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

СОГЛАСОВАНО	УТВЕРЖДАЮ
Директор института ЗО	Директор института ИТУС
_____ М.Н. Нестеров	_____ В.Г.Рубанов
«28» 04 2015 г.	«27» 04 2015 г.

РАБОЧАЯ ПРОГРАММА
дисциплины

Информационная безопасность

направление подготовки

09.03.02 Информационные системы и технологии

профиль программы

Информационные системы и технологии

Квалификация

бакалавр

Форма обучения

заочная

Институт: Информационных технологий и управляющих систем

Кафедра: Информационных технологий

Белгород – 2015

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.02 Информационные системы и технологии(уровень бакалавриата), утвержденного Приказом Министерства образования и науки Российской Федерации. от 12 марта 2015 г.N 219

- плана учебного процесса БГТУ им. В.Г. Шухова, введенного в действие в 2015 г.

Составитель: ст. преп. _____ (А.Г. Смышляев)

Рабочая программа обсуждена на заседании кафедры информационных технологий

«15»_____04_____2015 г., протокол № ____5_____

Зав. кафедрой:канд.техн. наук, доц._____ (И.В. Иванов)

Рабочая программа одобрена методической комиссией института ИТУС

«23»_____04_____2015 г., протокол № ____9/12_____

Председатель: доц. _____(Ю. И. Солопов)

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Формируемые компетенции			Требования к результатам обучения
№	Код компетенции	Компетенция	
Общепрофессиональные			
2	ПК-2	способность проводить техническое проектирование	В результате освоения дисциплины обучающийся должен **Знать:** – основные категории и аспекты информационной безопасности; – основные законодательные, процедурные, административные и программно-технические меры обеспечения информационной безопасности; – содержание основных отечественных и международных стандартов и спецификаций, действующих в области информационной безопасности; – основы построения криптосистем, а также средств создания и верификации электронных подписей и аутентификации; – особенности защиты распределенных информационных систем. **Уметь** – организовать процесс защиты информационных систем в соответствии с отечественными и международными стандартами в области информационной безопасности; – определить уязвимые места в защите информационной системы, выбрать необходимые и экономически обоснованные защитные мероприятия на административном, процедурном и программно-техническом уровнях обеспечения безопасности; – осуществлять программную реализацию наиболее распространенных криптоалгоритмов. **Владеть** – навыками применения криптографических пакетов и интерфейсов для построения подсистем информационной безопасности; – навыками адаптации и применения существующих систем защиты информации от несанкционированного доступа;

1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Содержание дисциплины основывается и является логическим продолжением следующих дисциплин:

№	Наименование дисциплины (модуля)
2	Информатика
3	Визуальное программирование
4	Информационные технологии

Содержание дисциплины служит основой для изучения следующих дисциплин:

№	Наименование дисциплины (модуля)
1	Отраслевые информационные системы
3	Методы и средства проектирования информационных систем и технологий

2. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 4 зач. единицы, 144 часов.

Вид учебной работы	Всего часов	Семестр № 7	Семестр № 8
Общая трудоемкость дисциплины, час	144	2	142
Контактная работа (аудиторные занятия), в т.ч.:	16	2	14
лекции	6	2	4
лабораторные	10		10
практические			
Самостоятельная работа студентов, в том числе:	128		128
Курсовой проект			
Курсовая работа			
Расчетно-графическое задание			
Индивидуальное домашнее задание	9		9
Другие виды самостоятельной работы	79		79
Форма промежуточная аттестация (зачет, экзамен)	Экзамен (40)		Экзамен (40)

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ
4.1 Наименование тем, их содержание и объем
Курс 3 Семестр 8

№ п/п	Наименование раздела (краткое содержание)	Объем на тематический раздел по видам учебной нагрузки, час			
		Лекции	Практические занятия	Лабораторные з анятия	Самостоятельная работа
1.	**Раздел 1. Основные аспекты информационной безопасности**				
	Понятие информационной безопасности. Основные категории информационной безопасности. Законодательные аспекты информационной безопасности. Анализ наиболее распространенных угроз и методов проникновения в информационные системы. Программное обеспечение, применяемое для проникновения в информационные системы и методы нейтрализации его воздействия.	0,5			2
2.	**Раздел 2. Криптографические средства защиты информации**				
	Основные понятия криптографии, терминология. Классификация криптоалгоритмов. Основные виды криптоаналитических атак. Законодательство РФ в области разработки и применения систем, содержащих элементы криптозащиты. Потоковые и блочные шифры. Принципы построения блочных шифров. Конструкции Фейстеля. Режимы работы блочных шифров. Криптоалгоритмы AES, ГОСТ 28147-89 и ГОСТ Р 34.12-2015. Основные принципы шифрования с открытым ключом. Области применения криптосистем с открытым ключом. Криптоалгоритм RSA. Управление ключами. Алгоритм Диффи-Хеллмана-Меркла.	2,5		7	45
3.	**Раздел 3. Стандарты информационной безопасности**				
	Основные понятия, вводимые стандартами и спецификациями. Руководящие документы Гостехкомиссии РФ. Нормативные документы ФСТЭК. Обзор наиболее значимых отечественных стандартов в области информационной безопасности: ИСО/МЭК 15408, серия стандартов ИСО/МЭК 27000.	0,5			2
4.	**Раздел 4. Электронная подпись и аутентификация**				
	Назначение функций хэширования и предъявляемые к ним требования. Обзор известных алгоритмов хэширования: MD5, SHA-1, 2, 3, ГОСТ Р 34.11-94, 2012. Требования к электронным подписям. Основные положения закона 63-ФЗ «Об электронной подписи». Характеристики алгоритмов создания и верификации электронных подписей: DSA, ECDSA, ГОСТ Р 34.10-94, 2001, 2012. Протоколы	1		3	24

	односторонней и двусторонней аутентификации на основе симметричного и асимметричного шифрования. Основные положения стандарта X.509. Структура сертификата открытого ключа, форматы хранения. Отзыв сертификатов. Общая схема аутентификации с использованием сертификатов X.509. Инфраструктуры открытых ключей.				
5.	**Раздел 5. Защита распределенных систем и корпоративных сетей**				
	Особенности протоколов защищенного обмена данными сетевого и транспортного уровня и их место в стеке протоколов TCP/IP. Обзор защищенных протоколов: IPSec, SSL, TLS. Атакуемые сетевые компоненты информационных систем. Классификация нарушителей сетевой безопасности информационных систем. Управление доступом. Методика обнаружения нарушителей. Протоколирование и аудит. Классификация вредоносных программ. Антивирусная защита. Основные характеристики и типы брандмауэров и систем обнаружения и предотвращения вторжений.	1			4
6.	**Раздел 6. Системы защиты электронной почты**				
	Назначение и принцип работы систем PGP и S/MIME.	0,5			2
	ВСЕГО	6		10	79

4.2. Содержание практических (семинарских) занятий

Не предусмотрено

4.3. Содержание лабораторных занятий

№ п/п	Наименование раздела дисциплины	Тема лабораторного занятия	К-во часов	К-во часов СРС
семестр № 6				
1	Криптографические средства защиты информации	Потоковое шифрование данных	2	8
2		Симметричное шифрование данных с использованием криптографических интерфейсов Microsoft CryptoAPI и Cryptography API: Next Generation	2	12
3		Симметричное и асимметричное шифрование данных средствами криптографического пакета OpenSSL	3	16
4	Электронная подпись и аутентификация	Создание криптографических сообщений с использованием интерфейса Microsoft CryptoAPI и цифровых сертификатов X.509	3	20
ИТОГО:			10	56
ВСЕГО:				66

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

5.1. Перечень контрольных вопросов (типовых заданий)

Контрольные вопросы для текущего контроля

1) Принципы работы потоковых шифров.
2) Какие операции используются при реализации потоковых шифров?
3) Что такое гамма шифра?
4) Что представляет собой регистр сдвига с линейной обратной связью?
5) Что такое отводная последовательность РСЛОС, и в какой форме ее можно представить?
6) Что такое период регистра сдвига?
7) Какие условия должны соблюдаться для того, чтобы РСЛОС имел максимальный период?
8) Что такое сеть Фейстеля? Каковы основные принципы работы блочных шифров, устроенных по принципу сети Фейстеля?
9) Назовите все режимы шифрования, определенные в ГОСТ 28147-89.
10) Каковы разрядности блока и ключа в алгоритме ГОСТ 28147-89?
11) Что представляют собой таблицы замен (S-блоки) в алгоритме ГОСТ 28147-89?
12) Что представляет собой один раунд (основной шаг) алгоритма ГОСТ 28147-89?
13) Как может производиться дополнение неполных блоков в режиме простой замены?
14) Каковы недостатки режима простой замены?
15) Что собой представляет режим гаммирования?
16) Что собой представляет режим гаммирования с обратной связью?
17) Как функционирует схема зашифрования алгоритма ГОСТ 28147-89?
18) Как функционирует схема расшифрования алгоритма ГОСТ 28147-89?
19) Что такое синхропосылка?
20) Что такое CryptoAPI? В чем заключается различие между CryptoAPI 1.0 и CryptoAPI 2.0?
21) Что такое криптопровайдер? Как можно подключиться к криптопровайдеру?
22) Какое количество функций должен поддерживать криптопровайдер?
23) Как создать контейнер ключей? Какие типы ключей в нем будут храниться?
24) Какие типы криптопровайдеров вы знаете? Чем они различаются?
25) Как можно выполнить генерацию ключа симметричного шифрования?
26) Какой режим шифрования устанавливается при генерации ключа по умолчанию?
27) Что такое хэш-объект? Какие функции для работы с хэш-объектами вы знаете?
28) Какие функции CryptoAPI выполняют зашифрование и расшифрование данных? Какие они имеют параметры?
29) Что такое Cryptography API: Next Generation? В чем заключаются его различия с CryptoAPI?
30) Какие типы провайдеров CNG доступны в операционных системах Windows? Как можно узнать, какие конкретно провайдеры установлены в системе?

31) Средства каких провайдеров CNG можно использовать в режиме ядра?
32) Как определить успешность вызова функции CNG?
33) Как сгенерировать ключ симметричного шифрования и установить его параметры?
34) Какие функции CNG выполняют зашифрование и расшифрование данных? Какие они имеют параметры?
35) Для чего используется криптографический пакет OpenSSL?
36) Как установить и сконфигурировать пакет OpenSSL.
37) Что собой представляет тип BIO? Какие его разновидности вы знаете?
38) Какими средствами в пакете OpenSSL можно осуществлять генерацию псевдослучайных чисел?
39) Какие функции и типы данных, необходимые для выполнения симметричного шифрования алгоритмом AES, вы знаете?
40) Как можно осуществлять асимметричное шифрование алгоритмом RSA средствами пакета OpenSSL?
41) Какие функции для файловой выгрузки-загрузки открытых и закрытых ключей ключевых пар алгоритма RSA вы знаете?
42) Как активировать поддержку отечественных криптоалгоритмов в пакете OpenSSL?
43) Какие функции и типы данных используются при шифровании криптоалгоритмом ГОСТ 28147-89?
44) Как в отечественной криптографии строится процесс обмена сеансовым ключом?
45) Как осуществляется генерация ключевых пар алгоритма электронной подписи ГОСТ Р 34.10-2001?
46) Какие функции используются для загрузки в файл и выгрузки из файла ключевых пар алгоритма электронной подписи ГОСТ Р 34.10-2001?
47) Какие параметры используются при выработке общего ключа с помощью алгоритма VKO GOST R 34.10-2001? Какие функции и типы данных используются для реализации этого алгоритма?
48) Для чего используются сертификаты открытых ключей X.509?
49) Что такое инфраструктура открытых ключей (PKI)? Какие варианты архитектуры PKI вы знаете?
50) Какова структура сертификата X.509?
51) Как сертификаты X.509 хранятся в запоминающих устройствах? Какие форматы сертификатов вы знаете?
52) Что такое поля расширений в составе сертификата X.509?
53) Как OpenSSL настраивается для работы тестового центра сертификации?
54) Какие команды OpenSSL используются для создания сертификатов?
55) Как установить созданный сертификат в системе?
56) Какие в ОС Windows имеются средства для управления установленными сертификатами?
57) Что определяют спецификация PKCS#7 и стандарт CMS?
58) Какие функции Microsoft CryptoAPI для управления хранилищами сертификатов вы знаете?
59) Какие функции Microsoft CryptoAPI для работы с сертификатами вы знаете?

60) Как определить имена всех сертификатов в хранилище?
61) Как верифицировать сертификат?
62) Какие функции Microsoft CryptoAPI поддержки криптографических сообщений вы знаете?
63) Какие структуры данных подготавливаются перед вызовом функции, создающей криптографическое сообщение?
64) Как в протоколе TLS осуществляется аутентификация сервера и клиента?
65) Как с помощью криптографического пакета OpenSSL осуществить генерацию ключевой пары алгоритма ГОСТ 34.10-2001 и создание самоподписанного сертификата?
66) Что собой представляет обобщенный алгоритм работы клиентского приложения, передающего и принимающего данные по протоколу TLS?
67) Какие функции WinSock API используются для открытия и закрытия сокетов, создания и разрыва TCP-соединений?
68) Как для клиентского приложения установить параметры хранилища доверенных сертификатов?
69) Что такое TLS Handshake Protocol?
70) Какие функции OpenSSL используются для создания и установки параметров контекста TLS?
71) Как создать объект TLS-соединения и связать его с сокетом, поддерживающим TCP-соединение?
72) Как разорвать TLS-соединение и освободить его объект и контекст TLS?
73) Как клиентское приложение может инициировать процедуру хендшейка?
74) Какие функции OpenSSL используются для передачи и приема данных по протоколу TLS?
75) Что собой представляет обобщенный алгоритм работы серверного приложения, передающего и принимающего данные по протоколу TLS?
76) Как установить в контекст TLS серверного приложения сертификат сервера и его закрытый ключ?
77) Как перевести серверное приложение в режим ожидания запроса клиента на проведение хендшейка?

Экзаменационные вопросы

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
1	Основные аспекты информационной безопасности	Понятие информационной безопасности. Основные типы угроз информационной безопасности
2		Законодательные аспекты информационной безопасности.
3	Криптографические средства защиты информации	Базовые понятия криптографии. Основные задачи, решаемые с помощью криптографии. Понятия криптоалгоритма и ключа
4		Криптоанализ. Понятие стойкости алгоритма. Основные разновидности криптоаналитических атак
5		Классификация алгоритмов классической криптографии. Одноразовые блокноты. Классификация компьютерных криптоалгоритмов.
6		Принципы построения блочных шифров. Сеть Фейстеля
7		Основные режимы работы блочных шифров
8		Криптоалгоритм ГОСТ 28147-89. Структура раунда. Базовые циклы зашифрования и расшифрования. Режимы шифрования, определенные стандартом
9		Криптоалгоритм AES. Характеристики алгоритма и его структура
10		Криптосистемы с открытым ключом. Принципы построения и отличия от симметричных криптосистем. Алгоритм с открытым ключом RSA
11		Управление ключами в симметричных и асимметричных криптосистемах. Генерация ключей. Распределение ключей для симметричных криптосистем
12		Обмен сеансовыми ключами средствами симметричной криптографии и криптографии с открытым ключом. Способы хранения ключей. Время жизни ключей
13		Алгоритм обмена ключами Диффи-Хеллмана-Меркла.
14		Потоковые шифры A5 и RC4
15	Стандарты информационной безопасности	Стандарты информационной безопасности РФ
16	Электронная подпись и аутентификация	Однонаправленные хэш-функции. Назначение. Основные требования, предъявляемые к хэш-функциям. Коллизии и их использование в процессе подделки сообщений
17		Характеристики и общие принципы построения алгоритмов хэширования MD5, SHA-1, 2, 3, ГОСТ Р 34.11-94, 2012
18		Коды проверки подлинности сообщений (MAC)
19		Электронная подпись (ЭП). Назначение электронной подписи, ее виды. Требования к ЭП. Общие принципы создания ЭП. Стандарты ЭП РФ и США
20		Протоколы односторонней и двухсторонней аутентификации
21		Стандарт X.509. Структура сертификата разных версий. Форматы хранения сертификатов
22		Стандарт X.509. Принципы аутентификации. Отзыв сертификатов
23		Инфраструктуры открытых ключей
24	Защита распределенных систем и корпоративных сетей	Атакуемые сетевые компоненты информационных систем. Классификация нарушителей сетевой безопасности информационных систем
25		Основные характеристики и типы брандмауэров и систем обнаружения и предотвращения вторжений

26		Защищенный протокол передачи данных IPSec
27		Защищенный протокол передачи данных SSL/TLS
28	Системы защиты электронной почты	Система защиты электронной почты PGP
29		Система защиты электронной почты S/MIME

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

Не предусмотрено

5.3. Перечень индивидуальных домашних заданий, расчетно-графических заданий.

Тематика ИДЗ:

Обзор функциональных возможностей средств криптографической защиты информации, представленных ведущими российскими разработчиками и сертифицированных ФСБ:

- CryptoPro.
- VipNet.
- МагКрипто.
- Шипка.
- Верба

и т.д.

4.4. Перечень контрольных работ.

Не предусмотрено

5. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

6.1. Перечень основной литературы

1. Галатенко В.А. Основы информационной безопасности: Курс лекций. – М.: Интернет-Университет Информационных Технологий, 2004. – 261 с.
2. Гашков С. Б., Применко С. Б., Черепнев М. А. Криптографические методы защиты информации : учеб. пособие / М. : Издательский центр "Академия", 2010. – 304 с.
3. Лапонина О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учебное пособие. - М. : БИНОМ, 2009. – 536 с.
4. Ярочкин В. И. Информационная безопасность : учеб. / 4-е изд. - М. : Академический Проект, 2006. – 639 с.
5. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд. – М.: Вильямс, 2001. – 672 с.
6. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: ДМК Пресс, 2012. – 592 с.
7. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: ТРИУМФ, 2003. – 815 с.
8. Щербаков А.Ю., Домашев А.В. Прикладная криптография. Использование и синтез криптографических интерфейсов. – М.: Русская редакция, 2003. – 416 с.
9. Смышляев А.Г. Информационная безопасность. Лабораторный практикум. Белгород: Изд-во БГТУ им. В.Г. Шухова, 2015. – 102 с.

6.2. Перечень дополнительной литературы

1. Аграновский А.В. Практическая криптография: алгоритмы и их программирование. – М.: СОЛОН-Пресс, 2002. – 255 с.
2. Анин Б.Ю. Защита компьютерной информации. – СПб.: БХВ-Петербург, 2000. – 384 с.
3. Бабаш А.В., Шанкин Г.П. Криптография. – М.: СОЛОН-Р, 2002. – 512 с.
4. Бернет С., Пэйн С. Криптография. Официальное руководство RSA Security. – М.: Бином-Пресс, 2002. – 384 с.
5. Блэк У. Интернет: Протоколы безопасности. Учебный курс. – СПб.: Питер, 2001. – 288 с.
6. Введение в криптографию / Под общ. ред. В.В. Ященко. – М.: МЦНМО: «ЧеРо», 2000. – 288 с.
7. Зензин О.С. Стандарт криптографической защиты– AES. Конечные поля. – М.: Кудий-Образ, 2002. – 174 с.
8. Молдовян А.А. Криптография. – СПб.: Лань, 2001. – 224 с.
9. Основы криптографии: Учебное пособие/ Сост. Алферов А.П., Зубов А.Ю., Кузьмин А.С. – М.: Гелиос АРВ, 2001. – 480 с.
10. Чмора А.Л. Современная прикладная криптография. – М.: Гелиос АРВ, 2002. – 256 с.

6.3. Перечень интернет ресурсов

1. Портал по информационной безопасности [Электронный ресурс]. Режим доступа: http://infosecurity.report.ru
2. Российский криптографический портал [Электронный ресурс]. Режим доступа: http://infosecurity.report.ru
3. Сервер компании НИП "Информзащита" [Электронный ресурс]. Режим доступа: http://infosecurity.report.ru
4. Информационный бюллетень "Jet Info" [Электронный ресурс]. Режим доступа: http://infosecurity.report.ru
5. Портал по информационной безопасности [Электронный ресурс]. Режим доступа: http://bugtraq.ru

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

Учебные аудитории для проведения лекционных занятий, лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы обучающихся, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации. Аудитории для лекционных занятий оборудованы специализированной мебелью, мобильным или стационарным мультимедийным проектором, переносным экраном, ноутбуком, или компьютерами на базе одно или двухъядерных процессоров с тактовой частотой не менее 2 ГГц, объемом оперативной памяти не менее 2 Гб и жесткого диска до 500 Гб; локальная сеть с пропускной способностью 100 Мбит/с; лазерные принтеры или многофункциональные устройства форматов А4, А3;

планшетные сканеры (при отсутствии МФУ).

Для проведения лабораторных занятий могут использоваться компьютерные классы, оснащенные компьютерами с установленными программными продуктами:

Лицензионное ПО:

- Microsoft Office Professional
- Microsoft Windows
- Kaspersky Endpoint Security 10 для Windows
- Microsoft Visual Studio

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Утверждение рабочей программы с изменениями, дополнениями

1. На титульном листе рабочей программы читать название «Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования» как «Федеральное государственное бюджетное образовательное учреждение высшего образования»
2. Институт информационных технологий и управляющих систем был переименован 30.04.2016 г. в институт Энергетики, информационных технологий и управляющих систем на основании приказа № 4/52 от 29.02.2016 г.

Рабочая программа с изменениями, дополнениями утверждена на 2016/2017 учебный год.

Протокол № 7 заседания кафедры ИТ от «15» 06 2016 г.

Заведующий кафедрой: канд.техн. наук, доц. _____ (И.В. Иванов)

Директор института ЭИТУС: канд.техн. наук, доц. _____ (А.В. Белоусов)

Утверждение рабочей программы без изменений

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

Протокол № 12 заседания кафедры ИТ от «27» 06 2017 г.

Заведующий кафедрой: канд.техн. наук, доц. _____ (И.В. Иванов)

Директор института ЭИТУС: канд.техн. наук, доц. _____ (А.В. Белоусов)

Утверждение рабочей программы с изменениями, дополнениями

1. Изменения в п. 6

Рабочая программа с изменениями, дополнениями утверждена на 2018/2019 учебный год.

Протокол № 6 заседания кафедры ИТ от «11» 04 2018 г.

Заведующий кафедрой: канд.техн. наук, доц. _____ (И.В. Иванов)

Директор института ЭИТУС: канд.техн. наук, доц. _____ (А.В. Белоусов)

6. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

6.1. Перечень основной литературы

1. Шаньгин, В. Ф. Информационная безопасность и защита информации [Электронный ресурс] : учебное пособие / Шаньгин В. Ф. - Москва : ДМК Пресс, 2014. - 702 с. http://www.iprbookshop.ru/63594.html?replacement=1/
2. Скрипник, Д. А. Общие вопросы технической защиты информации [Электронный ресурс] : учебное пособие / Скрипник Д. А. - Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 264 с. http://www.iprbookshop.ru/52161.html?replacement=1
3. Аверченков В.И., Рытов М.Ю. Организационная защита информации Учебное пособие Брянский государственный технический университет 2012 http://www.iprbookshop.ru/7002.html
4. Смышляев А. Г. Информационная безопасность и защита информации : метод. указания к выполнению лаб. работ / БГТУ им. В. Г. Шухова, каф. информ. технологий ; сост. А. Г. Смышляев. - Белгород : Изд-во БГТУ им. В. Г. Шухова, 2008. - 27 с.
5. Аверченков, В. И. Аудит информационной безопасности [Электронный ресурс] : учебное пособие для вузов / Аверченков В. И. - Брянск : Брянский государственный технический университет, 2012. - 268 с. http://www.iprbookshop.ru/6991.html
6. Гашков, С. Б. Криптографические методы защиты информации : учеб. пособие / С. Б. Гашков, С. Б. Применко, М. А. Черепнев. - Москва : Академия, 2010. - 298 с.
7. Смышляев А. Г. Информационная безопасность : лаб. практикум : учеб. пособие / А. Г. Смышляев ; БГТУ им. В. Г. Шухова. - Белгород : Изд-во БГТУ им. В. Г. Шухова, 2015. - 101 с.

6.2. Перечень дополнительной литературы

1. Петренко, С. А. Политики безопасности компании при работе в Интернет [Текст] / Петренко С. А. - Саратов : Профобразование, 2017. - 397 с. http://www.iprbookshop.ru/63807
2. Аверченков, В. И. Аудит информационной безопасности [Электронный ресурс] : учебное пособие для вузов / Аверченков В. И. - Брянск : Брянский государственный технический университет, 2012. - 268 с. http://www.iprbookshop.ru/7002
3. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие Учебное пособие М.: Книжный мир 2009 http://biblioclub.ru/index.php?page=book&id=89798
4. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности [Электронный ресурс] : учебное пособие / Авдошин С. М. - Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2010. - 326 с. http://biblioclub.ru/index.php?page=book&id=233684
5. Спицын, В. Г. Информационная безопасность вычислительной техники [Электронный ресурс] : учебное пособие / Спицын В. Г. - Томск : Эль Контент, Томский государственный университет систем управления и радиоэлектроники, 2011. - 148 с. http://www.iprbookshop.ru/13936.html
6. Федин, Ф. О. Информационная безопасность [Электронный ресурс] : учебное пособие / Федин Ф. О. - Москва : Московский городской педагогический университет, 2011. - 260 с. http://www.iprbookshop.ru/26486.html
7. Лапонина, О. Р. Основы сетевой безопасности : криптографические алгоритмы и протоколы взаимодействия : учеб. пособие / О. Р. Лапонина. - 2-е изд., испр. . - Москва : Интернет-Университет Информационных Технологий ; Москва : БИНОМ. Лаборатория знаний, 2007. - 531 с.
8. Платонов, В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учеб. пособие / В. В. Платонов. - Москва :

Академия, 2006. - 239 с.

Утверждение рабочей программы без изменений

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

Протокол № 9 заседания кафедры ИТ от «7» июня 2019 г.

И.о.зав. кафедрой ИТ: канд.техн. наук _____(Д.Н. Старченко)

Директор института ЭИТУС: канд.техн. наук, доц._____(А.В. Белоусов)

Утверждение рабочей программы без изменений

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

Протокол № 6 заседания кафедры ИТ от «12» 05 20 20 г.

И.о.зав. кафедрой ИТ: канд.техн. наук _____(Д.Н. Старченко)

Директор института ЭИТУС: канд.техн. наук, доц. _____(А.В. Белоусов)

Утверждение рабочей программы без изменений

Рабочая программа без изменений утверждена на 2021 /2022 учебный год.

Протокол № 6 заседания кафедры ИТ от «30» 04 2021 г.

И.о.зав. кафедрой ИТ канд.техн.наук _____(Д.Н. Старченко)

Директор института ЭИТУС канд.техн.наук, доц. _____(А.В. Белоусов)