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 обучения
_____ Нестеров М.Н.
«13» 03 2017 г.

УТВЕРЖДАЮ
Директор института
экономики и менеджмента
_____ Дорошенко Ю.А.
«13» марта 2017 г.

РАБОЧАЯ ПРОГРАММА
дисциплины

Информационная безопасность

специальность:
38.05.01 Экономическая безопасность

специализация
Экономико-правовое обеспечение экономической безопасности

Квалификация
экономист

Форма обучения
заочная

Институт: **экономики и менеджмента**

Кафедра: **экономики и организации производства**

Белгород – 2017

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта высшего профессионального образования по специальности 38.05.01за «Экономическая безопасность» (уровень специалитета), утвержденного приказом Министерства образования и науки Российской Федерации от 16 января 2017 г № 20;
- 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
стратегического управления
(название кафедры)

Заведующий кафедрой д.э.н., профессор (Дорошенко Ю.А.)
(подпись) (ФИО)

«02» марта 2017 г.

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

«01» 03 2017 г., протокол № 6/1

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)

«10» марта 2017 г., протокол № 7

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	
Общепрофессиональные			
1	ОК-12	Способность работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации.	В результате освоения дисциплины обучающийся должен **Знать:** - основные понятия и направления в защите компьютерной информации, принципы защиты информации; - принципы классификации и примеры угроз безопасности компьютерным системам, современные подходы к защите продуктов и систем информационных технологий, реализованные в действующих отечественных и международных стандартах ИТ-безопасности; - состояние и правовые основы информационной безопасности РФ, правовые гарантии информационной безопасности личности; - основные инструменты обеспечения многоуровневой безопасности в информационных системах. **Уметь:** - конфигурировать встроенные средства безопасности в операционной системе, проводить анализ защищенности компьютера и сетевой среды с использованием сканера безопасности; - устанавливать и использовать одно из средств для шифрования информации и организации обмена данными с использованием электронной цифровой подписи; устанавливать и использовать один из межсетевых экранов; - устанавливать и настраивать программное обеспечение для защиты от вредоносного программного обеспечения; - настроить инструменты резервного копирования и восстановления информации. **Владеть:** - методами аудита безопасности информационных систем, методами системного анализа информационных систем; - методами защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Содержание дисциплины основывается и является логическим продолжением следующих дисциплин:

№	Наименование разделов (тем)
1	Информационные ресурсы и технологии в экономике

Содержание дисциплины служит основой для изучения следующих дисциплин:

№	Наименование разделов (тем)
1	Документирование управленческой деятельности
2	Методы принятия управленческих решений

3. ОБЪЕМ ДИСЦИПЛИНЫ

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

Вид учебной работы	Всего часов	Семестр № 8	Семестр № 9
Общая трудоемкость дисциплины, час	180	4	176
Контактная работа (аудиторные занятия), в т. ч.:	18	2	16
лекции	6	2	4
лабораторные	12		12
практические			
Самостоятельная работа студентов, в том числе:	162	2	160
Курсовой проект			
Курсовая работа			
Расчетно-графические задания	18		18
Индивидуальное домашнее задание (ИДЗ)			
Рефераты			
Другие виды самостоятельной работы	108	2	106
Промежуточная аттестация (экзамен)	36		36

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Наименование тем, их содержание и объем

Курс 4 Семестр 9

№ 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		2	16
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		2	16
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).	1		2	18
4	**Межсетевые экраны, классы их защищенности.** Политика безопасности и стратегия создания брандмауэра. Режим	1		2	18

	функционирования межсетевых экранов и их 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.	1		2	18
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.	1		2	20
	ВСЕГО	**6**		**12**	**106**

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	8
		Место информационной безопасности ЭИС в национальной безопасности страны. Концепция информационной безопасности.	1	10
2	Разрушающие программные воздействия и средства несанкционированного доступа (НСД)	Комплексная система обеспечения информационной безопасности.	2	17
3	Инфраструктура открытых ключей. Защищенные протоколы.	Современные приложения криптографии	1	6
		Изучение ППП систем криптографической защиты информации, классическая	0,5	6

		криптография и распределение ключей		
		Практическое применение криптографии с открытым ключом. Пакет PGP	0,5	6
4	Межсетевые экраны, классы их защищенности.	Методы аутентификации	2	17
5	Обнаружение атак в глобальных сетях	Основные технологии построения защищенных ЭИС	2	17
6	Информационная безопасность банковских систем и систем электронной коммерции	Федеральный закон «Об электронной цифровой подписи». Электронная цифровая подпись (ЭЦП)	1	9
		Криптосистема операционной системы Windows. CryptoAPI: шифрование и дешифрование в CryptoAPI, ЭЦП в проектах на CryptoAPI	1	9
ИТОГО:			12	105
ВСЕГО:				117

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.

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

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

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

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		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 заданя 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. Информациоино-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. Всеобщая декларация прав человека (от 10 декабря 1948 г.). М., 2010.
2. Конституция РФ. М., 2010.
3. Гражданский кодекс РФ. М., 2010.
4. Доктрина информационной безопасности РФ. М., 2010.
5. Федеральный закон «О государственной тайне» от 21 июля 1993 г. № 5485-1. М., 1993.
6. Федеральный закон «Об авторском праве и смежных правах» от 9 июля 1993 г. № 5351-1 (с последующими изменениями). М., 1993.
7. Федеральный закон «Об электронной цифровой подписи» от 10 января 2002 г. № 1-ФЗ. М., 2002.
8. 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/
9. Емельянов Г.В., Стрельцов А.А. Информационная безопасность России. Основные понятия и определения. М., 2010.

10. Куняев Н.Н. Правовое обеспечение национальных интересов Российской Федерации и информационной сфере / Н.Н. Куняев. — М.: Логос, 2010. - 348 с. http://www.biblioclub.ru/book/84990/
11. 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/
12. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации [Текст] : учеб. пособие для студентов вузов по спец. 230201 "Информ. системы и технологии" / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова - М. : Академия, 2008 .- 336 с.
13. Петров В. П., Петров С. В. Информационная безопасность человека и общества: учебное пособие /В. П. Петров, С. В. Петров. - М.: ЭНАС,2007. - 336 с. http://www.biblioclub.ru/book/42835/

6.2. Перечень дополнительной литературы

1. Алешенков М. Основы национальной безопасности/М.Алешенков /Основы безопасности жизни.-2005.-№11.-С.5-10. [текст]
2. Алферов А. П. и др. Основы криптографии. М., Гелиос-АРВ, 2002. [текст]
3. Андреев Э. М., Миронов А.В. Социальные проблемы интеллектуальной уязвимости и информационной безопасности //Социально-гуманитарные знания.-2000.-№4.-С.169-180. [текст]
4. Брандман Э. М. Глобализация и информационная безопасность общества/Э.М.Брандман //Философия и общество.-2006.-№1.-С.31-41. [текст]
5. Брандман Э. М. Цивилизационные императивы и приоритеты информационной безопасности общества/Э.М.Брандман //Философия и общество.-2006.-№3.-С.60-77..-Предпринимательство, с.131-144. [текст]

6. Доктрина информационной безопасности //Средства массовой информации постсоветской России: Учеб. пособие /Я.Н. Засурский, Е. Л. Вартанова, И.И. Засурский.-М., 2002.-С.262-301. [текст]
7. Егозина В. Смотреть нельзя запретить (агрессивная информационная среда как угроза для безопасности)/В. Егозина, Н. Овчинников //ОБЖ.-2003.-№4.-С.15-18. [текст]
8. Еляков А.Д. Информационная свобода человека/А.Д.Еляков // Социально-гуманитарные знания.-2005.-№3.-С.125-141. [текст]
9. Кузнецов А. Двоичная тайнопись (по материалам открытой печати)/ А. Кузнецов //Компьютер пресс.-2004.-№4/апрель/.-С.38. [текст]
10. Козье Д.. Электронная коммерция. М., «Русская редакция», 1999г. [текст]
11. Лукацкий А. Технологии информационной безопасности вчера и сегодня (тема номера)/А. Лукацкий //Компьютер пресс.-2004.-№4/апрель/.- С.8. [текст]
12. Мамаев С.М., Петренко.Технологии защиты информации в Интернете. Санкт-Петрбург, Изд-во «ПИТЕР». Москва-Харьков-Минск. 2002г.[текст]
13. Морозов И. Л. Информационная безопасность политической системы / И.Л.Морозов //ПОЛИС.-2002.-№5.-С.134-146. [текст]
14. Норткат С., Новак Д.- Обнаружение нарушений безопасности в сетях. Изд-й дом Вильямс, 2003г. [текст]
15. Поляков В. П. Практическое занятие по изучению вопросов информационной безопасности/В.П.Поляков //Информатика и образование.- 2006.-№11.-С.75-80. [текст]
16. Поляков В.П. Информационная безопасность в курсе информатики /В.П.Поляков //Информатика и образование.-2006.-№10.-С.116-119.[текст]
17. Чмора А.. Современная прикладная криптография. М., Гелиос-АРВ, 2001г. [текст]

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 2018 /2019 учебный год.

Протокол № 9 заседания кафедры от « 21 » мая 2018 г.

Заведующий кафедрой _____

подпись, ФИО

Директор института _____

подпись, ФИО

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Утверждение рабочей программы без изменений

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

Протокол № 9/1 заседания кафедры от «13» 06 2019 г.

Заведующий кафедрой _____ Ю.И. Селиверстов
подпись, ФИО

Директор института _____ Ю.А. Дорошенко
подпись, ФИО

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Утверждение рабочей программы без изменений

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

Протокол № 8 заседания кафедры от «22» 05 2020 г.

Заведующий кафедрой _____ Ю.И. Селиверстов
подпись, ФИО

Директор института _____ Ю.А. Дорошенко
подпись, ФИО

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Утверждение рабочей программы

Рабочая программа с изменениями утверждена на 2019 /2020 учебный год.

Протокол № _____ заседания кафедры от «___» _____ 201 г.

3. ОБЪЕМ ДИСЦИПЛИНЫ

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

Вид учебной работы	Всего часов	Семестр № 7	Семестр № 8
Общая трудоемкость дисциплины, час	180	4	176
Контактная работа (аудиторные занятия), в т.ч.:	10	2	8
лекции	4	2	2
лабораторные	6		6
практические			
Самостоятельная работа студентов, в том числе:	170	2	168
Курсовой проект			
Курсовая работа			
Расчетно-графические задания	18		18
Индивидуальное домашнее задание			
Другие виды самостоятельной работы	116	2	114
Промежуточная аттестация (экзамен)	36		36

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Наименование тем, их содержание и объем

Курс 4 Семестр 8

№ п/п	Наименование раздела (модуля)	К-во лекцион-ных часов	Объем на тематический раздел час		
			Практич. и др. занятия	Лабораторные занятия	Самостоя-тельная 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	0,5		1	30

	информационные системы, парольная защита, аутентификация, разграничение прав доступа, способы закрытия информации и их значение. Аппаратные и программно-аппаратные средства защиты информационной безопасности.				
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.	0,5		1	30
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		1	30
4	**Межсетевые экраны, классы их защищенности.** Политика безопасности и стратегия создания брандмауэра. Режим функционирования межсетевых экранов и их 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.	1		1	30
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		1	30
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	1		1	20

	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.				
	ВСЕГО	4		6	170

4.2. Содержание лабораторных занятий

№ п/п	Наименование раздела дисциплины	Тема практического (лабораторного) занятия	К-во часов	К-во часов СРС
семестр №8				
1	Предмет, методология и понятийный аппарат курса.	Федеральный закон «Об информации, информатизации и защите информации». Методы оценки уязвимости информации	0,5	15
		Место информационной безопасности ЭИС в национальной безопасности страны. Концепция информационной безопасности.	0,5	15
2	Разрушающие программные воздействия и средства несанкционированного доступа (НСД)	Комплексная система обеспечения информационной безопасности.	1	30
3	Инфраструктура открытых ключей. Защищенные протоколы.	Современные приложения криптографии	0,25	10
		Изучение ППП систем криптографической защиты информации, классическая криптография и распределение ключей	0,5	10
		Практическое применение криптографии с открытым ключом. Пакет PGP	0,25	10
4	Межсетевые экраны, классы их защищенности.	Методы аутентификации	1	30
5	Обнаружение атак в глобальных сетях	Основные технологии построения защищенных ЭИС	1	30
6	Информационная безопасность банковских систем и систем электронной коммерции	Федеральный закон «Об электронной цифровой подписи». Электронная цифровая подпись (ЭЦП)	0,5	15
		Криптосистема операционной системы Windows. CryptoAPI: шифрование и дешифрование в	0,5	15

		CryptoAPI, ЭЦП в проектах на CryptoAPI		
			ИТОГО:	10	170
			ВСЕГО:		180

Заведующий кафедрой _____ Селиверстов Ю.И.

подпись, ФИО

Директор института _____ Дорошенко Ю.А.