МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»
(БГТУ им. В.Г. Шухова)

УТВЕРЖДАЮ
Директор института
«20» 05 2021 г.

РАБОЧАЯ ПРОГРАММА
дисциплины

Безопасность программно-информационных систем
направление подготовки:

09.03.04 «Программная инженерия»

Направленность программы (профиль):

Разработка программно-информационных систем

Квалификация

Бакалавр

Форма обучения

Очная

Институт энергетики, информационных технологий и управляющих систем

Кафедра программного обеспечения вычислительной техники и автоматизированных систем

Белгород 2021

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 09.03.04 «Программная инженерия», утвержденного приказа Минобрнауки России от 19.09.2017 № 920
- учебного плана, утвержденного ученым советом БГТУ им. В.Г. Шухова в 2021 году.

Составитель: _____ (Бондаренко Т.В.)
(ученая степень и звание, подпись) (инициалы, фамилия)

к.т.н., доцент _____ (Гаврющенко А.П.)
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа обсуждена на заседании кафедры

«14» 05 2021 г., протокол № 8

Заведующий кафедрой: к.т.н., доцент _____ (Поляков В.М.)
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа согласована с выпускающей кафедрой программного обеспечения вычислительной техники и автоматизированных систем
(наименование кафедры/кафедр)

Заведующий кафедрой: к.т.н., доцент _____ (Поляков В.М.)
(ученая степень и звание, подпись) (инициалы, фамилия)

«14» 05 2021 г.

Рабочая программа одобрена методической комиссией института

«20» 05 2021 г., протокол № 9

Председатель к.т.н., доцент _____ (Семернин А.Н.)
(ученая степень и звание, подпись) (инициалы, фамилия)

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Категория (группа) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Наименование показателя оценивания результата обучения по дисциплине
Разработка програм много обеспечения	ПК-2. Способен использовать различные технологии разработки программного обеспечения автоматизированны х систем	ПК-2.1 Анализирует и выбирает необходимую технологию разработки программного обеспечения для решения профессиональных задач	Знания
		ПК-2.2 Использует современные технологии разработки программного обеспечения для решения прикладных задач	Умения
		ПК-2.3 Использует необходимые стандарты и модели жизненного цикла программного обеспечения при разработке и реализации программного обеспечения	Знания Умения
		ПК-2.4 Применяет языки программирования различного уровня для написания компонентов программных продуктов	Знания Навыки
		ПК-2.5 Понимает формальные методы конструирования программного обеспечения	Знания Умения
		ПК-2.6 Использует методы. инструменты и технологии обеспечения качества программного обеспечения	Умения Навыки

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1. Компетенция ПК-2. Способен разрабатывать программное обеспечение для встраиваемых программно-аппаратных платформ

Данная компетенция формируется следующими дисциплинами.

Стадия	Наименования дисциплины
1.	Архитектура вычислительных систем
2.	Алгоритмы и структуры данных
3.	Объектно-ориентированное программирование
4.	Компьютерная графика
5.	Методы анализа данных
6.	Теория информации
7.	Технологии Web-программирования
8.	Проектирование клиент-серверных приложений
9.	Параллельное программирование
10.	Программирование микроконтроллеров
11.	Основы искусственного интеллекта
12.	Безопасность программно-информационных систем
13.	Теория автоматов и формальных языков
14.	Основы построения трансляторов
15.	Системы и среды программирования
16.	Программирование на языке Python
17.	Производственная преддипломная практика

3. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 5 зач. единиц, 180 часа.

Дисциплина реализуется в рамках практической подготовки: 3 зач. единиц.

Форма промежуточной аттестации *экзамен*

Вид учебной работы	Всего часов	Семестр № 7
Общая трудоемкость дисциплины, час	180	180
Контактная работа (аудиторные занятия), в т.ч.:	73	73
лекции	34	34
лабораторные	34	34
практические	-	-
групповые консультации в период теоретического обучения и промежуточной аттестации	5	5
Самостоятельная работа студентов, включая индивидуальные и групповые консультации, в том числе:	112	112
Курсовой проект	—	—
Курсовая работа	—	—
Расчетно-графическое задание	—	—
Индивидуальное домашнее задание		
Самостоятельная работа на подготовку к аудиторным занятиям (лекции, практические занятия, лабораторные занятия)	71	71
Экзамен	36	36

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ
4.1 Наименование тем, их содержание и объем
Курс 4 Семестр 7

№ п/п	Наименование раздела (краткое содержание)	Объем на тематический раздел по видам учебной нагрузки, час			
		Лекции	Практические занятия	Лабораторные занятия	Самостоятельная работа на подготовку к аудиторным занятиям
1.	Программно-информационные системы: основные понятия				
	Класификация программно-информационных систем. Общие вопросы оценки безопасности компьютерных систем.	6		6	12
2.	Программно-информационные системы: средства обеспечения безопасности				
	Комплексные средства обеспечения информационных объектов. Классификация программных, аппаратных и гибридных методов и средств обеспечения информационной безопасности.	6		6	12
3.	Средства контроля доступа к информационным объектам				
	Системы аутентификации, авторизации; межсетевой, межпрограммный уровень взаимодействия систем обеспечения безопасности; средства контроля доступа, системы разграничения доступа к ресурсам	6		6	12
4.	Безопасность информационных систем и сетей				
	Безопасность информационных систем локальных, городских глобальных информационных вычислительных сетей. Проектирование и управление системами обеспечения информационной безопасности в вычислительных сетях различного уровня.	5		5	12
5.	Протоколы авторизации, аутентификации и проверки подлинности				
	Протоколы авторизации, аутентификации и проверки подлинности в различных информационных системах. Инфраструктура открытого ключа PKI, Комплексные системы обеспечения антивирусной, антифишинговой, проактивной защиты.	5		5	11
6.	Сетевая защита				
	Безопасность программных информационных систем. Сетевая защита, защита почтовых серверов, защита критических элементов инфраструктуры.	6		6	12
	ВСЕГО	34		34	71

4.2. Содержание практических (семинарских) занятий

Не предусмотрено учебным планом

4.3. Содержание лабораторных занятий

№ п/п	Наименование раздела дисциплины	Тема лабораторного занятия	К-во часов	Самостоятельная работа на подготовку к аудиторным занятиям
семестр № 7				
1	Программно-информационные системы: основные понятия	Знакомство с программно-аппаратными комплексами обеспечение безопасности локально-вычислительных систем различного уровня.	4	8
2	Программно-информационные системы: средства обеспечения безопасности	Беспроводные системы обеспечения доступа к локально вычислительным сетям.	6	9
3	Средства контроля доступа к информационным объектам	Средства обеспечения безопасности сложных инфокоммуникационных систем. Создание и управление системами контроля ЛВС.	6	10
4	Безопасность информационных систем и сетей	Разработка документации согласно требованиям стандартов и ГОСТов, при построении комплексных систем обеспечения безопасности вычислительных сетей и комплекса управления ими. Системы реакции на инциденты безопасности	6	10
5	Протоколы авторизации, аутентификации и проверки подлинности	Безопасность информационных систем. Технология PKI в доменной инфраструктуре. Протоколы Radius, TACACS+	6	10
6	Сетевая защита	Безопасность информационных систем. Применение внутренних и внешних систем обеспечения информационной безопасности. Системы на базе продуктов Checkpoint.	3	10
		ИТОГО:	34	57

4.4. Содержание курсового проекта/работы

Учебным планом не предусмотрено.

4.5. Содержание расчетно-графического задания, индивидуальных домашних заданий

Учебным планом не предусмотрено.

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

5.1. Реализация компетенций

1 Компетенция ПК-2. Владение навыками использования различных технологий разработки программного обеспечения

Наименование индикатора достижения компетенции	Используемые средства оценивания
ПК-2.1 Анализирует и выбирает необходимую технологию разработки программного обеспечения для решения профессиональных задач	защита лабораторной работы, экзамен
ПК-2.2 Использует современные технологии разработки программного обеспечения для решения прикладных задач	защита лабораторной работы, экзамен
ПК-2.3 Использует необходимые стандарты и модели жизненного цикла программного обеспечения при разработке и реализации программного обеспечения	защита лабораторной работы, экзамен
ПК-2.4 Применяет языки программирования различного уровня для написания компонентов программных продуктов	защита лабораторной работы, экзамен
ПК-2.5 Понимает формальные методы конструирования программного обеспечения	защита лабораторной работы, экзамен
ПК-2.6 Использует методы. инструменты и технологии обеспечения качества программного обеспечения	защита лабораторной работы, экзамен

5.2. Типовые контрольные задания для промежуточной аттестации

5.2.1. Перечень контрольных вопросов (типовых заданий) для экзамена

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
1.	Программно-информационные системы: основные понятия	1. Необходимость обеспечения безопасности в информационных системах. 2. Прогресс информационных технологий и информационная безопасность. 3. Нормативно-правовые аспекты информационной безопасности. 4. Классификация угроз безопасности информационных объектов. 5. Основные виды каналов утечки информации. 6. Умышленные и неумышленные угрозы информационной безопасности. 7. Внешние угрозы информационной безопасности. 8. Мотивы и цели компьютерных преступлений. 9. Статьи уголовного кодекса о компьютерных преступлениях 10.Криминологическая характеристика преступлений в сфере компьютерной информации и их предупреждение.

		11.Объекты информационной безопасности на предприятии. 12.Организационные методы обеспечения информационной безопасности. 13.Физическая защита информационных систем. 14.Программно - технические методы обеспечения информационной безопасности.
2.	Программно-информационные системы: средства обеспечения безопасности	1. Организация системы защиты информации экономических систем. 2. Этапы построения системы защиты информации. 3. Политика безопасности. 4. Оценка эффективности инвестиций в информационную безопасность. 5. Обеспечение информационной безопасности автоматизированных банковских систем (АБС). 6. Информационная безопасность электронной коммерции (ЭК). 7. Обеспечение компьютерной безопасности учетной информации. 8. Сущность криптографических методов. 9. Организационно-административные мероприятия обеспечения компьютерной безопасности. 10.Организация конфиденциального делопроизводства. 11.Принципы обеспечения информационную безопасности на основе инженерно-технического обеспечения. 12.Типы и субъекты информационных угроз.
3.	Средства контроля доступа к информационным объектам	1. Технологии аутентификации 2. Факторы аутентификации человека 3. Аутентификация на основе паролей 4. Аутентификация на основе аппаратных аутентификаторов 5. Аутентификация информации.Электронная подпись 6. Аутентификация на основе цифровых сертификатов 7. Аутентификация программных кодов 8. Технологии управления доступом и авторизации 9. Формы представления ограничений доступа 10.Дискреционный метод управления доступом 11.Мандатный метод управления доступом 12.Ролевое управление доступом 13.Системы аутентификации и управления доступом операционных систем 14.Аутентификации пользователей ОС 15.Аутентификация в ОС семейства Unix.Протокол SSH 16.Управление доступом в операционных системах 17.Централизованные системы аутентификации и авторизации
4.	Безопасность информационных систем и сетей	1. Кто разрабатывает стратегию информационной безопасности и защиты управленческой информации? 2. Какие современные средства защиты информации применяются в корпоративных информационных системах? 3. Что включает в себя понятие "модель информационной безопасности предприятия"? 4. Перечислите внешние и внутренние угрозы для информационных потоков и систем компании. 5. Что такое "политика информационной безопасности" и какие элементы она содержит?

		6. Перечислите ключевые вопросы обеспечения информационной безопасности. 7. Какие программно-аппаратные средства применяются при обеспечении информационной безопасности предприятия? 8. Этапы проектирования сети. 9. Сетевые операционные системы. 10.Алгоритм установки сетевой ОС. 11.Служба доменных имен DNS. 12.Пространство доменных имен. 13.Работа запросов DNS. 14.Процесс рекурсии при разрешении имени. 15.Локальная система разрешения имени. 16.Типы ответов DNS-сервера. 17.Обратный просмотр. 18.Динамическое обновление. 19.Службы каталогов. 20.Active Directory. 21.Объекты службы каталогов. 22.Алгоритм добавления объекта в службу каталогов
5.	Протоколы авторизации, аутентификации и проверки подлинности	1. Протокол kerberos 2. Протокол kerberos + pkinit 3. Бщие сведения о криптографии с открытым ключом 4. Авторизация и обеспечение юридической значимости электронных документов 5. Конфиденциальность и контроль целостности передаваемой информации 6. Аутентификация связывающихся сторон 7. Установление аутентичного защищенного соединения 8. Инфраструктура открытых ключей (pki) 9. Аутентификация с помощью открытого ключа на основе сертификатов 10.Организация хранения закрытого ключа 11.Интеллектуальные устройства и аутентификация с помощью открытого ключа 12.Недостатки аутентификации с помощью открытых ключей. 13.Протокол ppp pap 14.Протокол ppp chap 15.Протокол ppp eap 7 16.Протокол tacacs+ 17.Протокол radius 18.Стандарт ieee 802.1x и протокол eapol 19.Протокол eap-tls с использованием российской криптографии
6.	Сетевая защита	1. Средства защиты операционной системы и ее конфигурации, программного и информационного обеспечения от потерь и несанкционированного доступа; 2. Системы доступа к информации по ключам и паролям; 3. Средства архивации данных на машинных носителях, в том числе, под паролями; 4. Антивирусные и профилактические средства; 5. Средства кодирования и раскодирования данных; 6. Средства восстановления данных при их частичной и полной утрате;

		7. Автоматизированная система копирования и дублирования наборов данных на архивные носители; 8. Система программ и утилит по восстановлению наборов данных с архивных или эталонных носителей. 9. Информационные системы резервирования служб каталогов 10.Инструменты резервирования почтовых серверов 11.Средства программной защиты от преднамеренных сетевых атак на критические элементы инфраструктуры. 12.Безопасность веб-сервиса 13.Безопасность веб-браузера 14.Приватность и куки 15.Протокол https 16.Безопасность средств создания динамических страниц 17.Безопасность электронной почты 18.Угрозы приватности почтового сервиса 19.Аутентификация отправителя 20.Шифрование содержимого письма 21.Защита метаданных пользователя 22.Спам 23.Атаки почтовых приложений 24.Облачные сервисы и их безопасность 25.Концепция облачных вычислений 26.Определение облачных вычислений 27.Модели сервисов облачных сервисов 28.Облачные вычисления как источник угрозы 29.Облачные сервисы как средство повышения сетевой безопасности

5.3. Типовые контрольные задания (материалы) для текущего контроля в семестре

Текущий контроль осуществляется в течение семестра в форме защиты лабораторных работ.

Защита лабораторной работы проводиться в форме устного опроса студента и направлена на проверку степени усвоения материала и понимания теоретических сведений, используемых в процессе выполнения работы; для защиты необходимо представить в печатной форме отчет по лабораторной работе, выполненный самостоятельно и в соответствии со всеми требованиями, приведёнными в методических указаниях к выполнению лабораторных работ. Примерные перечень контрольных вопросов для защиты лабораторных работ приведен в таблице:

Тематика лабораторной работы	Контрольные вопросы
Знакомство с программно-аппаратными комплексами обеспечение безопасности локально-вычислительных систем различного уровня.	Понятие программно-информационной системы. Классификация программно-информационных систем. Оценка безопасности компьютерных систем. Критерии безопасности компьютерных систем и их характеристика.
Беспроводные системы обеспечения доступа к локально	Комплексные средства обеспечения информационных объектов: понятие, виды, свойства.

вычислительным сетям.	Классификация программных методов обеспечения безопасности. Классификация аппаратных методов обеспечения безопасности. Классификация гибридных методов обеспечения безопасности. Средства обеспечения информационной безопасности.
Средства обеспечения безопасности сложных инфокоммуникационных систем. Создание и управление системами контроля ЛВС.	Системы аутентификации. Система авторизации. Межсетевой уровень взаимодействия систем обеспечения безопасности. Межпрограммный уровень взаимодействия систем обеспечения безопасности. Средства контроля доступа: понятие, свойства. Системы разграничения доступа к ресурсам: понятие, функции.
Разработка документации согласно требованиям стандартов и ГОСТов, при построении комплексных систем обеспечения безопасности вычислительных сетей и комплекса управления ими. Системы реакции на инциденты безопасности.	Безопасность локальных информационных систем. Безопасность городских информационных систем. Безопасность глобальных информационных систем. Безопасность информационных вычислительных сетей. Проектирование системам обеспечения информационной безопасности в вычислительных сетях локального уровня. Управление системами обеспечения информационной безопасности в вычислительных сетях глобального уровня.
Безопасность информационных систем. Технология PKI в доменной инфраструктуре. Протоколы Radius, TACACS+	Протокол авторизации в различных информационных системах. Протокол аутентификации в различных информационных системах Протокол проверки подлинности в различных информационных системах Комплексные системы обеспечения антивирусной, защиты. Комплексные системы обеспечения антифишинговой защиты. Комплексные системы обеспечения проактивной защиты.
Безопасность информационных систем. Применение внутренних и внешних систем обеспечения информационной безопасности. Системы на базе продуктов Checkpoint.	Сетевая защита; понятие, особенности, принципы организации. Защита почтовых серверов: понятие, организация. Критические элементы инфраструктуры: понятие, свойства, примеры Защита критических элементов инфраструктуры.

Критерии оценки лабораторной работы: лабораторная работа считается защищенной, если студент выполнил задание к работе полностью и во время устного опроса по работе правильно ответил на заданные преподавателем дополнительные вопросы.

5.4. Описание критериев оценивания компетенций и шкалы оценивания

При промежуточной аттестации в форме экзамена используется следующая шкала оценивания: 2 – неудовлетворительно, 3 – удовлетворительно, 4 – хорошо, 5 – отлично.

Критериями оценивания достижений показателей являются:

Наименование показателя оценивания результата обучения по дисциплине	Критерий оценивания
Знания	Знание терминов, определений, понятий безопасности программно-информационных систем
	Объем освоенного материала
	Полнота ответов на вопросы

	Четкость изложения и интерпретации знаний
Умения	Умение решать стандартные профессиональные задачи с учетом методов обеспечения безопасности программно-информационных систем
	Умение использовать теоретические знания для выбора методики решения профессиональных задач в
Навыки	Владение навыками выбора и использования методов обеспечения безопасности ПИС
	Качество обеспечения безопасности ПИС при решении профессиональных задач
	Самостоятельность выполнения решения задач обеспечения безопасности ПИС

Оценка преподавателем выставляется интегрально с учётом всех показателей и критериев оценивания.

Оценка сформированности компетенций по показателю Знания.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Знание терминов, определений, понятий безопасности программно-информационных систем	Не знает терминов и определений	Знает термины и определения, но допускает неточности формулировок	Знает термины и определения	Знает термины и определения, может корректно сформулировать их самостоятельно
Объем освоенного материала	Не знает значительной части материала дисциплины	Знает только основной материал дисциплины, не усвоил его деталей	Знает материал дисциплины в достаточном объеме	Обладает твердым и полным знанием материала дисциплины, владеет дополнительными знаниями
Полнота ответов на вопросы	Не дает ответы на большинство вопросов	Дает неполные ответы на все вопросы	Дает ответы на вопросы, но не все - полные	Дает полные, развернутые ответы на поставленные вопросы
Четкость изложения и интерпретации знаний	Излагает знания без логической последовательности	Излагает знания с нарушениями в логической последовательности	Излагает знания без нарушений в логической последовательности	Излагает знания в логической последовательности, самостоятельно их интерпретируя и анализируя
	Не иллюстрирует изложение поясняющими схемами, рисунками и примерами	Выполняет поясняющие схемы и рисунки небрежно и с ошибками	Выполняет поясняющие рисунки и схемы корректно и понятно	Выполняет поясняющие рисунки и схемы точно и аккуратно, раскрывая полноту усвоенных знаний
	Неверно излагает и интерпретирует знания	Допускает неточности в изложении и интерпретации знаний	Грамотно и по существу излагает знания	Грамотно и точно излагает знания, делает самостоятельные выводы

Оценка сформированности компетенций по показателю Умения.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Умение решать стандартные профессиональные задачи с учетом методов обеспечения безопасности программно-информационных систем	Не умеет решать стандартные профессиональные задачи обеспечения безопасности ПИС	Допускает неточности в решении стандартных профессиональных задач с применением методов обеспечения безопасности ПИС	Умеет решать стандартные профессиональные задачи с применением методов обеспечения безопасности ПИС	Безошибочно решает стандартные профессиональные задачи с применением методов обеспечения безопасности ПИС
Умение использовать теоретические знания для выбора методики решения профессиональных задач в	Не умеет использовать теоретические знания для выбора методики решения профессиональных задач	Использование теоретических знаний для выбора методики решения профессиональных задач вызывает затруднения	Умеет использовать теоретические знания для выбора методики решения профессиональных задач	Умело использует теоретические знания для выбора методики решения профессиональных задач

Оценка сформированности компетенций по показателю Навыки.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Владение навыками выбора и использования методов обеспечения безопасности ПИС	Не владеет навыками выбора и использования методов обеспечения безопасности ПИС	Не достаточно хорошо владеет выбора и использования методов обеспечения безопасности ПИС	Владеет навыками выбора и использования методов обеспечения безопасности ПИС	Профессионально владеет навыками выбора и использования методов обеспечения безопасности ПИС
Качество обеспечения безопасности ПИС при решении профессиональных задач	Не качественно выполняет обеспечения безопасности ПИС, допускает грубые ошибки	Не достаточно качественно выполняет обеспечения безопасности ПИС, допускает и исправляет ошибки с посторонней помощью	Не достаточно качественно выполняет обеспечения безопасности ПИС, допускает и исправляет ошибки самостоятельно	Качественно выполняет исследования обеспечения безопасности ПИС
Самостоятельность выполнения решения задач обеспечения безопасности ПИС	Не может самостоятельно выполнять решение задач обеспечения безопасности ПИС	Выполняет решение задач обеспечения безопасности ПИС с посторонней помощью	При выполнении решения задач обеспечения безопасности ПИС иногда требуется посторонняя помощь	Самостоятельно выполняет решения задач обеспечения безопасности ПИС

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

6.1. Материально-техническое обеспечение

№	Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
1.	Учебная аудитория для проведения лекционных занятий	Специализированная мебель. Мультимедийная установка, экран, доски
2.	Учебная аудитория для проведения лабораторных занятий	Специализированная мебель. Компьютеры на базе процессоров Intel или AMD.
3.	Читальный зал библиотеки для самостоятельной работы	Специализированная мебель. Компьютерная техника, подключенная к сети интернет и имеющая доступ в электронно-образовательную среду

6.2. Лицензионное и свободно распространяемое программное обеспечение

№	Перечень лицензионного программного обеспечения.	Реквизиты подтверждающего документа
1.	Microsoft Windows 10 Корпоративная	(Соглашение Microsoft Open Value Subscription V9221014 Соглашение действительно с 01.11.2020 по 31.10.2023). Договор поставки ПО № 128-21 от 30.10.2021.
2.	Microsoft Office Professional Plus 2016	(Соглашение Microsoft Open Value Subscription V9221014 Соглашение действительно с 01.11.2020 по 31.10.2023). Договор поставки ПО № 128-21 от 30.10.2021.
3.	Kaspersky Endpoint Security «Стандартный Russian Edition»	Сублицензионный договор № 102 от 24.05.2018. Срок действия лицензии до 19.08.2020 Гражданско-правовой Договор (Контракт) № 27782 «Поставка продления права пользования (лицензии) Kaspersky Endpoint Security от 03.06.2020. Срок действия лицензии 19.08.2022г.
4.	Google Chrome	Свободно распространяемое ПО согласно условиям лицензионного соглашения
5.	Среды программирования Free Pascal, Dev C++ или CodeBlocks. Система пакетного анализа tcp-dump, Wireshark. Системы обеспечения защиты межсетевого взаимодействия iptables, shorewall, Microsoft firewall	Свободно распространяемое ПО согласно условиям лицензионного соглашения

6.3. Перечень учебных изданий и учебно-методических материалов

1. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности: учебное пособие / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — 3-е изд. — Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 431 с. — ISBN 978-5-4497-0935-6. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/102070.html

2. Информационная безопасность. Практические аспекты: учебник для вузов / Л. Х. Сафиуллина, А. Р. Касимова, Я. С. Рябов [и др.]. — Санкт-Петербург: Интермедия, 2021. — 240 с. — ISBN 978-5-4383-0205-6. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/103997.html

3. В. С. Горбатов, О. Ю. Полянская - Основы технологии PKI - 2-е изд. - Телеком, 2011 1 + 1

4. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы: учеб. пособие / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб.: Питер, 2011.

5. Пакин, А. И. Информационная безопасность информационных систем управления предприятием: учебное пособие по части курса / А. И. Пакин. — Москва: Московская государственная академия водного транспорта, 2009. — 41 с. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/46462.html

6. Лиманова, Н. И. Архитектура вычислительных систем и компьютерных сетей: учебное пособие. — Самара: Поволжский государственный университет телекоммуникаций и информатики, 2017. — 197 с. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/75368.html

7. Катунин Г.П. Основы инфокоммуникационных технологий [Электронный ресурс]: учебник. — Саратов: Ай Пи Эр Медиа, 2018. — 797 с. — Режим доступа: http://www.iprbookshop.ru/74561.html

8. Голицына, О. Л. Программное обеспечение: учеб. пособие / О. Л. Голицына, Т. Л. Партыка, И. И. Попов. - 3-е изд., перераб. и доп. - М.: Форум, 2010.

9. Галицкий А. В., Рябко С. Д., Шаньгин В. Ф. Защита информации в сети — анализ технологий и синтез решений. М.: ДМК Пресс, 2004.

10. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.: Книжный мир, 2009.

11. Кравченко, Т. К. Инфокоммуникационные технологии управления предприятием: учеб. пособие / Т. К. Кравченко, В. Ф. Пресняков. - М. : ГУ ВШЭ, 2003.

12. Fuzzing: исследование уязвимостей методом грубой силы - ("High Tech") /Саттон М., Амини П., Грин А., Саттон М., Александр Грин, Амини П. Символ-Плюс, 2009.

13. Берлин, А. Н. Основные протоколы интернет: учебное пособие / А. Н. Берлин. — 3-е изд. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 601 с. — ISBN 978-5-4497-

0337-8. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/89452.html

14. Привалов И.М. Основы аппаратного и программного обеспечения [Электронный ресурс]: учебное пособие. — Ставрополь: Северо-Кавказский федеральный университет, 2015. — 145 с. — Режим доступа: http://www.iprbookshop.ru/63113.html

15. Петров, А. А. Компьютерная безопасность. Криптографические методы защиты. — 2-е изд. — Саратов: Профобразование, 2019. — 446 с. — ISBN 978-5-4488-0091-7. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/87998.html

16. Персова М.Г. Современные компьютерные технологии [Электронный ресурс]: конспект лекций / М.Г. Персова, Ю.Г. Соловейчик, П.А. Домников. — Новосибирск: Новосибирский государственный технический университет, 2014. — 80 с. — Режим доступа: http://www.iprbookshop.ru/45025.htm

17. Д.П. Зегжда, А.М. Ивашко. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000.

6.4. Перечень интернет ресурсов, профессиональных баз данных, информационно-справочных систем

1. Электронная библиотека (на базе ЭБС «БиблиоТех») — Режим доступа: http://ntb.bstu.ru
2. Электронно-библиотечная система IPRbooks — Режим доступа: http://www.iprbookshop.ru
3. Электронно-библиотечная система «Университетская библиотека ONLINE» — Режим доступа: http://www.biblioclub.ru/

6. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Рабочая программа утверждена на 20____ /20____ учебный год без изменений / с изменениями, дополнениями

Протокол № _____ заседания кафедры от «_ _»_____ 20___ г.

Заведующий кафедрой_____
подпись, ФИО

Директор института _____
подпись, ФИО