защиты информации и противодействия коррупции.

2. Объем и место дисциплины в структуре образовательной программы Объем дисциплины

Объем дисциплины в ЗЕ и академических/астрономических часах – 5 ЗЕ (180/135 ч).
Количество академических/астрономических часов, выделенных на контактную работу по очной форме обучения с преподавателем – 64/48 часа, на самостоятельную работу обучающихся – 80/60 часа;

Место дисциплины в структуре ОП ВО

Дисциплина Б1.О.10.05 «Информационная безопасность» относится к обязательным дисциплинам базовой части учебного плана по направлению подготовки 09.03.03 Прикладная информатика.
Дисциплина изучается в 5 семестре. Освоение дисциплины опирается на объём знаний в области информатики и программирования, теории систем и системного анализа.
Форма промежуточной аттестации –в 5 семестре экзамен.

2.1. Регламент распределения видов работ по дисциплине с ДОТ

Данная дисциплина реализуется с применением дистанционных образовательных технологий (ДОТ). Распределение видов учебной работы, форматов текущего контроля представлены в таблице:

Вид учебной работы	**Формат проведения**
Лекции	С применением ДОТ
Практические занятия	С применением ДОТ
Самостоятельная работа	Частично с применением ДОТ
Промежуточная аттестация	С применением ДОТ
Формы текущего контроля	**Формат проведения**
Тестирование	В системе дистанционного обучения (СДО)
Эссе	В системе дистанционного обучения (СДО)

Ответ на практическом занятии, участие в дискуссии	С применением ДОТ

Доступ к системе дистанционных образовательных осуществляется каждым обучающимся самостоятельно с любого устройства на портале: https://lms.ranepa.ru. Пароль и логин к личному кабинету / профилю предоставляется студенту в деканате. Все формы текущего контроля, проводимые в системе дистанционного обучения, оцениваются в системе дистанционного обучения. Доступ к видео и материалам лекций предоставляется в течение всего семестра. Доступ к каждому виду работ и количество попыток на выполнение задания предоставляется на ограниченное время согласно регламенту дисциплины, опубликованному в СДО. Преподаватель оценивает выполненные обучающимся работы не позднее 10 рабочих дней после окончания срока выполнения.

3. Содержание и структура дисциплины Очная форма обучения

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.						Форма текущего контроля успеваемости*,
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	Л Р	ПЗ	К Р		промежуточной аттестации
1	Актуальность информационной безопасности в современных условиях	20	4		4		12	
2	Угрозы и возможные каналы утечки конфиденциальной информации.	24	6		6		12	
3	Компьютерные вирусы и деструктивные программы.	26	6		6		14	
4	Методы защиты информации в автоматизированных системах обработки данных.	22	4		4		14	
5	Стандарты безопасности компьютерных	26	6		6		14	

	систем.							
6	Обеспечение информационной безопасности в Интернет. Сеть интранет как основной объект нападений из Интернет.	26	6		6		14	
Промежуточная аттестация		**36/27**						**Экзамен,**
Всего		**180/135**	**32/24**		**32/24**		**80/60**	**36/27**

Содержание дисциплины

№ п/п	**Название темы**	**Основные вопросы и положения, раскрывающие содержание темы**
1.	Актуальность информационной безопасности в современных условиях	Что такое информационная безопасность. Актуальность проблемы информационной безопасности. Понятия и определения в информационной безопасности.
2	Угрозы и возможные каналы утечки конфиденциальной информации.	Основные закономерности возникновения и классификация угроз информационной безопасности. Пути и каналы утечки информации и их обобщенная модель. Классификация каналов утечки информации.
3	Компьютерные вирусы и деструктивные программы.	Классификация компьютерных вирусов. Файловые вирусы. Загрузочные вирусы. Макровирусы. Сетевые вирусы. Прочие вредные программы.
4	Методы защиты информации в автоматизированных системах обработки данных.	Откуда берутся компьютерные вирусы. Основные правила защиты от компьютерных вирусов. Антивирусные программы. Восстановление пораженных компьютерными вирусами объектов.
5	Стандарты безопасности компьютерных систем.	Критерии безопасности компьютерных систем. "Оранжевая книга". Руководящие документы Гостехкомиссии. Краткий обзор современных методов защиты информации. Ограничение доступа. Контроль доступа к аппаратуре. Разграничение и контроль доступа к информации АСОД. Разграничение привилегий на доступ. Идентификация и установление подлинности объекта. Криптографическое преобразование информации. Защита информации от утечки за счет побочного электромагнитного излучения и наводок.
6	Обеспечение информационной безопасности в Интернет. Сеть интранет как основной объект нападений из Интернет.	Примеры взломов сетей и Web-узлов. Пользователи и злоумышленники в Internet. Причины уязвимости сети Internet. Обеспечение информационной безопасности организации при ее подключении к Internet. Защита архитектуры клиент/сервер Удаленные атаки на интрасети.

		Классические методы взлома интрасетей. Современные методы взлома интрасетей. Улучшение паролей. Одноразовые пароли. Серверы аутентификации. Физическая изоляция. Изоляция протокола. Выделенные каналы и маршрутизаторы. Защита систем управления базами данных. Защита в сетевых операционных системах.

4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине

4.1. Формы и методы текущего контроля успеваемости обучающихся и промежуточной аттестации

4.1.1 В ходе реализации дисциплины «Информационная безопасность» используются следующие методы текущего контроля успеваемости обучающихся:

Тема (раздел)	Методы текущего контроля успеваемости
Тема 1	Опрос 1
Тема 2	Практическое задание 1, опрос 2
Тема 3	Практическое задание 2, опрос 3
Тема 4	Практическое задание 3, опрос 4
Тема 5, 6	Контрольная работа 1,2

− при проведении занятий семинарского типа дистанционно: опрос, дискуссия (устные ответы на вопросы преподавателя по теме занятия, групповое обсуждение вопросов); преподаватель, реализующий дисциплину, определяет самостоятельно планы семинарских занятий;
− при контроле результатов самостоятельной работы студентов дистанционно: эссе / устный экзамен по билетам / тест.

4.1.2. Экзамен проводится с применением следующих методов (средств):

Экзамен принимается в устной форме, по билетам. Экзаменационный билет включает два теоретических вопроса и один практический. Оценка знаний обучающегося на экзамене носит комплексный характер и определяется его:

- ответом на экзамене;
- учебными достижениями в семестровый период.

4.2. Материалы текущего контроля успеваемости

Текущий контроль успеваемости осуществляется непрерывно, на протяжении всего курса. Прежде всего, это устный опрос по ходу занятия, выполняемый для оперативной активизации внимания обучающихся и оценки их уровня восприятия. Помимо этого, контроль самостоятельной работы обучающихся осуществляется на практических занятиях, докладах с презентацией.

№ п/п	Контролируемые разделы (темы) дисциплины	Наименование оценочного средства

1	Темы 1-3	Контрольная работа
2	Тема 4.	Контрольная работа
3	Темы 5-6	Контрольная работа

4.3. Оценочные средства для промежуточной аттестации

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

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа формирования компетенции
УК ОС-2	Способность разработать проект на основе оценки ресурсов и ограничений	УК-2.1	УК-2.1.1 Знает необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы принятия управленческого решения. УК-2.1.2 Умеет использовать методологические основы принятия управленческого решения в профессиональной области
		УК-2.2	УК-2.2.1 Знает методы анализа альтернативных решений для достижения намеченных результатов УК-2.2.2 Умеет разрабатывать план, определять целевые этапы и основные направления работ
		УК-2.3	УК-2.3.1 Знает методики разработки цели и задач проекта УК-2.3.2 Владеет методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах.
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-	ОПК- 3.1	ОПК-3.1.1 Знает основные принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры ОПК-3.1.2 Умеет применять информационно-коммуникационные технологии для решения стандартных задач профессиональной деятельности с

	коммуникационных технологий и с учетом основных требований информационной безопасности		учетом основных требований информационной безопасности.
		ОПК-3.2	ОПК-3.2.1 Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры ОПК-3.2.2 Умеет решать стандартные задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
		ОПК-3.3	ОПК-3.3.1 Умеет выполнять анализ и формировать его результаты в виде докладов, презентаций, научных публикаций с использованием библиографии по научно-исследовательской работе с учетом требований информационной безопасности. ОПК-3.3.2 Владеет навыками научно-исследовательской работы с учетом требований информационной безопасности.
ОПК-4	Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.1	ОПК-4.1.1 Знает особенности всех этапов жизненного цикла информационной системы ОПК-4.1.2 Знает основные стандарты оформления технической документации для информационной системы
		ОПК-4.2	ОПК-4.2.1 Умеет применять стандарты оформления технической документации на ИС ОПК-4.2.2 Владеет навыками оформления технической документации для информационной системы.
		ОПК-4.3	ОПК-4.3.1 Знает перечень стандартной технической документации для каждого этапа жизненного цикла информационной системы. ОПК-4.3.2 Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы в соответствии с действующими стандартами

УК ОС-10	Способен демонстрировать и формировать нетерпимое отношение к коррупционному поведению	УК ОС-10.1. УК ОС-10.2. УК ОС-10.3	УК-10.1.1 Знает необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы защиты информации и противодействия коррупции. УК-10.1.2 Умеет использовать методологические основы принятия управленческого решения для обеспечения защиты информации и противодействия коррупции. УК-10.2.1 Знает методы анализа альтернативных решений для достижения намеченных результатов для обеспечения защиты информации и противодействия коррупции. УК-10.2.2 Умеет разрабатывать план, определять целевые этапы и основные направления работ для обеспечения защиты информации и противодействия коррупции. УК-10.3.1 Знает методики разработки цели и задач проекта для обеспечения защиты информации и противодействия коррупции. УК-10.3.2 Владеет методиками разработки цели и задач проекта; методами обеспечения защиты информации и противодействия коррупции.

4.3.2 Показатели и критерии оценивания компетенций на различных этапах их формирования

Этап освоения компетенции	Показатель оценивания	Критерий оценивания
1 этап (код этапа - УК-2.1)	Способен применять необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы принятия управленческого решения.	УК-2.1.1 Знает необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы принятия управленческого решения. УК-2.1.2 Умеет использовать методологические основы принятия управленческого решения в профессиональной области

2 этап (код этапа - УК-2.2)	Способен анализировать альтернативные варианты решений для достижения намеченных результатов; разрабатывать план, определять целевые этапы и основные направления работ.	УК-2.2.1 Знает методы анализа альтернативных решений для достижения намеченных результатов УК-2.2.2 Умеет разрабатывать план, определять целевые этапы и основные направления
3 этап (код этапа - УК-2.3)	Владеет методиками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах.	УК-2.3.1 Знает методики разработки цели и задач проекта УК-2.3.2 Владеет методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах.
1 этап этапа – ОПК-3.1)	Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	ОПК-3.1.1 Знает основные принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры ОПК-3.1.2 Умеет применять информационно-коммуникационные технологии для решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности.
2 этап этапа – ОПК-3.2)	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	ОПК-3.2.1 Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры ОПК-3.2.2 Умеет решать стандартные задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
3 этап (код этапа - ОПК-3.3)	Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	ОПК-3.3.1 Умеет выполнять анализ и формировать его результаты в виде докладов, презентаций, научных публикаций с использованием библиографии по научно-исследовательской работе с учетом требований информационной безопасности. ОПК-3.3.2 Владеет навыками научно-исследовательской работы с учетом требований информационной безопасности.
1 этап этапа –ОПК-4.1)	Знает основные стандарты оформления технической документации на	ОПК-4.1.1 Знает особенности всех этапов жизненного цикла информационной

	различных стадиях жизненного цикла информационной системы.	системы ОПК-4.1.2 Знает основные стандарты оформления технической документации для информационной системы
2 этап этапа –ОПК-4.2)	Способен применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	ОПК-4.2.1 Умеет применять стандарты оформления технической документации на ИС ОПК-4.2.2 Владеет навыками оформления технической документации для информационной системы.
3 этап (код этапа - ОПК-4.3)	Способен составлять техническую документацию на различных этапах жизненного цикла информационной системы.	ОПК-4.3.1 Знает перечень стандартной технической документации для каждого этапа жизненного цикла информационной системы. ОПК-4.3.2 Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы в соответствии с действующими стандартами
1 этап (код этапа – УК ОС - 10.1)	Способен применять необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы защиты информации и противодействия коррупции.	УК-10.1.1 Знает необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы защиты информации и противодействия коррупции. УК-10.1.2 Умеет использовать методологические основы принятия управленческого решения для обеспечения защиты информации и противодействия коррупции.
2 этап (код этапа – УК ОС- 10.2)	Способен анализировать альтернативные варианты решений для обеспечения защиты информации и противодействия коррупции.	УК-10.2.1 Знает методы анализа альтернативных решений для достижения намеченных результатов для обеспечения защиты информации и противодействия коррупции. УК-10.2.2 Умеет разрабатывать план, определять целевые этапы и основные направления работ для

		обеспечения защиты информации и противодействия коррупции.
3 этап этапа – УК ОС-10.3)	Владеет методиками разработки цели и задач проекта; методами обеспечения защиты информации и противодействия коррупции.	УК-10.3.1 Знает методики разработки цели и задач проекта для обеспечения защиты информации и противодействия коррупции. УК-10.3.2 Владеет методиками разработки цели и задач проекта; методами обеспечения защиты информации и противодействия коррупции.

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

Промежуточная аттестация включает в себя сдачу экзамена.

Экзамен предусматривает ответ на вопросы по билету (2 устных вопроса и одно практическое задание).

Типовые контрольные вопросы и задания для проведения промежуточной аттестации:

Перечень контрольных вопросов для экзамена:

1. Сущность, содержание понятий «опасность» и «безопасность», факторы, оказывающие влияние на информационную безопасность.
2. Топология информационного объекта и содержание ее элементов социотехнического информационного объекта.
3. Представить в виде схемы и прокомментировать методический аппарат формирования системы обеспечения информационной безопасности.
4. Методы обеспечения информационной безопасности Российской Федерации.
5. Цели и задачи обеспечения информационной безопасности предприятия.
6. Содержание организационных основ обеспечения информационной безопасности предприятия.
7. Силы, обеспечивающие информационную безопасность предприятия, роль и задачи службы обеспечения информационной безопасности.
9. Средства обеспечения информационной безопасности предприятия.
10. Технологии обеспечения информационной безопасности предприятия и направления их реализации.
11. Организационные меры эксплуатации системы обеспечения информационной безопасности.
12. Роль высших корпоративных органов, органов управления и акционеров в обеспечении информационной безопасности предприятия.
13. Возможности акционеров по формированию требований к информационной безопасности предприятия и контролю эффективности их выполнения.
14. Охрана объекта, охранные меры и режим охраны: сущность и содержание.
15. Содержание организации и осуществления охраны; неотложные меры руководства по защите персонала.
16. Сущность и принципы организации внутриобъектового режима.

17. Функциональные зоны внутриобъектового режима: методика разграничения и обособления .

18. Сущность и основы классификации средств охраны предприятия.

19. Сущность, содержание и принципы организации пропускного режима.

20. Контрольно-пропускной пункт: задачи, оборудование и организация дежурства.

21. Порядок осуществления пропускного режима.

22. Противопожарная защита: сущность, основы организации и средства.

23. Содержание основных документов организации противопожарной защиты.

24. Охрана конфиденциальных документов и имущества при транспортировке.

25. Требования и перечень мер по обеспечению безопасности в местах проведения закрытых и массовых мероприятий.

26. Обеспечение информационной безопасности совещаний и заседаний по конфиденциальным вопросам в ходе их подготовки.

27. Требования к помещению для проведения совещаний и заседаний по конфиденциальным вопросам.

28. Основные организационные меры по исключению закладок разведывательных электронных устройств.

29. Профилактическая работа с участниками совещаний и заседаний по конфиденциальным вопросам в интересах обеспечения информационной безопасности.

30. Обеспечение информационной безопасности совещаний и заседаний по конфиденциальным вопросам в ходе их проведения.

31. Понятие о персонале и психологических факторах воздействия на него как источниках угроз информационной безопасности.

32. Роль управления персоналом в обеспечении информационной безопасности предприятия, содержание функций управления персоналом, направления и методы работы с персоналом.

33. Особенности приема сотрудников на работу, связанную с конфиденциальной информацией.

34. Работа с кандидатами на замещение должностей, связанных с обработкой конфиденциальной информации.

35. Разрешительная система предприятия, обучение и увольнение персонала, связанного с конфиденциальной информацией.

36. Мониторинг осведомленности персонала о тайнах работодателя.

37. Факторы угроз информационной безопасности через СМИ и рекламу.

38. Основные приемы психологического воздействия через СМИ.

39. Типы манипулятивной рекламы и техника формирования доверия к коммуникатору в рекламных материалах и СМИ как фактор угроз информационной безопасности личности.

40. Роль и задачи органов управления в формировании условий обеспечения информационной безопасности при работе со СМИ и в рекламно-выставочной деятельности.

41. Задачи пресс-службы по обеспечению информационной безопасности деятельности предприятия.

42. Меры, исключающие открытое опубликование информации с ограниченным доступом в плане мероприятий по защите конфиденциальной информации на предприятии.

43. Формы и особенности работы со СМИ руководителя предприятия и его пресс-службы.

44. Направления защиты информации предприятия в ходе публикаторской деятельности.

45. Основы защиты информации предприятия в рекламно-выставочной деятельности.

46. Деятельность по обеспечению сервисов и содержание управления инцидентами.

47. Принципы эффективной политики реагирования на инциденты информационной безопасности.

48. Содержание основных инцидентов в обеспечении информационной безопасности согласно требованиям ГОСТ Р ИСО/МЭК ТО 18044-2007.

49. Содержание политики менеджмента инцидентов информационной безопасности согласно ГОСТ Р ИСО/МЭК ТО 18044-2007.

50. Содержание политики, ресурсы и инструменты расследования инцидентов информационной безопасности согласно ГОСТ Р ИСО/МЭК ТО 18044-2007.

51. Модели команды реагирования на инциденты и по расследованию инцидентов информационной безопасности.

52. Уровни организационных ролей и распределения ответственности в ходе эскалации реагирования на инциденты информационной безопасности.

53. Содержание процессов управления инцидентами, контроля проблем и ошибок согласно модели ITIL (Information Technology Infrastructure Library).

54. Содержание и виды эскалации проблемы в обеспечении информационной безопасности согласно модели ITIL.

55. Содержание понятия «риски» и технологии их анализа в интересах защиты информации.

56. Понятие качественной и количественной оценки рисков, шкалы и критерии измерения.

57. Комплексная оценка рисков безопасности и ее основные этапы. Особенности применения инструментальных средств оценки рисков на примере программного комплекса MSAT (Microsoft Security Assessment Tool).

58. Критерии оценки уровня информационной безопасности предприятия. Методика оценки рисков OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation).

59. Оценка текущего состояния информационной безопасности компании. Модели оценки угроз безопасности КСЗИ.

60. Сущность правовой нормы. Информационно-правовые нормы и их классификация.

61. Технико-правовые нормы в обеспечении информационной безопасности. Основы технического регулирования.

62. Роль и место информационного права в базовых звеньях отраслей права РФ.

63. Структура и направленность правовых мер обеспечения информационной безопасности.

64.Информация в правовой системе. Юридические особенности и свойства информации.

65. Сущность, назначение информационного права и содержание информационных отношений.

66. Методы правового регулирования и принципы информационного права.

67. Условия субъектности в информационном праве. Субъекты и объекты правоотношений в информационной сфере.

68. Система и нормы информационного права.

69. Сущность, содержание и социально-правовая структура информационных отношений. Правонарушения в информационной сфере.

70. Информационные правоотношения, возникающие при производстве, передаче и распространении информации, информационных ресурсов, продуктов и услуг.

71. Информационные правоотношения, возникающие при создании и применении информационных систем, их сетей, средств обеспечения.

72. Информационные правоотношения, возникающие при создании и применении средств и механизмов информационной безопасности.

73. Характеристики информационного общества, отражаемые Окинавской хартией глобального информационного общества 2000 г.

74. Структура Окинавской хартии глобального информационного общества 2000 г. Окинавская хартия о вхождении государств в информационное общество.

75. Сущность и Соглашения о сотрудничестве государств - участников СНГ в области обеспечения информационной безопасности и его основные положения.

76. Проблемы принятия международных конвенций по информационной безопасности. Предложения РФ в области совершенствования международной информационной безопасности.

77. Назначение базовых международных стандартов обеспечения информационной безопасности ISO/IEC 27001, 27002, 27003, 27004, 27007, 27011.

78. Акты отрасли информационного законодательства РФ и отрасли законодательства, акты которых включают отдельные информационно-правовые нормы.

79. «Стратегия обеспечения национальной безопасности РФ до 2020 г.» об информационной безопасности.

80. Сущность, предназначение и структура Доктрины информационной безопасности РФ.

81. Доктрина информационной безопасности РФ о национальных интересах России в информационной сфере и составляющих их достижения.

82 Задачи и методы обеспечения информационной безопасности в Доктрине информационной безопасности РФ.

83. Исходная концептуальная схема обеспечения информационной безопасности организаций Банковской системы РФ.

84. Сущность, роль и место политик безопасности в деятельности предприятия. Стратегии и политика обеспечения информационной безопасности согласно требованиям ГОСТ Р ИСО/МЭК 13335-1-2006.

85. Структура, исходные данные и уровни документирования требований политики информационной безопасности согласно требованиям ГОСТ Р ИСО/МЭК 17799-2005.

86. Сущность, цели, задачи лицензирования отдельных видов деятельности, основные принципы и полномочия органов, уполномоченных для ведения лицензионной деятельности.

87. Перечень видов деятельности, лицензируемых в интересах защиты государственной тайны и лицензионные требования.

88. Лицензирование деятельности по технической защите конфиденциальной информации, лицензионные требования, предъявляемые к соискателю лицензии и лицензиату.

89. Сущность, место и роль сертификации в техническом регулировании согласно требованиям ФЗ № 184 от 27 декабря 2002 г. Предмет технического регулирования.

90. Содержание сертификации в техническом регулировании согласно требованиям ФЗ № 184 от 27 декабря 2002 г.

91. Информация как объект правовых отношений.

92. Содержание, объект, виды и право интеллектуальной собственности.

93. Объекты институтов права интеллектуальной собственности.

94. Содержание интеллектуальных прав и отношения исключительного права на интеллектуальную собственность. Распоряжение исключительным правом.

95. Сущность и содержание, а также виды и исполнение лицензионного договора.

96. Нарушения и защита личных неимущественных и исключительных прав на интеллектуальную собственность.

97. Сущность, функции, источники и субъекты авторского и смежного права.

98. Объекты авторского права.
99. Содержание авторских прав.
100. Договоры, заключаемые автором произведения.

Оценочным средством промежуточной аттестации является оценка на экзамене результатов выполнения текущего контроля по дисциплине.

Оценивание студента на экзамене по дисциплине «Информационная безопасность»

Оценка	Требования к знаниям
Отлично	Оценка «отлично» выставляется обучающемуся, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает на экзамене, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, правильно обосновывает принятое решение. Учебные достижения в семестровый период демонстрируют высокую степень овладения программным материалом.
Хорошо	Оценка «хорошо» выставляется обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения. Учебные достижения в семестровый период демонстрируют хорошую степень овладения программным материалом.
Удовлетво-рительно	Оценка «удовлетворительно» выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ. Учебные достижения в семестровый период демонстрируют достаточную (удовлетворительную) степень овладения программным материалом.
Неудовлет-ворительно	Оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится обучающимся, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине. Учебные достижения в семестровый период не демонстрировали достаточную степень овладения программным материалом на пороговом уровне.

4.4. Методические материалы

4.4.1. Методические материалы, определяющие процедуру оценивания ответов обучающихся на вопросы на понимание пройденного материала

Критериями оценки ответа обучающихся на занятии выступают:

- правильность ответов на вопросы преподавателя по изученному материалу;
- полнота и лаконичность ответа;
- степень понимания тематики предмета;
- логика и аргументированность изложения материала;
- приведение примеров, демонстрирующих умение и владение полученными знаниями по темам предмета в раскрытии поставленных вопросов.

4.4.2. Методические материалы, определяющие процедуру оценивания при проведении опроса на практическом занятии

Оценки **"отлично"** заслуживает обучающийся, обнаруживший всестороннее, систематическое и глубокое знание вопроса, умение свободно ориентироваться в теме, усвоивший основную, и знакомый с дополнительной литературой, рекомендованной программой. Как правило, оценка "отлично" выставляется обучающимся, усвоившим взаимосвязь основных понятий в их значении для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании учебно-программного материала;

Оценки **"хорошо"** заслуживает обучающийся, обнаруживший полное знание темы, успешно выполняющий предусмотренные программой задания, усвоивший основную литературу, рекомендованную в программе. Как правило, оценка "хорошо" выставляется обучающимся, показавшим систематический характер знаний по пройденному материалу и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебы и профессиональной деятельности;

Оценки **"удовлетворительно"** заслуживает обучающийся, обнаруживший знание основного материала в объеме, необходимом для дальнейшего усвоения материала и предстоящей работы по профессии, знакомый с основной литературой, рекомендованной программой.

Оценка **"неудовлетворительно"** выставляется обучающемуся, обнаружившему пробелы в знаниях основного материала темы, допустившему принципиальные ошибки в понимании и изложении учебного материала.

5. Методические указания для обучающихся по освоению дисциплины

5.1. Методические указания по вопросам на понимание материала

На занятиях рекомендуется слушать предлагаемый материал, при этом параллельно конспектировать основные положения, поскольку это дает наибольший результат в усвоении материала. Предоставляется возможность задавать вопросы на уточнение понимания темы и принимать участие в ее обсуждении.

Кроме этого, для лучшего освоения материала и систематизации знаний по дисциплине, необходимо постоянно разбирать материалы по конспектам и учебным пособиям. Во время самостоятельной проработки материала особое внимание следует уделять возникшим вопросам, непонятным терминам, спорным точкам зрения. Все такие моменты следует выделить или выписать отдельно для дальнейшего обсуждения на семинарском занятии. В случае необходимости обращаться к преподавателю за консультацией. Полный список литературы по дисциплине приведен в разделе 6 программы.

5.2. Методические указания по подготовке вопросов для самостоятельного изучения к занятиям практического (семинарского) типов

Подготовка обучающегося к практическому занятию осуществляется на основании плана раскрытия темы практического занятия, которое разрабатывается преподавателем на основе рабочей программы и доводится до сведения обучающегося своевременно.

При подготовке к практическому занятию обучающемуся необходимо изучить внимательно основные вопросы темы семинара. Важным условием успешной подготовки к практическому занятию является четкая организация самостоятельной работы студентов по изучению учебной и дополнительной литературы. Умение анализировать и применять для ответов на вопросы и решения задач и заданий полученные знания при самостоятельной подготовке в значительной степени определяет успешность освоения материала по дисциплине и формирование у обучающихся соответствующих компетенций.

Подготовка вопросов для самостоятельного изучения включает: изучение необходимой литературы (обязательной, дополнительной литературы, специальных периодических изданий, Интернет-ресурсов), подготовку конспекта ответа, ответы на вопросы.

При подготовке к практическим занятиям важно:

– использовать достаточно широкий диапазон массива информации, провести обзор литературы и специальных изданий, составить каталог Интернет-ресурсов;

– представить различные подходы, четко и полно определить рассматриваемые понятия, выявить взаимосвязи понятий и явлений, взаимозависимости и связи с другими вопросами;

– грамотно структурировать материал, ясно, четко и логично его излагать, приводить соответствующие примеры из практики, для иллюстрации положений, тезисов и выводов использовать таблицы, схемы, графики, диаграммы.

Вопросы для самостоятельной подготовки к занятиям практического (семинарского) типа указаны в разделе 4.2.

5.3. Методические рекомендации по подготовке к экзамену по дисциплине

Ответ на экзамене предусматривает устный ответ.

При подготовке к экзамену обучающийся обращается к пройденному материалу, сосредоточенному в конспектах, учебниках и других источниках информации. Повторяя, обобщая, закрепляя и дополняя полученные знания, поднимает их на качественно-новый уровень — уровень системы совокупных данных, что позволяет ему понять логику всего предмета в целом. Новые знания обучающийся получает в ходе самостоятельного изучения того, что не было изложено на семинарских занятиях.

Экзамен как особая форма учебного процесса имеет свои особенности, специфические черты и некоторые аспекты, которые необходимо обучающемуся знать и учитывать в своей работе. Это, прежде всего:

• что и как запоминать при подготовке к экзамену;
• по каким источникам и как готовиться;
• на чем сосредоточить основное внимание;
• каким образом в максимальной степени использовать программу курса;

• что и как записать, а что выучить дословно и т. п.

На экзамене, как правило, проверяется не столько уровень запоминания обучающимся учебного материала, сколько то, насколько успешно он оперирует теми или иными понятиями и категориями, систематизирует факты, как умеет мыслить, аргументировано отстаивать определенную позицию, объясняет и пересказывает заученную информацию.

Программу курса необходимо максимально использовать как в ходе подготовки, так и на самом экзамене. Ведь она включает в себя разделы, темы и основные проблемы, в рамках которых и формируются вопросы для экзамена.

Оптимальным для подготовки к экзамену является вариант, когда обучающийся начинает подготовку к нему с первых занятий по данному курсу.

При подготовке к экзамену по наиболее сложным вопросам, ключевым проблемам и важнейшим понятиям необходимо сделать краткие письменные записи в виде тезисов, планов, определений. Особое внимание в ходе подготовки к экзамену следует уделять конспектам лекций, ибо они обладают рядом преимуществ по сравнению с печатной продукцией. Как правило, они более детальные, иллюстрированные, что позволяет оценивать современную ситуацию, отражать самую свежую научную и оперативную информацию, отвечать на вопросы, интересующие аудиторию, в данный момент, тогда как при написании и опубликовании печатной продукции проходит определенное время, и материал быстро устаревает.

В то же время подготовка по одним конспектам недостаточна, необходимо использовать и иную учебную литературу. Не следует бояться дополнительных и уточняющих вопросов на экзамене. Они, как правило, задаются или помимо экзаменационного вопроса для выявления общей подготовленности, или в рамках билета для уточнения высказанной мысли.

5.3.1. Учебно-методическое обеспечение самостоятельной работы

Самостоятельная работа студентом осуществляется для закрепления изученного материала после практических занятий или лабораторных работ, для выполнения домашних заданий, для подготовки к контрольным работам, для изучения дополнительных материалов.

6. Учебная литература и ресурсы информационно- телекоммуникационной сети «Интернет», учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине

6.1. Основная литература

1. Кияев, В. Безопасность информационных систем : курс / В. Кияев, О. Граничин. - Москва : Национальный Открытый Университет «ИНТУИТ», 2019. - 192 с. : ил. ; То же [Электронный ресурс]. - URL:http://biblioclub.ru/index.php?page=book&id=429032.

2. Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара : Самарский государственный архитектурно-строительный университет, 2018. - 113 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-9585-0603-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=438331.

3. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - Москва ; Берлин : Директ-Медиа,

2019. - 253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557.
4. Комплексное обеспечение информационной безопасности автоматизированных систем : лабораторный практикум / авт.-сост. М.А. Лапина, Д.М. Марков, Т.А. Гиш, М.В. Песков и др. - Ставрополь : СКФУ, 2020. - 242 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458012.
5. Кремер, А.С. Обеспечение доверия и безопасности при использовании ИКТ [Текст] : учебное пособие / А. С. Кремер, С. А. Мальянов, А. А. Малюк ; Федер. агентсво связи ; Моск. техн. ун-т связи и информатики. - 2-е изд., доп. - М. : МТУСИ, 2019. - 314 с. : табл.

6.2. Дополнительная литература

1. Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - Санкт-Петербург : Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. - ISBN 978-5-7422-4331-1 ; То же [Электронный ресурс]. – URL : http://biblioclub.ru/index.php?page=book&id=363040.
2. Окинавская хартия глобального информационного общества. 22 июля 2000 г.
3. Гражданский кодекс Российской Федерации. Часть IV.
4. Федеральный закон № 310-ФЗ «О безопасности», 26 декабря 2010 г.
5. «Стратегия национальной безопасности Российской Федерации до 2020 г.». Указ Президента РФ №537 от 12.05.2009
6. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 9 сентября 2000 г. № Пр-1895).
7. Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07. 2006 г. № 149-ФЗ.
8. «О подписании Соглашения о сотрудничестве государств-участников СНГ в области обеспечения информационной безопасности». Расп. Пр. РФ от 28.05.2012 № 856-р «Собрание законодательства РФ», 04.06.2012, № 23, ст. 3058.
9. Федеральный закон № 5485-1 «О государственной тайне», 21 июля 1993 г. (с изм. от 6.10.97 г. и от 11.12.2011 г.), – М.: МВК по ЗГТ, 2011.
10. Федеральный закон № 98-ФЗ «О коммерческой тайне», 29 июля 2004 г.
11. Федеральный закон № 152-ФЗ «О персональных данных», 27 июля 2006 г.
12. Федеральный закон № 69-ФЗ «О пожарной безопасности».
13. Постановление правительства РФ «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в ФОИВ» № 1233 от 03 ноября 1994 г. – М.: МВК по ЗГТ, 1998.
14. Постановление правительства РФ «Об утверждении правил отнесения сведений к различным степеням секретности» № 170 от 20 февраля 1995 г. – М.: МВК по ЗГТ, 1998.
15. Инструкция о порядке допуска должностных лиц и граждан РФ к государственной тайне. Постановление Правительства РФ от 6 февраля 2010 г. № 63
16. Международный стандарт ИСО/МЭК 27001. Первое издание 2005-10-15. Информационные технологии. Методы защиты. Системы менеджмента защиты информации.
17. ГОСТ Р ИСО/МЭК 15408-2002. Методы и средства обеспечения безопасности критерии оценки безопасности информационных технологий (КОБИТ). Части 1, 3-5.
18. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.

6.3. Учебно-методическое обеспечение самостоятельной работы

1. Положение об организации самостоятельной работы студентов федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации» (в редакции приказа РАНХиГС от 01 сентября 2017 г. №02-539) https://www.ranepa.ru/images/docs/prikazy-ranhigs/Pologenie_o_samostoyatelnoi_rabote.pdf

6.4. Нормативные правовые документы

1. Федерального государственный образовательный стандарт высшего образования по направлению подготовки 09.03.03 Прикладная информатика (уровень бакалавриата), утвержденный приказом Минобрнауки России от 19 сентября 2017 г. № 922 (зарегистрирован Министерством юстиции Российской Федерации 12 октября 2017 г. регистрационный номер 48531.

6.5. Интернет-ресурсы

1. ЭБС IPRbooks (www.iprbookshop.ru),
2. ЭБС ZNANIUM.COM (www.znanium.com),
3. ЭБС eLibrary (www.eLibrary.ru),
4. УБД ООО «ИВИС» (www.ebiblioteka.ru),
5. ЭБС «Университетская библиотека онлайн» (www.biblioclub.ru),
6. ЭБС ЮРАЙТ (www.urait.ru),
7. ЭБС ACADEMIA-MOSCOW.RU (www.academia-moscow.ru),
8. ЭБС «Лань» (www. e.lanbook.com).

7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Учебная аудитория для проведения практических занятий и промежуточной аттестации не требуется.

Библиотека (абонемент, читальный и компьютерный залы)

Учебная аудитория для самостоятельной работы студента не требуется**.**

Программное обеспечение:

Microsoft Windows 10 Corporate 1909 (контракт с продавцом АО «Ланит» от 18.10.2019 №117/08-19, до 31.12.2020г.);

Microsoft Office 2019 (контракт с продавцом АО «Ланит» от 18.10.2019 №117/08-19, до 31.12.2020г.);

Google Chrome 76.0.3809.100 (свободная лицензия);

Deductor Academic 5.3.0.88 (свободная лицензия);

Microsoft Project Professional 2019 (контракт с продавцом АО «Ланит» от 18.10.2019 №117/08-19, до 31.12.2020г.).

Project Expert 7 Tutorial (60 уч. мест, сеть) (контракт с продавцом SoftLine от 14.11.2013 №Tr060872);

Vmware Horizon Client 4.3.0.4209 (свободная лицензия);

CA AllFusion R7.2 (контракт с продавцом ООО «Интерфейс ПРОФ» от 27.10.2008 №227/07-08-ИОП, бессрочный);

Oracle VM VirtualBox 6.0.10 (свободная лицензия);

ArgoUML 0.34 (свободная лицензия);

ARIS Express 2.4d (свободная лицензия);

Stata/SE Educational Network Edition Renewal (Stata) (контракт с продавцом АО «СОФТЛАЙН ТРЕЙД» от 25.06.2019 №373100037619000000, до 25.06.2020г.);

PostgreSQL Database 10.9-2 (свободная лицензия);

EViews Academic Base License+ Unlimited Lab License (Eviews) (контракт с продавцом АО «Ланит» от 18.10.2019 №117/08-19, до 31.12.2020г.);

Weka 3.8.3 (свободная лицензия);

Консультант (контракт с продавцом ЗАО «КонсультантПлюс» от 18.06.2009 № б/н).