ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
МИНИСТЕРСТВА СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НАРОДНОГО ХОЗЯЙСТВА ИМЕНИ В.И. ВЕРНАДСКОГО»
(Университет Вернадского)

Кафедра электрооборудования и электротехнических систем

Принято Ученым советом
Университета Вернадского
«30» августа 2023 г., протокол №1

«УТВЕРЖДЕНО»
Проректор по образовательной деятельности
_____ Кудрявцев М.Г.
«30» августа 2023 г.

Рабочая программа дисциплины

Информационная безопасность и защита информации

Направление подготовки: 09.03.03 Прикладная информатика

Направленность (профиль) программы: Информационные и электротехнические системы в АПК
Квалификация бакалавр

Форма обучения **очная, очно-заочная, заочная**

Балашиха 2023 г.

Рабочая программа разработана в соответствии с ФГОС ВО по направлению подготовки .
Рабочая программа дисциплины разработана *доцентом*
кафедры *электрооборудования и электротехнических систем*, *кандидатом экономическиxx наук, Сидоровым А.В.*

Рецензенты:
- О.А. Липа, к.т.н., доцент кафедры электрооборудования и электротехнических систем ФГБОУ ВО РГАЗУ

1 Планируемые результаты обучения по дисциплине, соотнесенные с установленными в ОПОП ВО индикаторами достижения компетенций

1.1 Перечень компетенций, формируемых учебной дисциплиной

Код и наименование компетенции	Индикаторы достижения компетенций Планируемые результаты обучения
Универсальная компетенция	
ПК-1 Способен выполнять и управлять работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	**Знать (З):** процесс согласования и утверждения требований к типовой ИС; основы инженерно-технической поддержки подготовки коммерческого предложения заказчику на создание (модификацию) и ввод в эксплуатацию типовой ИС на этапе предконтрактных работ; модульное тестирование ИС (верификация); процесс интеграции ИС с существующими ИС заказчика; процесс планирования коммуникаций с заказчиком в рамках типовых регламентов организации; процесс проведения приемо-сдаточных испытаний (валидации) ИС в соответствии с установленными регламентами.
	Уметь (У): определить первоначальные требования заказчика к ИС и возможности их реализации в типовой ИС на этапе предконтрактных работ; исправлять дефекты и несоответствий в коде ИС и документации к ИС; идентифицировать конфигурацию ИС в соответствии с регламентами организации.
	Владеть (В): интеграционного тестирование ИС; настройки оборудования, необходимого для работы ИС; адаптации бизнес-процессов заказчика к возможностям типовой ИС; выявления требований к типовой ИС; разработки прототипов ИС на базе типовой ИС; кодирования на языках программирования; создания пользовательской документации к модифицированным элементам типовой ИС; установки и настройка системного и прикладного по, необходимого для функционирования ИС; проведения аудитов качества в соответствии с планами проведения аудита.

2. Цели и задачи освоения учебной дисциплины, место дисциплины в структуре ОПОП ВО

Дисциплина «Информационная безопасность и защита информации» относится к вариативной части ОПОП ВО.

Целью изучения дисциплины является ознакомление обучающихся с особенностями обеспечения информационной безопасности в среде операционной системы Linux.

Задачами изучения являются:

- овладение теоретическими, практическими и методическими вопросами информационной безопасности и защиты информации;
- ознакомление с программными средствами операционной системы Linux;
- расширение мировоззренческого кругозора.

3. Объем учебной дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий, текущий и промежуточный контроль по дисциплине) и на самостоятельную работу обучающихся

3.1 Очная форма обучения

Вид учебной работы	6 семестр
Общая трудоемкость дисциплины, зачетных единиц	144
часов	
Аудиторная (контактная) работа, часов	**48,3**
в т.ч. занятия лекционного типа	16
занятия семинарского типа	32
промежуточная аттестация	0,3
Самостоятельная работа обучающихся, часов	**86,7**
в т.ч. курсовая работа	-
Контроль	**9**
Вид промежуточной аттестации	экзамен

3.2 Очно-заочная форма обучения

Вид учебной работы	8 семестр
Общая трудоемкость дисциплины, зачетных единиц	144
часов	
Аудиторная (контактная) работа, часов	**24,3**
в т.ч. занятия лекционного типа	8
занятия семинарского типа	16
промежуточная аттестация	0,3
Самостоятельная работа обучающихся, часов	**110,7**
в т.ч. курсовая работа	-
Контроль	**9**
Вид промежуточной аттестации	экзамен

3.3 Заочная форма обучения

Вид учебной работы	8 семестр
Общая трудоемкость дисциплины, зачетных единиц	144
часов	
Аудиторная (контактная) работа, часов	**14,3**
в т.ч. занятия лекционного типа	6
занятия семинарского типа	8
промежуточная аттестация	0,3
Самостоятельная работа обучающихся, часов	**120,7**
в т.ч. курсовая работа	-
Контроль	**9**
Вид промежуточной аттестации	экзамен

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Перечень разделов дисциплины с указанием трудоемкости аудиторной (контактной) и самостоятельной работы, видов контролей и перечня компетенций

Очная форма обучения

Наименование разделов и тем	Трудоемкость, часов			Наименование оценочного средства	Код компетенции
	всего	в том числе			
		аудиторной (контактной) работы	самостоятельной работы		
				Практические задания	ПК-1
РАЗДЕЛ 1. СОДЕРЖАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.	**44**	**14**	**30**		
Тема 1.1. Понятие «информационная безопасность»	5	1	4		
Тема 1.2. Общая схема информационной безопасности	6	2	4		
Тема 1.3. Содержание информационной безопасности	6	2	4		
Тема 1.4. Составляющие информационной безопасности	6	2	4		
Тема 1.5. Задачи информационной безопасности общества	6	2	4		
Тема 1.6. Уровни формирования информационной безопасности	8	2	6		
Тема 1.7. Нормативно-правовые основы информационной безопасности в РФ	6	2	4		
Тема 1.8. Стандарты информационной безопасности	5	1	4		
РАЗДЕЛ 2. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И СПОСОБЫ ПРОТИВОДЕЙСТВИЯ	**38,7**	**10**	**28,7**		
Тема 2.1. Виды угроз информационной безопасности.	5	1	4		
Тема 2.2. Модель нарушителя информационной безопасности.	5	1	4		
Тема 2.3. Принципы построения системы защиты	5	1	4		

информации.					
Тема 2.4. Методы защиты информации.	9,7	1	8,7		
Тема 2.5. Повышение надежности информационной системы	6	2	4		
Тема 2.6. Методы и средства защиты информации от шпионажа и несанкционированного доступа	6	2	4		
РАЗДЕЛ 3. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ	**44**	**14**	**30**		
Тема 3.1. Компьютерные вирусы и информационная безопасность.	5	1	4		
Тема 3.2. Классификация компьютерных вирусов.	6	2	4		
Тема 3.3. Антивирусные программы.	6	2	4		
Тема 3.4. Особенности безопасности компьютерных сетей.	6	2	4		
Тема 3.5. Классификация удаленных угроз в компьютерных сетях.	6	2	4		
Тема 3.6. Причины успешной реализации удаленных угроз в компьютерных сетях.	8	2	6		
Тема 3.7. Механизмы безопасности компьютерных сетей.	6	2	4		
Тема 3.8. Криптография и шифрование.	5	1	4		
Промежуточная аттестация	9	0,3		Итоговое тестирование	
ИТОГО по дисциплине	**144**	**48,3**	**86,7**		

Очно-заочная форма обучения

Наименование разделов и тем	Трудоемкость, часов			Наименование оценочного средства	Код компетенции
	всего	в том числе			
		аудиторной (контактной) работы	самостоятельной работы		
				Практические задания	ПК-1
РАЗДЕЛ 1. СОДЕРЖАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.	**53**	**8**	**45**		

Тема 1.1. Понятие «информационная безопасность»	6	1	5		
Тема 1.2. Общая схема информационной безопасности	6	1	5		
Тема 1.3. Содержание информационной безопасности	6	1	5		
Тема 1.4. Составляющие информационной безопасности	6	1	5		
Тема 1.5. Задачи информационной безопасности общества	6	1	5		
Тема 1.6. Уровни формирования информационной безопасности	11	1	10		
Тема 1.7. Нормативно-правовые основы информационной безопасности в РФ	6	1	5		
Тема 1.8. Стандарты информационной безопасности	6	1	5		
РАЗДЕЛ 2. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И СПОСОБЫ ПРОТИВОДЕЙСТВИЯ	**28,7**	**8**	**20,7**		
Тема 2.1. Виды угроз информационной безопасности.	4	1	3		
Тема 2.2. Модель нарушителя информационной безопасности.	4	1	3		
Тема 2.3. Принципы построения системы защиты информации.	4	1	3		
Тема 2.4. Методы защиты информации.	6,7	1	5,7		
Тема 2.5. Повышение надежности информационной системы.	5	2	3		
Тема 2.6. Методы и средства защиты информации от шпионажа и несанкционированного доступа.	5	2	3		
РАЗДЕЛ 3. ИНФОРМАЦИОННАЯ	**53**	**8**	**45**		

БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ					
Тема 3.1. Компьютерные вирусы и информационная безопасность.	11	1	10		
Тема 3.2. Классификация компьютерных вирусов.	6	1	5		
Тема 3.3. Антивирусные программы.	6	1	5		
Тема 3.4. Особенности безопасности компьютерных сетей.	6	1	5		
Тема 3.5. Классификация удаленных угроз в компьютерных сетях.	6	1	5		
Тема 3.6. Причины успешной реализации удаленных угроз в компьютерных сетях.	6	1	5		
Тема 3.7. Механизмы безопасности компьютерных сетей.	6	1	5		
Тема 3.8. Криптография и шифрование.	6	1	5		
Промежуточная аттестация	9	0,3		Итоговое тестирование	
ИТОГО по дисциплине	**144**	**24,3**	**110,7**		

Заочная форма обучения

Наименование разделов и тем	Трудоемкость, часов			Наименование оценочного средства	Код компетенции
	всего	в том числе			
		аудиторной (контактной) работы	самостоятельной работы		
				Практические задания	ПК-1
РАЗДЕЛ 1. СОДЕРЖАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.	**45**	**5**	**40**		
Тема 1.1. Понятие «информационная безопасность»	5,5	0,5	5		
Тема 1.2. Общая схема информационной безопасности	5,5	0,5	5		
Тема 1.3. Содержание информационной безопасности	5,5	0,5	5		
Тема 1.4. Составляющие информационной безопасности	5,5	0,5	5		
Тема 1.5. Задачи информационной	5,5	0,5	5		

безопасности общества					
Тема 1.6. Уровни формирования информационной безопасности	5,5	0,5	5		
Тема 1.7. Нормативно-правовые основы информационной безопасности в РФ	6	1	5		
Тема 1.8. Стандарты информационной безопасности	6	1	5		
РАЗДЕЛ 2. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И СПОСОБЫ ПРОТИВОДЕЙСТВИЯ	**44,7**	**4**	**40,7**		
Тема 2.1. Виды угроз информационной безопасности.	6	1	5		
Тема 2.2. Модель нарушителя информационной безопасности.	6	1	5		
Тема 2.3. Принципы построения системы защиты информации.	6	1	5		
Тема 2.4. Методы защиты информации.	11,7	1	10,7		
Тема 2.5. Повышение надежности информационной системы	7	2	5		
Тема 2.6. Методы и средства защиты информации от шпионажа и несанкционированного доступа	12	2	10		
РАЗДЕЛ 3. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ	**45**	**5**	**40**		
Тема 3.1. Компьютерные вирусы и информационная безопасность.	10,5	0,5	10		
Тема 3.2. Классификация компьютерных вирусов.	5,5	0,5	5		
Тема 3.3. Антивирусные программы.	5,5	0,5	5		
Тема 3.4. Особенности безопасности компьютерных сетей.	5,5	0,5	5		

Тема 3.5. Классификация удаленных угроз в компьютерных сетях.	5,5	0,5	5		
Тема 3.6. Причины успешной реализации удаленных угроз в компьютерных сетях.	5,5	0,5	5		
Тема 3.7. Механизмы безопасности компьютерных сетей.	6	1	5		
Тема 3.8. Криптография и шифрование.	6	1	5		
Промежуточная аттестация	9	0,3		Итоговое тестирование	
ИТОГО по дисциплине	**144**	**14,3**	**120,7**		

Примерный перечень оценочных средств для текущего контроля успеваемости

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1	практическое задание	Средство оценки умения применять полученные теоретические знания в практической ситуации. Задача (задание) должна быть направлена на оценивание тех компетенций, которые подлежат освоению в данной дисциплине, должна содержать четкую инструкцию по выполнению или алгоритм действий.	Комплект задач и заданий
2	Тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Фонд тестовых заданий

4.2 Содержание дисциплины по темам

РАЗДЕЛ 1. СОДЕРЖАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Цели: приобретение теоретических знаний об основах информационной безопасности.

Задачи:

- изучение теоретического материала;
- анализ результатов по исследуемой тематике.

Перечень учебных элементов раздела:

Тема 1.1. Понятие «информационная безопасность».

информационная безопасность. Задачи по информационной безопасности. Информационная безопасность и "компьютерная безопасность".

Тема 1.2. Общая схема информационной безопасности

Проблемы обеспечения информационной безопасности. Схема обеспечения информационной безопасности.

Тема 1.3. Содержание информационной безопасности.

Действия для обеспечения информационной безопасности. Обнаружение угроз. Общие признаки защиты охраняемой информации. Основные цели защиты информации.

Тема 1.4. Составляющие информационной безопасности.

Три задачи решаемые в рамках обеспечения информационной безопасности. Доступность, целостность и конфиденциальность информации.

Тема 1.5. Задачи информационной безопасности общества.

Доктрина информационной безопасности. Четыре основные составляющие национальных интересов РФ в информационной сфере. методы обеспечения информационной безопасности РФ.

Тема 1.6. Уровни формирования информационной безопасности.

Три уровня формирования режима информационной безопасности. Шаги при определении политики информационной безопасности. Процедурный и программно-технический уровень программы безопасности.

Тема 1.7. Нормативно-правовые основы информационной безопасности в РФ.

Законодательные меры в сфере информационной безопасности. Основные задачи системы защиты информации.

Тема 1.8. Стандарты информационной безопасности.

Стандарт ISO/IEC 15408. Классы требований доверия безопасности. Рекомендации X.800. Руководящие документы – стандарты информационной безопасности.

РАЗДЕЛ 2. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И СПОСОБЫ ПРОТИВОДЕЙСТВИЯ

Цели: приобретение знаний об угрозах информационной безопасности и способах противодействия.

Задачи:

- изучение теоретического материала;
- анализ результатов по исследуемой тематике.

Тема 2.1. Виды угроз информационной безопасности.

Угроза информационной безопасности. Классификация угроз информационной безопасности. Непреднамеренные и преднамеренные угрозы. Несанкционированный доступ (НСД). Каналы НСД. Система разграничения доступа.

Тема 2.2. Модель нарушителя информационной безопасности.

Нарушитель. Модель нарушителя. Классификация нарушителей.

Тема 2.3. Принципы построения системы защиты информации.

Принципы защиты информации. Прикладной уровень защиты информации. Защита информации.

Тема 2.4. Методы защиты информации.

Дублирование информации.

Тема 2.5. Повышение надежности информационной системы.

Понятие надежности. Направления повышения надежности программных средств. Три подхода к созданию отказоустойчивых систем. Избыточность. Помехоустойчивость.

Тема 2.6. Методы и средства защиты информации от шпионажа и несанкционированного доступа.

Задачи защиты объектов информационных ресурсов от угроз шпионажа. Система защиты от исследования и копирования информации. Два подхода к организации разграничения доступа к информационной системе. Методы криптографического преобразования информации.

РАЗДЕЛ 3. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ.

Цели: приобретение знаний и навыков в области обеспечения безопасности компьютерных систем и сетей.

Задачи:

- изучение теоретического материала;
- анализ результатов по исследуемой тематике.

Тема 3.1. Компьютерные вирусы и информационная безопасность.

Понятие о компьютерных вирусах. Программный вирус – определение. Внешние признаки проявления деятельности вируса. Пути проникновения вирусов на компьютер.

Тема 3.2. Классификация компьютерных вирусов.

Классификация компьютерных вирусов. Утилиты скрытого администрирования.

Тема 3.3. Антивирусные программы.

Понятие антивирусной программы. Виды антивирусных программ. Наиболее популярные сегодня антивирусные решения.

Тема 3.4. Особенности безопасности компьютерных сетей.

Удаленная угроза. Использование технологии клиент/сервер с точки зрения информационной безопасности.

Тема 3.5. Классификация удаленных угроз в компьютерных сетях.

Классификация удаленных угроз. Удаленные атаки.

Тема 3.6. Причины успешной реализации удаленных угроз в компьютерных сетях.

Отсутствие выделенного канала связи между объектами вычислительной сети. Недостаточная идентификация объектов и субъектов сети. Взаимодействие объектов без установления виртуального канала. Отсутствие в распределенных вычислительных сетях возможности контроля за маршрутом сообщений. Отсутствие в распределенных вычислительных сетях полной информации об ее объектах. Отсутствие в распределенных вычислительных сетях криптозащиты сообщений. Отсутствие контроля за маршрутом сообщения в сети. Контроль за виртуальным соединением.

Тема 3.7. Механизмы безопасности компьютерных сетей.

Идентификация и аутентификация. Три категории аутентификации.

Тема 3.8. Криптография и шифрование.

Понятие криптосистемы. Два класса систем шифрования. Типы классических криптографических методов шифрования. Понятие электронно-цифровой подписи. Дискретное управление доступом. Мандатное управление доступом.

5. Оценочные материалы по дисциплине

Оценочные материалы по дисциплине представлены в виде фонда оценочных средств.

6. Материально-техническое и учебно-методическое обеспечение дисциплины

6.1 Перечень учебно-методического обеспечения по дисциплине

№ п/п	Автор, название, место издания, издательство, год издания, количество страниц, режим доступа
1	Методические указания по изучению дисциплины и задания для лабораторно-практических занятий

6.2 Перечень учебных изданий, необходимых для освоения дисциплины

Электронные учебные издания в электронно-библиотечных системах (ЭБС):

№ п/п	Автор, название, место издания, год издания, количество страниц	Ссылка на учебное издание в ЭБС
Основная:		
1	Капустин, Д.А. Информационно-вычислительные сети [Электронный ресурс]: учеб. пособие / Д.А.Капустин, В.Е. Дементьев /Ульяновск: Ульяновский ГТУ, 2011. - 141 с.	Электронно-библиотечная система «AgriLib»: сайт – Балашиха, 2011. URL: http://ebs.rgazu.ru/?q=node/3525.
2	Платунова, С.М. Администрирование вычислительных сетей на базе MS Winsows Server® 2008 [Электронный ресурс]: учеб. пособие / С.М. Платунова /СПб.: СПбГУ ИТМО, 2012. - 41 с.	Электронно-библиотечная система «AgriLib»: сайт – Балашиха, 2012. URL: http://ebs.rgazu.ru/?q=node/3169.
Дополнительная		
1	Пользовательская документация	http://help.ubuntu.ru
2	Документация по ОС Linux	https://linuxcookbook.ru

3	Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 года № Пр-1895.	
4	Мельников, В.П. Информационная безопасность и защита информации: учеб. пособие для студентов высших учебных заведений / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под. ред. С.А. Клейменова. – М.: Издательский центр «Академия», 2009. – 336 с.	

*6.3 Перечень электронных образовательных ресурсов **

№ п/п	Электронный образовательный ресурс	Доступ в ЭОР (сеть Интернет, локальная сеть, авторизованный/свободный доступ
1	Учебник по администрированию Linux	https://coderlessons.com/tutorials/devops/izuchite-linux-admin/uchebnik-po-administrirovaniiu-linux

6.4 Современные профессиональные базы данных, информационные справочные системы и лицензионное программное обеспечение

Современные профессиональные базы данных, информационные справочные системы, цифровые электронные библиотеки и другие электронные образовательные ресурсы

1. Договор о подключении к Национальной электронной библиотеке и предоставлении доступа к объектам Национальной электронной библиотеки №101/НЭБ/0502-п от 26.02.2020 5 лет с пролонгацией
2. Соглашение о бесплатном тестовом доступе к Polpred.com. Обзор СМИ 27.04.2016 бессрочно
3. Соглашение о бесплатном тестовом доступе к Polpred.com. Обзор СМИ 02.03.2020 бессрочно
4. Информационно-справочная система «Гарант» – URL: https://www.garant.ru/ Информационно-справочная система Лицензионный договор № 261709/ОП-2 от 25.06.2021
5. «Консультант Плюс». – URL: http://www.consultant.ru/ свободный доступ
6. Электронно-библиотечная система AgriLib http://ebs.rgazu.ru/ (свидетельство о государственной регистрации базы данных №2014620472 от 21.03.2014).

Доступ к электронной информационно-образовательной среде, информационно-телекоммуникационной сети «Интернет»

1. Система дистанционного обучения Moodle www.portfolio.rgazu.ru (свободно распространяемое)
2. Право использования программ для ЭВМ Mirapolis HCM в составе функциональных блоков и модулей: Виртуальная комната. Стандартная лицензия до 1000 пользователей на 1 месяц (Лицензионный договор № 77/03/22 – К от 25 апреля 2022)
3. Инновационная система тестирования – программное обеспечение на платформе 1С (Договор № К/06/03 от 13.06.2017)
4. Образовательный интернет – портал Российского государственного аграрного заочного университета (свидетельство о регистрации средства массовых информации Эл № ФС77-51402 от 19.10.2012).

Лицензионное и свободно распространяемое программное обеспечение

1. OpenOffice – свободный пакет офисных приложений (свободно

распространяемое)

2. linuxmint.com https://linuxmint.com/ (свободно распространяемое)

3. Электронно-библиотечная система AgriLib http://ebs.rgazu.ru/ (свидетельство о государственной регистрации базы данных №2014620472 от 21.03.2014)

4. Официальная страница ФГБОУ ВО «Российский государственный аграрный заочный университет» https://vk.com/rgazuru (свободно распространяемое)

5. Портал Федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный аграрный заочный университет» (свободно распространяемое) https://zen.yandex.ru/id/5fd0b44cc8ed19418871dc31

6. Антивирусное программное обеспечение Dr. WEB Desktop Security Suite (Сублицензионный договор №13740 на передачу неисключительных прав на программы для ЭВМ от 01.07.2021).

6.5 Перечень учебных аудиторий, оборудования и технических средств обучения

Предназначение помещения (аудитории)	**Наименование корпуса, № помещения (аудитории)**	**Перечень оборудования (в т.ч. виртуальные аналоги) и технических средств обучения***
Учебная аудитория для занятий лекционного типа, семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы), для проведения групповых консультаций и индивидуальной работы обучавшихся с педагогическими работниками, для проведения текущего контроля и промежуточной аттестации	Учебно-административный корпус. Каб. 412, 320	Специализированная мебель, доска меловая. Персональные компьютеры в сборке с выходом в интернет
Помещение для самостоятельной работы	Учебно-административный корпус. Читальный зал № ТИ 177	Персональные компьютеры в сборке с выходом в интернет.

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
МИНИСТЕРСТВА СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НАРОДНОГО ХОЗЯЙСТВА ИМЕНИ В.И. ВЕРНАДСКОГО»
(Университет Вернадского)

Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине

Информационная безопасность и защита информации

Направление подготовки: 09.03.03 Прикладная информатика

Направленность (профиль) программы: Информационные и электротехнические системы в АПК
Квалификация бакалавр

Форма обучения **заочная, очно-заочная, очная**

Балашиха 2023г.

1.Описание показателей и критериев оценивания планируемых результатов обучения по учебной дисциплине

Компетенций	Уровень освоения*	Планируемые результаты обучения	Наименование оценочного средства
ПК-1 Способен выполнять и управлять работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	**Пороговый (удовлетворительно)**	**Знает:** процесс согласования и утверждения требований к типовой ИС; основы инженерно-технической поддержки подготовки коммерческого предложения заказчику на создание (модификацию) и ввод в эксплуатацию типовой ИС на этапе предконтрактных работ; модульное тестирование ИС (верификация); процесс интеграции ИС с существующими ИС заказчика; процесс планирования коммуникаций с заказчиком в рамках типовых регламентов организации; процесс проведения приемо-сдаточных испытаний (валидации) ИС в соответствии с установленными регламентами. **Умеет:** определить первоначальные требования заказчика к ИС и возможности их реализации в типовой ИС на этапе предконтрактных работ; исправлять дефекты и несоответствий в коде ИС и документации к ИС; идентифицировать конфигурацию ИС в соответствии с регламентами организации. **Владеет:** интеграционного тестирование ИС; настройки оборудования, необходимого для работы ИС; адаптации бизнес-процессов заказчика к возможностям типовой ИС; выявления требований к типовой ИС; разработки прототипов ИС на базе типовой ИС; кодирования на языках программирования; создания пользовательской документации к модифицированным элементам типовой ИС; установки и настройка системного и прикладного по, необходимого для функционирования ИС; проведения аудитов качества в соответствии с планами проведения аудита.	Выполнение практического задания Итоговое тестирование
	Продвинутый (хорошо)	**Твердо знает:** процесс согласования и утверждения требований к типовой ИС; основы инженерно-технической	Выполнение практического задания

		поддержки подготовки коммерческого предложения заказчику на создание (модификацию) и ввод в эксплуатацию типовой ИС на этапе предконтрактных работ; модульное тестирование ИС (верификация); процесс интеграции ИС с существующими ИС заказчика; процесс планирования коммуникаций с заказчиком в рамках типовых регламентов организации; процесс проведения приемо-сдаточных испытаний (валидации) ИС в соответствии с установленными регламентами. **Уверенно умеет:** определить первоначальные требования заказчика к ИС и возможности их реализации в типовой ИС на этапе предконтрактных работ; исправлять дефекты и несоответствий в коде ИС и документации к ИС; идентифицировать конфигурацию ИС в соответствии с регламентами организации. **Уверенно владеет:** интеграционного тестирование ИС; настройки оборудования, необходимого для работы ИС; адаптации бизнес-процессов заказчика к возможностям типовой ИС; выявления требований к типовой ИС; разработки прототипов ИС на базе типовой ИС; кодирования на языках программирования; создания пользовательской документации к модифицированным элементам типовой ИС; установки и настройка системного и прикладного по, необходимого для функционирования ИС; проведения аудитов качества в соответствии с планами проведения аудита.	Итоговое тестирование
	Высокий (отлично)	**Сформировавшееся систематическое знание:** процесс согласования и утверждения требований к типовой ИС; основы инженерно-технической поддержки подготовки коммерческого предложения заказчику на создание (модификацию) и ввод в эксплуатацию типовой ИС на этапе предконтрактных работ; модульное тестирование ИС (верификация);	Выполнение практического задания Итоговое тестирование

		процесс интеграции ИС с существующими ИС заказчика; процесс планирования коммуникаций с заказчиком в рамках типовых регламентов организации; процесс проведения приемо-сдаточных испытаний (валидации) ИС в соответствии с установленными регламентами. **Сформировавшееся систематическое умение:** определить первоначальные требования заказчика к ИС и возможности их реализации в типовой ИС на этапе предконтрактных работ; исправлять дефекты и несоответствий в коде ИС и документации к ИС; идентифицировать конфигурацию ИС в соответствии с регламентами организации. **Сформировавшееся систематическое владение:** интеграционного тестирование ИС; настройки оборудования, необходимого для работы ИС; адаптации бизнес-процессов заказчика к возможностям типовой ИС; выявления требований к типовой ИС; разработки прототипов ИС на базе типовой ИС; кодирования на языках программирования; создания пользовательской документации к модифицированным элементам типовой ИС; установки и настройка системного и прикладного по, необходимого для функционирования ИС; проведения аудитов качества в соответствии с планами проведения аудита.	

2. Описание шкал оценивания

2.1 Шкала оценивания на этапе текущего контроля

* Студенты, показавшие уровень усвоения ниже порогового, не допускаются к промежуточной аттестации по дисциплине.

Форма текущего контроля	Отсутствие усвоения (ниже порогового)*	Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
Выполнение практического задания	не выполнена или все задания решены неправильно	Решено более 50% задания, но менее 70%	Решено более 70% задания, но есть ошибки	все задания решены без ошибок
Тест	Менее 51%	51-79%	80-90%	91% и более

2.2 Шкала оценивания на этапе промежуточной аттестации (зачет и экзамен в виде итогового теста, курсовая работа)

Форма промежуточной аттестации	**Отсутствие усвоения (ниже порогового)**	**Пороговый (удовлетворительно)**	**Продвинутый (хорошо)**	**Высокий (отлично)**
Выполнение итоговых тестов (не менее 15 вопросов на вариант)	Менее 51%	51-79%	80-90%	91% и более

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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

Лабораторно-практическая работа. Изучение основ обеспечения информационной безопасности в среде ОС Linux.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

КОМПЛЕКТ ТЕСТОВ для промежуточной аттестации (экзамен) по дисциплине Информационная безопасность и защита информации

Зачет проводится в виде Тестирования (Итоговый тест). Для выполнения теста отводится 45 минут.

Примерные задания Тест
Примеры тестовых заданий, выполненных в программе «GIFT»:

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

Разработка аппаратных средств обеспечения правовых данных

Разработка и установка во всех компьютерных правовых сетях журналов учета действий

Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:

Хищение жестких дисков, подключение к сети, инсайдерство

Перехват данных, хищение данных, изменение архитектуры системы

Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:

Персональная, корпоративная, государственная

Клиентская, серверная, сетевая

Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:

несанкционированного доступа, воздействия в сети

инсайдерства в организации

чрезвычайных ситуаций

5) Основные объекты информационной безопасности:

Компьютерные сети, базы данных

Информационные системы, психологическое состояние пользователей

Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:

Искажение, уменьшение объема, перекодировка информации

Техническое вмешательство, выведение из строя оборудования сети

Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:

Экономической эффективности системы безопасности

Многоплатформенной реализации системы

Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:

руководители, менеджеры, администраторы компаний

органы права, государства, бизнеса

сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:

Установление регламента, аудит системы, выявление рисков

Установка новых офисных приложений, смена хостинг-компании

Внедрение аутентификации, проверки контактных данных пользователей

10) Принципом информационной безопасности является принцип недопущения:

Неоправданных ограничений при работе в сети (системе)

Рисков безопасности сети, системы

Презумпции секретности

11) Принципом политики информационной безопасности является принцип:

Невозможности миновать защитные средства сети (системы)

Усиления основного звена сети, системы

Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:

Усиления защищенности самого незащищенного звена сети (системы)

Перехода в безопасное состояние работы сети, системы

Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:

Разделения доступа (обязанностей, привилегий) клиентам сети (системы)

Одноуровневой защиты сети, системы

Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:

Компьютерный сбой

Логические закладки («мины»)

Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:

Прочитать приложение, если оно не содержит ничего ценного – удалить

Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама

Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:

Секретность ключа определена секретностью открытого сообщения

Секретность информации определена скоростью передачи данных

Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:

Электронно-цифровой преобразователь

Электронно-цифровая подпись

Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:

Покупка нелицензионного ПО

Ошибки эксплуатации и неумышленного изменения режима работы системы

Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:

Распределенный доступ клиент, отказ оборудования

Моральный износ сети, инсайдерство

Сбой (отказ) оборудования, нелегальное копирование данных

20) Наиболее распространены средства воздействия на сеть офиса:

Слабый трафик, информационный обман, вирусы в интернет

Вирусы в сети, логические мины (закладки), информационный перехват

Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:

Потерей данных в системе

Изменением формы информации

Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

Целостность

Доступность

Актуальностьl

23) Угроза информационной системе (компьютерной сети) – это:

Вероятное событие

Детерминированное (всегда определенное) событие

Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

Регламентированной

Правовой

Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:

Программные, технические, организационные, технологические

Серверные, клиентские, спутниковые, наземные

Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:

Владелец сети

Администратор сети

Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:

Руководств, требований обеспечения необходимого уровня безопасности

Инструкций, алгоритмов поведения пользователя в сети

Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:

Аудит, анализ затрат на проведение защитных мер

Аудит, анализ безопасности

Аудит, анализ уязвимостей, риск-ситуаций