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

РАБОЧАЯ ПРОГРАММА
дисциплины

Основы информационной безопасности
направление подготовки:

38.03.05 Бизнес-информатика

Направленность программы (профиль):

Технологическое предпринимательство

Квалификация

бакалавр

Форма обучения

очная

Институт информационных технологий и управляющих систем

Кафедра прикладной информатики

Белгород 2025

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.03 Прикладная информатика утвержденного приказом Минобрнауки России от 19.09.2017г. №922
- учебного плана, утвержденного ученым советом БГТУ им. В.Г. Шухова в 2025 году.

Составитель (составители): канд.экон.наук, доц. (Д.В. Кадацкая),
В.А. Бондарь

Рабочая программа обсуждена на заседании кафедры

«28» апреля 2025 г., протокол № 5

Заведующий кафедрой: канд. экон. наук, доц. (Д.В. Кадацкая)

Рабочая программа согласована с выпускающей кафедрой
прикладной информатики

Заведующий кафедрой: канд. экон. наук, доц. (Д.В. Кадацкая)

«28» апреля 2025 г.

Рабочая программа одобрена методической комиссией института

«29» апреля 2025 г., протокол № 8

Председатель: доц. _____ (Ю.Д. Рязанов)

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
	ПК-2. Способен выполнять работы по сопровождению информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы	ПК-2.6 Применяет информационно-коммуникационные технологии, учитывая основные требования информационной безопасности для решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры	**Знания** понятия информационной безопасности; **Умения** применять способы обеспечения собственной информационно-психологической безопасности в различных коммуникационных ситуациях, в том числе при работе в сети Интернет. **Навыки** владения базовой терминологией и гуманитарными аспектами в области информационной безопасности личности, общества, государства

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1. Компетенция ПК-2. Способен выполнять работы по сопровождению информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы

Стадия	Наименования дисциплины
1	Производственная научно-исследовательская работа
2	Электронный бизнес: стратегия и инновации
3	Информационные системы управления фирмой / Автоматизированные информационные технологии в экономике
4	Экономика и эффективность информационных систем
5	Производственная (преддипломная) практика
6	Современные подходы и стандарты цифрового предприятия
7	Управление ИТ-проектами
8	Организационное обеспечение ИТ-услуг *Регламентация ИТ-услуг и процессов

9	Моделирование бизнес-процессов
10	Производственная технологическая (проектно-технологическая) практика

3. ОБЪЕМ ДИСЦИПЛИНЫ

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

Форма промежуточной аттестации – экзамен

Вид учебной работы	Всего часов	Семестр № 8
Общая трудоемкость дисциплины, час	180	180
Контактная работа (аудиторные занятия), в т.ч.:	58	58
лекции	18	18
лабораторные	36	36
практические		
групповые консультации в период теоретического обучения и промежуточной аттестации	4	4
Самостоятельная работа студентов, включая индивидуальные и групповые консультации, в том числе:	122	122
Курсовой проект		
Курсовая работа		
Расчетно-графическое задание	9	9
Индивидуальное домашнее задание		
Самостоятельная работа на подготовку к аудиторным занятиям (лекции, практические занятия, лабораторные занятия)		
Экзамен	36	36

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Наименование тем, их содержание и объем

Курс 4 Семестр 8

№ 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.	Тема 1. Информационная безопасность в системе национальной безопасности Российской Федерации				
	Понятие (концепция) национальной безопасности. Виды безопасности. Доктрина информационной безопасности	3		6	15
2.	Тема 2. Основные понятия и термины информационной безопасности				
	Информация как актив государства, бизнеса, личности. Базовые свойства информации как объекта защиты.	4		8	15

	Угроза, риск, инцидент, ущерб информационной безопасности. Уязвимость.				
3.	Тема 3. Основные методы защиты информации от базовых угроз				
	Основные методы защиты от угроз нарушения конфиденциальности информации. Основные методы защиты от угроз нарушения целостности и доступности информации.	4		8	16
4.	Тема 4. Стандарты информационной безопасности				
	Стандарты информационной безопасности. Роль стандартов. Основные оценочные стандарты. Основные управленческие стандарты (спецификации). Понятие об управлении информационной безопасностью.	4		8	16
5.	Тема 5. Проблематика построения систем защиты информации				
	Функциональная модель системы защиты информации. Проблемы защиты информации и пути их решения.	3		6	15
	ВСЕГО	18		36	77

4.2. Содержание практических (семинарских) занятий

Практические занятия не предусмотрены 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 № 8				
1	Тема 1. Информационная безопасность в системе национальной безопасности Российской Федерации	Роль информационной безопасности в обеспечении национальной безопасности	6	15
2	Тема 2. Основные понятия и термины информационной безопасности	Связь и взаимное влияние базовых свойств информации как объекта защиты. Информационные ресурсы информационной системы. Оценки риска и ущерба информационной безопасности	8	15
3	Тема 3. Основные методы защиты информации от базовых угроз	Построение полного списка угроз Построения дерева угроз	8	16
4	Тема 4. Стандарты информационной безопасности	Оценочные стандарты 1-го поколения: Оранжевая книга, РД ФСТЭК	8	16
5	Тема 5. Проблематика построения систем защиты информации	Способы разграничения доступа к информации в информационной системе. Идентификация и аутентификация	6	15
		ИТОГО:	36	77

4.4. Содержание курсового проекта/работы

Курсовая работа не предусмотрена учебным планом.

4.5. Содержание расчетно-графического задания, индивидуальных домашних заданий

В процессе выполнения **расчетно-графического задания** осуществляется контактная работа обучающегося с преподавателем. Консультации проводятся в аудитория и/или посредствам электронной информационно-образовательной среды университета.

На выполнение РГЗ предусмотрено 9 часов самостоятельной работы студента.

Цель задания: закрепление теоретических знаний, полученных при изучении дисциплины, и развитие практических навыков применения основных бизнес-моделей для управления серией ИТ-продуктов.

Структура работы. Теоретическое задание, включающее темы рефератов. Практическое задание – это решение кейсовых задач по рассматриваемым разделам.

Перечень примерных тем для рефератов:

1. Организация и управление информационной безопасностью в крупных компаниях.
2. Роль человеческого фактора в обеспечении информационной безопасности.
3. Биометрические технологии идентификации и их роль в информационной безопасности.
4. Социальная инженерия и манипуляции человеческим фактором в ИТ.
5. Безопасность мобильных устройств и приложений.

Типовое кейс-задание: "Уязвимость в системе управления".

Ситуация:

Вы работаете в компании "ТехноСистемы", которая разрабатывает программное обеспечение для управления данными клиентов. Недавно в вашей компании была обнаружена уязвимость в системе, которая может привести к утечке конфиденциальной информации. Уязвимость связана с недостаточной защитой пользовательских данных и возможностью несанкционированного доступа к базе данных.

Задание:

1. Анализ уязвимости:

Опишите, какие типы данных могут быть под угрозой из-за этой уязвимости.

Какие последствия могут возникнуть для компании и клиентов в случае утечки данных?

2. Оценка рисков:

Проведите оценку рисков, связанных с данной уязвимостью. Используйте методику, например, SWOT-анализ или матрицу рисков.

Определите вероятность возникновения инцидента и его потенциальное воздействие.

3. Разработка мер по устранению уязвимости:

Предложите конкретные меры по устранению уязвимости. Укажите, какие технологии или подходы могут быть использованы для повышения безопасности.

Опишите, как можно обучить сотрудников компании для предотвращения подобных инцидентов в будущем.

4. Создание плана реагирования на инциденты:

Разработайте план реагирования на инциденты, который будет включать шаги по обнаружению, реагированию и восстановлению после утечки данных.

Укажите, какие роли и обязанности должны быть у сотрудников в случае возникновения инцидента.

Формат выполнения:

Подготовьте краткую презентацию (5-7 слайдов), в которой изложите результаты вашего анализа, предложенные меры и план реагирования.

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

5.1. Реализация компетенций

Компетенция ПК-2. Способен выполнять работы по сопровождению информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы.

Наименование индикатора достижения компетенции	Используемые средства оценивания
ПК-2.6 Применяет информационно-коммуникационные технологии, учитывая основные требования информационной безопасности для решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры	Тестовый контроль, собеседование, кейсы, защита расчетно-графического задания, экзамен

5.2. Типовые контрольные задания для промежуточной аттестации

5.2.1. Перечень контрольных вопросов (типовых заданий) для экзамена

1. Сущность и понятие информационной безопасности. Характеристики ее составляющих.
2. Требования к информации как к объекту защиты.
3. Виды безопасности. Классификация видов безопасности.
4. Модель нарушителя информационной безопасности.
5. Компьютерные преступления.
6. Угрозы в информационной безопасности. Классификация угроз.
7. Базовые угрозы информационной безопасности.
8. Уязвимости в информационной безопасности. Классификация уязвимостей
9. Носители информации. Классификация носителей информации.
10. Человек – как носитель защищаемой информации.
11. Угрозы нарушения конфиденциальности информации. Основные методы защиты от угроз нарушения конфиденциальности.
12. Угрозы нарушения целостности информации. Основные методы защиты от угроз нарушения целостности информации
13. Угрозы нарушения доступности информации. Основные принципы построения систем защиты от угроз нарушения доступности.
14. Идентификация. Определение, виды идентификаторов.
15. Аутентификация. Определение, основные методы аутентификации.
16. Классификация защищаемой информации по характеру сохраняемой тайны.
17. Разграничение доступа. Основные методы разграничения доступа.
18. Стандарты информационной безопасности. Роль стандартов в обеспечении ИБ. Виды стандартов.
19. Оранжевая книга. Основные положения. Значение для развития информационной безопасности.
20. РД ФСТЭК. Основные положения и принципы защиты от НСД.

5.2.2. Перечень контрольных материалов для защиты курсового проекта/ курсовой работы

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

№ п/п	Наименование раздела дисциплины	Компе-тенция	Содержание вопросов (типовых заданий)
1	Тема 1. Информационная безопасность в системе национальной безопасности Российской Федерации	ПК-2	Типовые вопросы: 1.Основные угрозы информационной безопасности, с которыми сталкивается Российская Федерация, и какие меры принимаются для их предотвращения? 2.Роль Федеральной службы безопасности (ФСБ) и других государственных органов в обеспечении информационной безопасности в России? 3. Основные законодательные инициативы и нормативные акты, регулирующие вопросы информационной безопасности в Российской Федерации? Тестовый контроль 1.Какие сведения относятся к охраняемой законом тайне в Российской Федерации? a) Информация о доходах физических лиц b) Государственная тайна, коммерческая тайна, персональные данные граждан c) Любая служебная документация государственных органов власти d) Информационно-развлекательные материалы СМИ 2.Какие цели преследует обеспечение информационной безопасности в рамках национальной безопасности страны? a) Ограничение свободы слова в средствах массовой информации b) Создание препятствий международному обмену научной информацией c) Защита национальных интересов и суверенитета страны в информационной среде d) Контроль над всеми источниками распространения информации 3.Как называется официальный государственный портал, созданный для информирования населения о мерах информационной безопасности? a) Портал Госуслуг b) Официальный сайт ФСБ России c) Сайт Министерства обороны РФ d) Сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК)
2	Тема 2. Основные понятия и термины информационной безопасности	ПК-2	Типовые вопросы: 1.Перечислите три основных базовых свойства информации, защищаемых в информационной безопасности, и коротко охарактеризуйте каждое из них.

			2.Приведите пример нарушения какого-либо из базовых свойств информации и укажите возможные последствия такого нарушения. 3.Что такое инцидент информационной безопасности, и какие действия следует предпринять в случае его возникновения? Тестовый контроль 1.Какое базовое свойство информации связано с предотвращением её раскрытия посторонним лицам? a) Достоверность b) Конфиденциальность c) Доступность d) Целостность 2.Какой компонент информационных ресурсов обеспечивает возможность обработки и анализа больших объемов данных? a) Аппаратные средства b) Программное обеспечение c) Данные и базы данных d) Методические материалы 3.Что представляет собой оценка уязвимости информационной системы? a) Анализ эффективности мер защиты b) Определение потенциальных рисков нарушения конфиденциальности, доступности и целостности информации c) Оценка экономических последствий нарушений информационной безопасности d) Измерение количества пользователей системы
3	Тема 3. Основные методы защиты информации от базовых угроз	ПК-2	Типовые вопросы: 1.Какие основные меры предосторожности помогают защитить персональные данные пользователей от случайного разглашения? 2.Каковы наиболее эффективные способы предотвращения несанкционированного доступа к корпоративным информационным ресурсам? 3.Что включает в себя комплексный подход к защите информации от внутренних угроз в организациях разного масштаба? Тестовый контроль 1.Какой метод защиты используется для предотвращения перехвата передаваемых данных? a) Шифрование данных b) Регистрация действий пользователей c) Резервное копирование данных d) Антивирусная защита 2.Какой способ позволяет ограничить доступ к

			информации определённой группе лиц? a) Использование паролей и биометрической аутентификации b) Установка межсетевых экранов (брандмауэров) c) Применение антивирусных программ d) Организация резервного копирования данных 3.Какой механизм предназначен для восстановления данных после инцидента информационной безопасности? a) Фильтрация трафика b) Резервное копирование и архивация данных c) Шифрование файлов d) Контроль прав доступа
4	Тема 4. Стандарты информационной безопасности	ПК-2	Типовые вопросы: 1.Какие международные стандарты в области информационной безопасности являются наиболее распространёнными и почему важно следовать именно этим стандартам? 2.Чем отличаются требования стандартов ISO/IEC 27001 и ГОСТ Р ИСО/МЭК 27001 в части подхода к обеспечению информационной безопасности организаций? 3.Как внедрение стандарта информационной безопасности помогает снизить риски потери критически важной информации в российских компаниях? Тестовый контроль 1.Основная цель применения оценочных стандартов 1-го поколения, таких как "Оранжевая книга" и РД ФСТЭК? a) Повышение производительности труда b) Оценка и управление рисками в области информационной безопасности c) Разработка новых технологий защиты информации d) Обучение сотрудников основам информационной безопасности 2.Что представляет собой "Оранжевая книга" в контексте оценочных стандартов 1-го поколения? a) Методические рекомендации по оценке рисков b) Стандарт по управлению качеством c) Документ, описывающий методы оценки защищенности информации d) Руководство по внедрению системы менеджмента качества 3.Какой из следующих принципов является основным в оценке защищенности информации согласно "Оранжевой книге"? a) Принцип минимизации затрат b) Принцип системного подхода c) Принцип максимальной открытости

			d) Принцип случайного выбора
5	Тема 5. Проблематика построения систем защиты информации	ПК-2	Типовые вопросы: 1.Какие сложности возникают при интеграции различных технологий защиты информации в рамках одной организации и как минимизировать такие проблемы? 2.Почему современные организации сталкиваются с трудностями в обеспечении баланса между уровнем защиты информации и удобством пользования системами пользователями? 3.Какие ключевые факторы влияют на выбор методов и инструментов защиты информации, и как определить оптимальную стратегию защиты исходя из специфики деятельности предприятия? Тестовый контроль 1.К какой категории проблем относится отсутствие единой стратегии защиты информации внутри организации? a) Организационная проблема b) Экономическая проблема c) Техническая проблема d) Юридическая проблема 2.Почему система защиты информации должна учитывать человеческие факторы? a) Для минимизации финансовых затрат b) Для снижения технических сложностей c) Потому что сотрудники часто становятся причиной утечек информации d) Для упрощения администрирования системы 3.Основной проблемой обеспечения эффективной защиты информации считается? a) Неадекватная оценка существующих угроз b) Недостаточное финансирование проектов c) Неправильная настройка правил доступа d) Нехватка квалифицированных кадров

5.4. Описание критериев оценивания компетенций и шкалы оценивания

При промежуточной аттестации в форме экзамена, дифференцированного зачета, дифференцированного зачета при защите курсового проекта/работы 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
ПК-2. Способен выполнять работы по сопровождению информационных систем,	

автоматизирующих задачи организационного управления и бизнес-процессы	
Знания	Знания понятия информационной безопасности
	Объем освоенного материала
Умения	Умения применять способы обеспечения собственной информационно-психологической безопасности в различных коммуникационных ситуациях, в том числе при работе в сети Интернет.
Навыки	Владения базовой терминологией и гуманитарными аспектами в области информационной безопасности личности, общества, государства

Оценка сформированности компетенций по показателю *Знания*.

Критерий	Уровень освоения и оценка			
	2	3	4	5
ПК-2. Способен выполнять работы по сопровождению информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы				
Знания понятия информационной безопасности	Не знает понятия информационной безопасности	Знает понятия информационной безопасности, но допускает неточности формулировок	Знает понятия информационной безопасности.	Знает понятия информационной безопасности, 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

Оценка сформированности компетенций по показателю *Умения*.

Критерий	Уровень освоения и оценка			
	2	3	4	5
ПК-2. Способен выполнять работы по сопровождению информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы				
Умения применять способы обеспечения собственной информационно-психологической безопасности в различных коммуникационных ситуациях, в том числе при работе в сети Интернет.	Не может применять способы обеспечения собственной информационно-психологической безопасности в различных коммуникационных ситуациях, в том числе при работе в сети Интернет.	Может применять способы обеспечения собственной информационно-психологической безопасности в различных коммуникационных ситуациях, в том числе при работе в сети Интернет., но допускает неточности	Может применять способы обеспечения собственной информационно-психологической безопасности в различных коммуникационных ситуациях, в том числе при работе в сети Интернет.	Умеет правильно, самостоятельно применять способы обеспечения собственной информационно-психологической безопасности в различных коммуникационных ситуациях, в том числе при работе в сети Интернет.

Оценка сформированности компетенций по показателю *Навыки*.

Критерий	Уровень освоения и оценка			
	2	3	4	5
ПК-2. Способен выполнять работы по сопровождению информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы				
Владения базовой терминологией и гуманитарными аспектами в области информационной безопасности личности, общества, государства	Не владеет базовой терминологией и гуманитарными аспектами в области информационной безопасности личности, общества, государства.	Неуверенно владеет базовой терминологией и гуманитарными аспектами в области информационной безопасности личности, общества, государства.	Владеет базовой терминологией и гуманитарными аспектами в области информационной безопасности личности, общества, государства.	В полной мере владеет базовой терминологией и гуманитарными аспектами в области информационной безопасности личности, общества, государства.

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	Читальный зал библиотеки для самостоятельной работы	Специализированная мебель; компьютерная техника, подключенная к сети «Интернет», имеющая доступ в электронную информационно-образовательную среду
2	Учебная аудитория для проведения лекционных и практических занятий, консультаций, текущего контроля, промежуточной аттестации, самостоятельной работы	Специализированная мебель; мультимедийный проектор, переносной экран, ноутбук
3	Методический кабинет	Специализированная мебель; мультимедийный проектор, переносной экран, ноутбук

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 V6328633. Соглашение действительно с 02.10.2017 по 31.10.2023). Договор поставки ПО 0326100004117000038-0003147-01 от 06.10.2017
2	Microsoft Office Professional Plus 2016	Соглашение Microsoft Open Value Subscription V6328633. Соглашение действительно с 02.10.2017 по 31.10.2023
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	Mozilla Firefox	Свободно распространяемое ПО согласно условиям лицензионного соглашения

6.3. Перечень учебных изданий и учебно-методических материалов

1.Карпенко, В. В. Основы информационной безопасности : учебное пособие / В. В. Карпенко ; Томский политехнический университет. — Томск : Изд-во Томского политехнического университета, 2020. — 124 с.

2.Комягин, В. Б. Основы информационной безопасности : учебник и практикум для прикладного бакалавриата / В. Б. Комягин, Н. И. Тихоновская. — 3-е изд., испр. и доп. — Москва : Юрайт, 2021. — 368 с.

3.Максимов, Ю. Н. Основы информационной безопасности : учебник / Ю. Н. Максимов, В. Н. Кузнецов. — Ростов-на-Дону : Феникс, 2022. — 320 с.

4.Сергеев, С. Ф. Основы информационной безопасности : учебное пособие / С. Ф. Сергеев, А. В. Куприянов. — Новосибирск : Новосибирский государственный технический университет, 2021. — 148 с.

5.Федотов, А. А. Основы информационной безопасности : учебное пособие / А. А. Федотов, Я. С. Коротких. — Красноярск : Сибирский федеральный университет, 2020. — 184 с.

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

1. https://www.it-world.ru/it-news/tech/ – Портал о новостях в мире технологий.
2. https://www.ixbt.com/live/ – Сайт с ревью на компьютерную технику, новостями об информационных технологиях и новинках программного обеспечения.
3. https://thecode.media/about/ – журнал «Яндекс Практикума» о технологиях и программировании в России.
4. https://habr.com/ru/companies/skillfactory/articles/ – экосистема для сообщества разработчиков, инженеров, дизайнеров, менеджеров – всех, кто создаёт IT-продукты.
5. https://rb.ru/ – медиа, комьюнити и сервисы для предпринимателей и всех людей, которые уже развивают свой бизнес или хотят заняться этим и самостоятельно растить свой проект.
6. https://www.cnews.ru/about – оперативные новости и аналитические материалы мира высоких технологий в России и странах СНГ

7. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ[1]

Рабочая программа утверждена на 20____ /20____ учебный год без изменений / с изменениями, дополнениями[2]

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

Заведующий кафедрой_____
подпись, ФИО

Директор института _____
подпись, ФИО

[1] Заполняется каждый учебный год на отдельных листах
[2] Нужное подчеркнуть