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)

УТВЕРЖДАЮ
Директор института
экономики и менеджмента
_____ Дорошенко Ю.А.
«23» января 2017 г.

РАБОЧАЯ ПРОГРАММА
дисциплины

Информационная безопасность

направление:
41.03.06 Публичная политика и социальные науки

профиль подготовки:
Публичная политика в социально-экономической сфере

Степень
Бакалавр

Форма обучения
Очная

Институт: _____экономики и менеджмента_____

Кафедра:_____экономики и организации производства____

Белгород – 2017

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта высшего образования 41.03.06 «Публичная политика и социальные науки» (уровень бакалавриата), утвержденного Приказом Министерства образования и науки РФ от 20 октября 2015 г. № 1174;
- плана учебного процесса БГТУ им. В.Г. Шухова, введенного в действие в 2017 году;

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

Рабочая программа согласована с выпускающей кафедрой
Теории и методологии науки
(название кафедры)

Заведующий кафедрой д.э.н., профессор (Чижова Е.Н.)
(подпись) (ФИО)

«11» 01 2017 г.

Рабочая программа обсуждена на заседании кафедры
экономики и организации производства
(наименование кафедры)

«11» января 2017 г., протокол № 5

Заведующий кафедрой д.э.н., профессор (Ю.И. Селиверстов)
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа одобрена методической комиссией института
института экономики и менеджмента
(наименование института)

«26» 01 2017 г., протокол № 5

Председатель к.э.н., профессор (В.В. Выборнова)
(ученая степень и звание, подпись) (инициалы, фамилия)

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, в том числе защиты государственной тайны. **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 опасности и 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	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;

		информационной безопасности	**Уметь:** - разрабатывать комплекс мер по обеспечению информационной безопасности и защиты информации в сфере документооборота и архивного дела и при решении стандартных задач профессиональной деятельности. **Владеть:** - навыками разработки документационного обеспечения информационной безопасности и защиты информации при решении стандартных задач профессиональной деятельности

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Содержание дисциплины основывается и является логическим продолжением следующих дисциплин:

Наименование дисциплины (модуля)
1. Информационные технологии в публичной политике

Содержание дисциплины служит основой для изучения следующих дисциплин:

Наименование дисциплины (модуля)
1. Учебная практика

3. ОБЪЕМ ДИСЦИПЛИНЫ

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

Вид учебной работы	Всего часов	Семестр № 7
Общая трудоемкость дисциплины, час	108	108
Контактная работа (аудиторные занятия), в т.ч.:	51	51
лекции	34	34
лабораторные	17	17
практические		
Самостоятельная работа студентов, в том числе:	57	57
Курсовой проект		
Курсовая работа		
Расчетно-графические задания	18	18
Индивидуальное домашнее задание (ИДЗ)		
Рефераты		
Другие виды самостоятельной работы	39	39
Промежуточная аттестация (зачет, экзамен)	зачет	зачет

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Наименование тем, их содержание и объем

Курс 4 Семестр 7

№ 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.	6		3	6
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.	4		2	6
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).	4		3	6
4	**Межсетевые экраны, классы их защищенности.** Политика безопасности и стратегия создания брандмауэра. Режим функционирования межсетевых экранов и их основные компоненты. Маршрутизаторы.	8		3	6

	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.	6		3	8
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.	6		3	7
	ВСЕГО	**34**		**17**	**39**

4.2. Содержание лабораторных занятий

№ п/п	Наименование раздела дисциплины	Тема практического (лабораторного) занятия	К-во часов	К-во часов СРС
семестр №9				
1	Предмет, методология и понятийный аппарат курса.	Федеральный закон «Об информации, информатизации и защите информации». Методы оценки уязвимости информации	1	2
		Место информационной безопасности ЭИС в национальной безопасности страны. Концепция информационной безопасности.	2	2
2	Разрушающие программные воздействия и средства несанкционированного доступа (НСД)	Комплексная система обеспечения информационной безопасности.	2	2
3	Инфраструктура открытых ключей. Защищенные протоколы.	Современные приложения криптографии	1	1
		Изучение ППП систем криптографической защиты информации, классическая криптография и распределение ключей	1	1

		Практическое применение криптографии с открытым ключом. Пакет PGP	1	2
4	Межсетевые экраны, классы их защищенности.	Методы аутентификации	3	4
5	Обнаружение атак в глобальных сетях	Основные технологии построения защищенных ЭИС	3	4
6	Информационная безопасность банковских систем и систем электронной коммерции	Федеральный закон «Об электронной цифровой подписи». Электронная цифровая подпись (ЭЦП)	1	2
		Криптосистема операционной системы Windows. CryptoAPI: шифрование и дешифрование в CryptoAPI, ЭЦП в проектах на CryptoAPI	2	2
		ИТОГО:	17	22

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

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		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 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.

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		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. Защищенные протоколы.	25. Методы криптографии. Основные принципы криптографии. Шифрование. История тайнописи. 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

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		точки зрения информационной безопасности. Мероприятия, осуществляемые в процессе эксплуатации ИС. 40.Концепция информационной безопасности. Концепция информационной безопасности предприятия. Управления рисками. Политика информационной 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

Не предусмотрены 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. Компания занимается розничной торговлей мультимедийной продукцией
2. Компания занимается оказанием логистических услуг
3. Компания занимается учебной деятельностью
4. Компания занимается производством мебели
5. Компания является туроператором
6. Компания занимается оказанием услуг в сфере здравоохранения деятельностью
7. Компания разрабатывает средства защиты информации
8. Компания занимается изготовлением полиграфической продукции
9. Компания оказывает услуги по инкассации торговых объектов
10. Компания занимается разработкой и сопровождением отраслевого программного обеспечения
11. Компания занимается кинопрокатом фильмов
12. Компания занимается книгоизданием
13. Компания занимается выпуском журналов (Издательский дом)
14. Компания осуществляет подключение к сети Интернет и IP телефонии
15. Компания занимается разработкой и администрированием веб-сайтов
16. Компания занимается изготовлением POS терминалов
17. Компания занимается бронированием гостиниц по России
18. Компания занимается бронированием и доставкой железнодорожных и авиабилетов.
19. Компания занимается локализацией программных продуктов
20. Компания занимается тиражированием оптических дисков

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 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.
2. Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] : учебник / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 474 с. — Режим доступа: https://e.lanbook.com/book/39990.
3. Теплов, Э.П. Гуманитарные аспекты информационной безопасности: основные понятия, логические основы и операции [Электронный ресурс]: учебное пособие / Э.П. Теплов, Ю.А. Гатчин, А.П. Нырков, А.Г. Коробейников. — Электрон. дан. — Санкт-Петербург: НИУ ИТМО, 2016. — 122 с. — Режим доступа: https://e.lanbook.com/book/91401.
4. Фаронов, А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс]: учебное пособие / А.Е. Фаронов. — Электрон. дан. — Москва, 2016. — 154 с. — Режим доступа: https://e.lanbook.com/book/100296

6.2. Перечень дополнительной литературы

1. Всеобщая декларация прав человека (от 10 декабря 1948 г.). М., 2015.
2. Конституция РФ. М., 2015.
3. Гражданский кодекс РФ. М., 2015.
4. Доктрина информационной безопасности РФ. М., 2015.
5. Федеральный закон «О государственной тайне» от 21 июля 1993 г. № 5485-1. М., 1993.

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 – Учебная аудитория для проведения лекционных занятий.

Практические занятия – специализированная аудитория, оснащенная специализированной мебелью, мультимедийным проектором, переносным экраном, ноутбуком

Лабораторные занятия – компьютерные классы с установленным специализированным лицензионным программным обеспечением: Microsoft Office Professional 2013 Лицензионный договор № 31401445414 от 25.09.2014. Google Chrome Свободно распространяемое ПО согласно условиям лицензионного соглашения. Kaspersky Endpoint Center 10 Лицензионный договор № 17E0170707130320867250

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Рабочая программа без изменений утверждена на 2017/2018 учебный год.
Протокол № 5 заседания кафедры от «11» января 2017 г.

Заведующий кафедрой _____/Ю.И. Селиверстов/

Директор института _____/Ю.А. Дорошенко/

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Рабочая программа без изменений утверждена на 2018/2019 учебный год.
Протокол № 9 заседания кафедры от «21» мая 2018 г.

Заведующий кафедрой _____/Ю.И. Селиверстов/

Директор института _____/Ю.А. Дорошенко/