МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г. ШУХОВА»
(БГТУ им. В.Г. Шухова)

СОГЛАСОВАНО
Директор института заочного образования
_____ С.Е. Спесивцева
«28» 04 2020 г.

УТВЕРЖДАЮ
Директор института
_____ Ю.А. Дорошенко
«28» 04 2020 г.

РАБОЧАЯ ПРОГРАММА
дисциплины

Информационная безопасность

направление:
41.03.06 Публичная политика и социальные науки

профиль подготовки:
41.03.06 Публичная политика в социально-экономической сфере

Степень
Бакалавр

Форма обучения
заочная

Институт: экономики и менеджмента

Кафедра: экономики и организации производства

Белгород – 2020

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта высшего профессионального образования для бакалавриата по направлению подготовки 41.03.06 Публичная политика и социальные науки (утв. приказом Министерства образования и науки РФ от 20 октября 2015 г. N 1174);
- плана учебного процесса БГТУ им. В.Г. Шухова, введенного в действие в 2020 году;

Составитель: к.э.н., доц. (А.А. Рябов)

Рабочая программа обсуждена на заседании кафедры

теории и методологии науки

«28» апреля 2020 г., протокол № 8

Заведующий кафедрой: д-р экон. наук., проф. Е.Н. Чижова

Рабочая программа обсуждена на заседании кафедры
экономики и организации производства

«29» апреля2020 г., протокол № 8

Заведующий кафедрой: д.э.н., профессор Ю.И. Селиверстов

Рабочая программа одобрена методической комиссией

института экономики и менеджмента

«28» апреля2020 г., протокол № 8

Председатель: канд. экон. наук, доц. Л.И. Журавлева

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

• Формируемые компетенции			• Требования к результатам обучения
№	Код компетенции	Компетенция	
Общекультурные			
1	ОК-8	Способность понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны	В результате освоения дисциплины обучающийся должен: **Знать:** - историю, современное состояние, проблемы и тенденции развития систем информационной безопасности и защиты информации; - нормативно-правовую базу обеспечения информационной безопасности и защиты информации; - систему органов власти, определяющих и реализующих государственную политику в области информационной безопасности и защиты информации. **Уметь:** - анализировать проблемы информационной безопасности и защиты информации в системах документооборота и архивном деле; - применять отечественные и зарубежные стандарты в области информационной безопасности и защиты информации; - определять угрозы, уязвимости и риски информационной безопасности; **Владеть:** - терминологией и понятийным аппаратом в области информационной безопасности и защиты информации; навыками использования методов и средств обеспечения информационной безопасности и защиты информации.
Общепрофессиональные			
2	ОПК-10	Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	В результате освоения дисциплины обучающийся должен: **Знать:** -- систему документационного обеспечения информационной безопасности и защиты информации; - место и роль информационной безопасности и защиты информации в области документооборота и архивного дела; методы и средства обеспечения информационной безопасности и защиты информации; **Уметь:** - разрабатывать комплекс мер по

			обеспечению информационной безопасности и защиты информации в сфере документооборота и архивного дела. **Владеть:** - навыками разработки документационного обеспечения информационной безопасности и защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Содержание дисциплины основывается и является логическим продолжением следующих дисциплин:

Наименование дисциплины (модуля)	Наименование разделов (тем)
Информационные технологии в публичной политике	все разделы

Содержание дисциплины служит основой для изучения следующих дисциплин:

Наименование дисциплины (модуля)	Наименование разделов (тем)
Государственная итоговая аттестация (6)	все разделы

3. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 3 зач. единиц, 108часов.

Вид учебной работы	Обозначение	Всего часов	Семестр № 8	Семестр № 9
Общая трудоемкость дисциплины, час		108		108
Аудиторные занятия, в т.ч.:		6	2	4
лекции	Л	4	2	2
лабораторные	ЛЗ			
практические	ПЗ	2		2
семинары	СЗ			
консультации	К			
Самостоятельная работа студентов, в том числе:	СРС	102	34	68
Курсовой проект	КП			
Курсовая работа	КР			
Расчетно-графические задания	РГЗ	18		18
Другие виды самостоятельной работы	ДВСР	84	34	50
Промежуточная аттестация (зачет)		зачет		зачет

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Наименование тем, их содержание и объем

Курс 4 Семестр 8

№ п/п	Наименование раздела (модуля)	К-во лекционных часов	Объем на тематический раздел час		
			Практич. и др. занятия	Лабораторные занятия	Самостоятельная работа
1	2	3	4	5	6
1	**Предмет, методология и понятийный аппарат курса.** Предмет информационной безопасности. Концепция информационной безопасности, важность и ценность информации, модели информационной безопасности, физические и программные каналы утечки информации, закладки и вирусы как средства атаки на информационные системы, парольная защита, аутентификация, разграничение прав доступа, способы закрытия информации и их значение. Аппаратные и программно-аппаратные средства защиты информационной безопасности.	1			17
2	**Разрушающие программные воздействия и средства несанкционированного доступа (НСД).** Технологии защиты от НСД. Защита операционных систем. Безопасность компьютерной сети. Закрытие информации шифрованием, финансовые применения и протоколы.	1			17
	Курс 5 Семестр 9				
3	**Инфраструктура открытых ключей. Защищенные протоколы.** Краткая история развития криптологии. Основные понятия и определения. Подстановочные и перестановочные шифры. Американский стандарт шифрования DES: алгоритм, скорость работы на различных платформах, режимы пользования, основные результаты по анализу стойкости. Отечественный стандарт шифрования данных ГОСТ 28147-89: алгоритм, скорость работы на различных платформах, режимы пользования. Асимметричные системы шифрования (системы с открытым ключом).	0,5	0,5		17
4	**Межсетевые экраны, классы их защищенности.** Политика безопасности и стратегия создания брандмауэра. Режим функционирования межсетевых экранов и их	0,5	0,5		17

	основные компоненты. Маршрутизаторы. Шлюзы сетевого уровня. Усиленная аутентификация. Основные схемы сетевой защиты на базе межсетевых экранов. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Программные методы защиты.				
5	**Обнаружение атак в глобальных сетях.** Виртуальные сети и прозрачные сетевые службы. Построение защищенных ВЧС. Многоуровневая защита информации в компьютерных системах и сетях.	0,5	0,5		17
6	**Информационная безопасность банковских систем и систем электронной коммерции.** Общие сведения об электронной цифровой подписи (ЭЦП). Алгоритм ЭЦП в симметричной криптосистеме. Алгоритм ЭЦП в асимметричной криптосистеме. Проблема обмена открытыми ключами при ЭЦП. Сложные математические задачи и алгоритмы ЭЦП с открытыми ключами. Алгоритм DSA. Алгоритм ГОСТ Р34.10–94. Стандарт ЭЦП Р34.10–2001.	0,5	0,5		17
	ВСЕГО	**4**	**2**		**102**

4.2. Содержание практических занятий

№ п/п	Наименование раздела дисциплины	Тема практического (лабораторного) занятия	К-во часов	К-во часов СРС
семестр №9				
1	Инфраструктура открытых ключей. Защищенные протоколы.	Современные приложения криптографии	0,15	5
		Изучение ППП систем криптографической защиты информации, классическая криптография и распределение ключей	0,15	5
		Практическое применение криптографии с открытым ключом. Пакет PGP	0,2	7
2	Межсетевые экраны, классы их защищенности.	Методы аутентификации	0,5	17
3	Обнаружение атак в глобальных сетях	Основные технологии построения защищенных ЭИС	0,5	17

4	Информационная безопасность банковских систем и систем электронной коммерции	Федеральный закон «Об электронной цифровой подписи». Электронная цифровая подпись (ЭЦП)	0,25	7
		Криптосистема операционной системы Windows. CryptoAPI: шифрование и дешифрование в CryptoAPI, ЭЦП в проектах на CryptoAPI	0,25	10
		ИТОГО:	2	68
			ВСЕГО:	70

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

5.1. Перечень контрольных вопросов (типовых заданий)

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
1	Предмет, методология и понятийный аппарат курса.	1.Место информационной безопасности экономических систем в национальной безопасности страны. Информационная безопасность в условиях функционирования в России глобальных сетей. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Международные стандарты информационного обмена. 2.Основные положения теории информационной безопасности информационных систем. Конфиденциальность. Целостность. Доступность. 3.Основные положения теории информационной безопасности информационных систем. Объект и субъект доступа. Средство работы с информацией. Несанкционированный доступ к информации. 4.Основные положения теории информационной безопасности информационных систем. Идентификация. Аутентификация. 5.Основные положения теории информационной безопасности информационных систем. Принципы распределения прав и ответственности. 6.Модели безопасности и их применение. Модели доступа. Решетчатая модель. Модель Белл-ЛаПадула. Модель безопасности. 7.Модели безопасности и их применение. Модели доступа. Модель Биба. Модель Гогена-Мезигера. Модель безопасности. 8.Модели безопасности и их применение. Модели

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		доступа. Модель Сазерленда. Модель Кларка-Вильсона. Модель безопасности. 9.Модели безопасности и их применение. Модели доступа. Обязательное управление доступом и переназначаемое управление доступом Доступ по правилам и доступ по ролям. Модель безопасности. 10.Таксономия (классификация) нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Три вида возможных нарушений информационной системы. Нарушения конфиденциальности. 11.Таксономия (классификация) нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Три вида возможных нарушений информационной системы. Изменения в системе. 12.Таксономия (классификация) нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Три вида возможных нарушений информационной системы. Утрата работоспособности или производительности.
2	Разрушающие программные воздействия и средства несанкционированного доступа (НСД)	13.Анализ способов нарушений информационной безопасности. Виды противников или "нарушителей". Источники и мотивы нарушений. Непреднамеренные действия сотрудников. 14.Анализ способов нарушений информационной безопасности. Виды противников или "нарушителей". Источники и мотивы нарушений. Преднамеренные действия сотрудников. 15.Анализ способов нарушений информационной безопасности. Виды противников или "нарушителей". Источники и мотивы нарушений. Действия сторонних лиц криминального характера. 16.Понятие угрозы. Классификация угроз информационной безопасности. Угрозы, не зависящие от человека. 17.Понятие угрозы. Классификация угроз информационной безопасности. Искусственные угрозы. 18.Понятие угрозы. Классификация угроз информационной безопасности. Угрозы информационной безопасности от использования специальных средств. 19.Атака. Локальная и удаленная атака. Хакер. Кракер. Фрикер. 20.Типовая атака на систему. 21.Локальные атаки. Социальная инженерия. 22.Закладки в аппаратном обеспечении. 23.Преодоление ограничений доступа на уровне firmware. 24.Получение доступа на этапе загрузки ОС.
3	Инфраструктура открытых ключей.	25. Методы криптографии. Основные принципы криптографии. Шифрование. История тайнописи.

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
	Защищенные протоколы.	Исторические пример. Шифр Цезаря. Привести пример. 26. Методы криптографии. Основные принципы криптографии. Шифрование. История тайнописи. Исторические пример. Квадрат Полибия (тюремная азбука). Привести пример. 27. Методы криптографии. Основные принципы криптографии. Шифрование. История тайнописи. Исторические пример. Квадрат Кардано. Привести пример. 28. Методы криптографии. Основные принципы криптографии. Шифрование. История тайнописи. Исторические примеры. Таблица Виженера. Многоалфавитная замена. Привести пример. 29. Методы криптографии. Основные принципы криптографии. Шифрование. История тайнописи. Исторические примеры. Шифрование по книге. Привести пример. 30. Методы криптографии. Практически стойкий шифр. Абсолютная стойкость шифра. Атака на основе шифротекста, на основе известного открытого текста, на основе выбранного открытого текста. Надежный шифр. 31. Методы криптографии. Поточное шифрование. Исключающее ИЛИ (сложение по модулю 2). 32. Методы криптографии. Линейные регистры сдвига. Привести пример. 33. Методы криптографии. Блочное шифрование. 34. Методы криптографии. Симметричное шифрование (шифрование на секретном ключе). Асимметричное шифрование (шифрование на открытом ключе). 35. Методы криптографии. Электронная цифровая подпись. 36.Методы криптографии. Хэш-функция в электронной цифровой подписи.
4	Межсетевые экраны, классы их защищенности.	37.Защита. Использование защищенных компьютерных систем. Механизмы защиты. Нормативно-правовые, морально-этические, организационные и физические (технические) средства защиты. 38.Основные технологии построения защищенных ЭИС. Контроль жизненного цикла программного обеспечения с точки зрения информационной безопасности. Мероприятия, осуществляемые при создании ИС. Сертификация программного обеспечения. 39.Основные технологии построения защищенных ЭИС. Контроль жизненного цикла программного обеспечения с точки зрения информационной безопасности. Мероприятия, осуществляемые в процессе эксплуатации ИС. 40.Концепция информационной безопасности. Концепция информационной безопасности предприятия. Управления рисками. Политика информационной

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		безопасности. 41.Защита. Механизмы защиты. Физические средства защиты. 42.Аппаратно-программные средства защиты. Системы идентификации и аутентификации пользователей. Системы шифрования дисковых данных. 43.Аппаратно-программные средства защиты. Системы аутентификации электронных данных. 44.Аппаратно-программные средства защиты. Средства управления криптографическими ключами.
5	Обнаружение атак в глобальных сетях	45.Атаки на средства аутентификации. Биометрические средства аутентификации. 46.Атаки на средства аутентификации. Токены. 47.Атаки на средства аутентификации. Пароли. Способы хранения паролей Системной политики паролей 48.Атаки на средства аутентификации. Пароли. Имитация системного приглашения Атака на слабость паролей. 49.Атаки класса "повышение привилегий". 50.Постороннее программное обеспечение. 51.Удаленные атаки. Зловредные программы. 52.Понятия о видах вирусов. 53.Удаленные атаки. Атаки на отказ в обслуживании. Маскировка. 54.Удаленные атаки. Атаки на маршрутизацию. Переполнение буфера. 55.Удаленные атаки. Атаки на севрверы: *CGI* и *HTTP*. Атаки на клиентов: *ActiveX, Java*. 56.Удаленные атаки. Атаки на поток данных. Активные атаки. Атака повтором. 57.Атака "злоумышленник-посредник". Атаки на основе сетевой маршрутизации. Перехват сессии.
6	Информационная безопасность банковских систем и систем электронной коммерции	58.Информационная безопасность при подключении к Internet. Межсетевые экраны. 59.Информационная безопасность при подключении к Internet. Управляемые коммутаторы. 60.Информационная безопасность при подключении к Internet. Сетевые фильтры. 61.Информационная безопасность при подключении к Internet. Шлюзы сеансового уровня. Посредники прикладного уровня. 62.Информационная безопасность при подключении к Internet. Инспекторы состояния.

5.2. Перечень тем курсовых проектов, курсовых работ, их краткое содержание и объем

Курсовая работа не предусмотрена учебным планом по направлению.

5.3. Перечень расчетно-графических заданий

Успешное выполнение РГЗ во многом зависит от четкого соблюдения установленных сроков и последовательного выполнения отдельных этапов работы:

1. Выбор темы не позднее, чем за 2 месяца до сдачи работы

2. Подбор научной литературы

3. Написание и представление преподавателю работы не позднее, чем за 7 дней до ее сдачи.

Оформление работы

Текстовый материал в работе должен быть изложен согласно правилам оформления студенческих работ.

Объем расчетно-графического задания 15-25 стр.

Структура и содержание РГЗ

Структура работы состоит из следующих частей:

- Введение
- Раздел 1. Теоретические основы изучаемой проблемы
- Раздел 2. Анализ рассматриваемой проблемы на конкретном примере
- Заключение
- Список литературы

В работе следует отразить вопросы, касающиеся рассматриваемой проблемы, в соответствии с приведенным ниже содержанием.

Введение. Во вступительной части рассматриваются основные тенденции изучения и развития проблемы, обосновывается актуальность проблемы, а также формируются цель и задачи работы.

Раздел 1. Теоретические основы изучения проблемы. В данном разделе, прежде всего, необходимо охарактеризовать объект и предмет исследования. Затем оценить степень изученности данной проблемы в научной литературе и привести различные точки зрения по данному вопросу. В процессе изучения имеющихся литературных источников по исследуемой проблеме очень важно найти сходство и различия точек зрения разных авторов, дать их анализ и обосновать свою позицию по данному вопросу.

Раздел 2. Анализ рассматриваемой проблемы на конкретном примере

При выполнении этой части работы студенты должны провести анализ состояния дел по данному вопросу, дать характеристику имеющимся особенностям и высказать свое мнение для их корректировки в случае необходимости.

Заключение

В заключении должны быть приведены основные выводы, вытекающие из результатов проведенного исследования.

Порядок выбора темы

Выбор темы определяется в соответствии со следующей схемой.

Номер темы РГЗ выбирается в зависимости от номера фамилии студента в журнале группы.

Порядок проверки и защиты РГЗ

Задание представляется преподавателю на проверку не позднее, чем за 7 дней до ее сдачи.

Ознакомившись с работой, преподаватель принимает решение о форме ее приема. Задание либо зачитывается, либо назначается время сдачи.

Замечания о необходимости доработок содержания оформляются преподавателем на титульном листе. Защита предполагает краткий доклад по ключевым вопросам.

Если работа не представлена в срок, то ее сдача производится комиссии, назначаемой зав. кафедрой.

Темы РГЗ

1. Доктрина информационной безопасности РФ.
2. Информационное обеспечение государственной политики РФ.
3. Развитие современных информационных технологий.
4. Угрозы информационной безопасности РФ.
5. Информационно-психологическое оружие.

6. Информационо-психологическая война.

7. Защита информационных ресурсов от несанкционированного доступа.

8. Информационный терроризм.

9. Международное сотрудничество РФ в области защиты информации.

10. Государственная тайна.

11. Служебная тайна.

12. Коммерческая тайна.

13. Персональные данные.

14. Личная тайна.

15. Семейная тайна.

16. Тайна ЗАГСа.

17. Врачебная (медицинская) тайна.

18. Тайна вероисповедания.

19. Тайна исповеди.

20. Адвокатская тайна.

21. Тайна следствия.

22. Судебная тайна.

23. Тайна нотариата.

24. Налоговая тайна.

25. Банковская тайна.

26. Журналистская тайна (тайна СМИ).

27. Авторское право.

5.4. Перечень контрольных работ

Контрольные работы не предусмотрены учебным планом по направлению.

6. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

6.1. Перечень основной литературы

1. Башлы П.Н. Информационная безопасность: учебно-практическое пособие / Башлы П.Н., Бабаш А.В., Баранова Е.К. - М.: Изд. центр ЕАОИ, 2011. - 376 с. http://www.biblioclub.ru/book/90539/
2. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: http://www.iprbookshop.ru/10677.html.— ЭБС «IPRbooks»
3. Креопалов В. В. Технические средства и методы защиты информации: учебно-практическое пособие / В.В. Креопалов. - М.: Изд. центр ЕАОИ, 2011.- 278 с. http://www.biblioclub.ru/book/90753/
4. Ярочкин В.И. Информационная безопасность [Электронный ресурс]: учебник для вузов/ Ярочкин В.И.— Электрон. текстовые данные.— М.: Академический Проект, 2008.— 544 с.— Режим доступа: http://www.iprbookshop.ru/36331.html.— ЭБС «IPRbooks»

6.2. Перечень дополнительной литературы

1. Гвоздева В.А. Информационные технологии в юридической деятельности [Электронный ресурс]: курс лекций/ Гвоздева В.А.— Электрон. текстовые данные.— М.: Московская государственная академия водного транспорта, 2013.— 87 с.— Режим доступа: http://www.iprbookshop.ru/47934.html.— ЭБС «IPRbooks»

6.3. Перечень интернет ресурсов

1. http:// www.consultantplus.ru/ - нормативно-правовая база
2. http://www.garant.ru/ - нормативно-правовая база
3. http://www.promo.s-director.ru/ – сайт журнала «Директор по безопасности»
4. http://college.ru/UDP/texts/ – учебный курс «Защита информации»;
5. http://www.mirash.ru/doki11.html - нормативная база по защите информации;
6. http://tk.plexor.ru/web-links/info/38-zakon.html - нормативные документы по защите информации.
7. http://www.inattack.ru/ - антивирусное программное обеспечение
8. http://securityvulns.ru/ - нормативные документы по защите информации
9. http://www.glossary.ru/cgi-bin/gl_sch2.cgi?RIt(uwsg.outtg9!hlnuvgxtuxy
10. http://www.gosecure.ru/ - сайт форматов ЭЦП
11. http://z-oleg.com/ - антивирусное программное обеспечение
12. http://www.aladdin.ru/ - сайт производителя средств защиты информации

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

Реализация данной учебной дисциплины осуществляется с использованием материально-технической базы, обеспечивающей проведение всех видов учебных занятий и научно-исследовательской работы обучающихся, предусмотренных программой учебной дисциплины и соответствующей действующим санитарным и противопожарным правилам и нормам:

- оборудованные кабинеты и аудитории;
- компьютерные классы;
- аудитории, оборудованные мультимедийными средствами обучения.

Лекционные занятия – аудитория, оснащенная презентационной техникой, комплект электронных презентаций.

Лабораторные занятия – компьютерные классы с установленным специализированным лицензионным программным обеспечением.

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Утверждение рабочей программы без изменений

Рабочая программа без изменений утверждена на 2017 /2018 учебный год.

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

Заведующий кафедрой_____Селиверстов Ю.И.

подпись, ФИО

Директор института _____Дорошенко Ю.А.

подпись, ФИО

Утверждение рабочей программы без изменений

Рабочая программа без изменений утверждена на 2018 /2019 учебный год.

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

Заведующий кафедрой_____Селиверстов Ю.И.

подпись, ФИО

Директор института _____Дорошенко Ю.А._

подпись, ФИО

Утверждение рабочей программы без изменений

Рабочая программа без изменений утверждена на 2019 /2020 учебный год.

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

Заведующий кафедрой_____Селиверстов Ю.И.

подпись, ФИО

Директор института _____Дорошенко Ю.А._

подпись, ФИО

Утверждение рабочей программы без изменений

Рабочая программа без изменений утверждена на 2020 /2021 учебный год.

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

Заведующий кафедрой_____Селиверстов Ю.И.

подпись, ФИО

Директор института _____Дорошенко Ю.А._

подпись, ФИО