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

УТВЕРЖДАЮ
Директор института ИТУС
_____ В.Г. Рубанов
«23» 04 2015 г.

РАБОЧАЯ ПРОГРАММА
дисциплины

Информационная безопасность

направление подготовки

09.03.03 Прикладная информатика

профиль программы

Прикладная информатика в бизнесе

квалификация

бакалавр

Форма обучения

очная

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 09.03.03 Прикладная информатика (уровень бакалавриата), утвержденного Приказом Министерства образования и науки Российской Федерации. от 12 марта 2015 г. N 207

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

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

«22» 04 2015 г., протокол № 9/12

Председатель: канд.техн. наук, доц. _____ (Ю.И. Солопов)

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

№	Код компетенции	Компетенция	Требования к результатам обучения
Общепрофессиональные			
1	ОПК-4	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:** – 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. **Уметь** организовать процесс защиты информационных систем в соответствии с отечественными и международными стандартами в области информационной безопасности. **Владеть** навыками адаптации и применения существующих систем защиты информации от несанкционированного доступа.
Профессиональные			
2	ПК-11	способность эксплуатировать и сопровождать информационные системы и сервисы	В результате освоения дисциплины обучающийся должен **Знать:** – основы построения криптосистем, а также средств создания и верификации электронных подписей и аутентификации; – особенности защиты распределенных информационных систем. **Уметь:** – 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.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Содержание дисциплины основывается и является логическим продолжением следующих дисциплин:

№	Наименование дисциплины (модуля)
2	Информатика и программирование
3	Программная инженерия
4	Информационные системы и технологии

Содержание дисциплины служит основой для изучения следующих дисциплин:

№	Наименование дисциплины (модуля)
1	Отраслевые информационные системы
3	Проектирование информационных систем

3. ОБЪЕМ ДИСЦИПЛИНЫ

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

Вид учебной работы	Всего часов	Семестр № 6
Общая трудоемкость дисциплины, час	144	144
Контактная работа (аудиторные занятия), в т.ч.:	51	51
лекции	17	17
лабораторные	34	17
практические		
Самостоятельная работа студентов, в том числе:	93	93
Курсовой проект		
Курсовая работа		
Расчетно-графическое задание	18	18
Индивидуальное домашнее задание		
Другие виды самостоятельной работы	35	35
Форма промежуточная аттестация (зачет, экзамен)	40	40 Экзамен

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ
4.1 Наименование тем, их содержание и объем
Курс 3 Семестр 6

№ 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.	1			1
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.	6		22	21
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.	1			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	4		6	5

	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.	2		6	4
6.	**Раздел 6. Системы защиты электронной почты**				
	Назначение и принцип работы систем PGP и S/MIME.	2			1
7.	**Раздел 7. Организационное обеспечение информационной безопасности**				
	Административный уровень информационной безопасности. Формирование политики безопасности. Управление рисками. Процедурный уровень информационной безопасности. Основные меры поддержания работоспособности информационной системы.	1			1
	ВСЕГО	17		34	35

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	4	2
2		Алгоритм блочного шифрования данных ГОСТ 28147-89	6	3
3		Симметричное шифрование данных с использованием криптографических интерфейсов Microsoft CryptoAPI и Cryptography API: Next Generation	6	3
4		Симметричное и асимметричное шифрование данных средствами криптографического пакета OpenSSL	6	3
5	Электронная	Создание криптографических сообщений с	6	3

	подпись и аутентификация	использованием интерфейса Microsoft CryptoAPI и цифровых сертификатов X.509		
6	Защита распределенных систем и корпоративных сетей	Реализация защищенной передачи данных по протоколу TLS средствами криптографического пакета OpenSSL	6	3
		ИТОГО:	34	17
			ВСЕГО:	51

5. 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	Атакуемые сетевые компоненты информационных систем. Классификация нарушителей сетевой безопасности

	систем и корпоративных сетей	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
30	Организационное обеспечение информационной безопасности	Организационное обеспечение информационной безопасности

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

Не предусмотрено

5.3. Перечень индивидуальных домашних заданий, расчетно-графических заданий

Темы расчетно-графических заданий

вариант	тема
1	Безопасность в Интеренете
2	Источники угроз безопасности персональных данных
3	Отличительные особенности информационной безопасности РФ
4	Методы защиты информации в современных ОС
5	Роль информационной безопасности в современном мире
6	Проблемы обеспечения информационной безопасности
7	Системы обнаружения вторжений
8	Обеспечение защиты данных в беспроводных сетях
9	Проблемы информатизации общества. Способы защиты своей индивидуальности
10	Нововведения в законодательную базу РФ в области информационной безопасности
11	Методы оценки рисков безопасности
12	Особенности защиты информации в сетях различной архитектуры
13	Компьютерное пиратство. Методы борьбы.
14	Защита данных с помощью биометрики
15	Анализ возможных каналов утечки информации

5.4. Перечень контрольных работ

Не предусмотрено

6. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

6.1. Перечень основной литературы

1. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях Учебное пособие М.: ДМК Пресс 2012. http://e.lanbook.com/view/book/3032/
2. Скрипник Д.А. Общие вопросы технической защиты информации Учебное пособие Интернет-Университет Информационных Технологий (ИНТУИТ) 2012 http://www.iprbookshop.ru/16710.html
3. Аверченков В.И., Рытов М.Ю. Организационная защита информации Учебное пособие Брянский государственный технический университет 2012 http://www.iprbookshop.ru/7002.html
4. Метелица Н.Т. Вычислительные сети и защита информации Учебное пособие Южный институт менеджмента 2013 http://www.iprbookshop.ru/25962.html
5. Аверченков В.И. Аудит информационной безопасности Учебное пособие Брянский государственный технический университет 2012 http://www.iprbookshop.ru/6991.html
6. Гашков С. Б., Применк С. Б., Черепнев М. А. Криптографические методы защиты информации Учебное пособие М.: Издательский центр "Академия" 2010
7. Смышляев А. Г. Информационная безопасность и защита информации. Учебное пособие Учебное пособие Белгород:
8. Изд-во БГТУ 2012
9. Смышляев А. Г. Информационная безопасность и защита информации : метод. указания к выполнению лаб. работ Метод. указания Белгород:
10. Изд-во БГТУ 2008
11. Смышляев А. Г. Информационная безопасность : лаб. практикум : учеб. пособие для студентов очной формы обучения направления бакалавриата 09.03.02 - Информац. системы и технологииУчебное пособие Белгород:
12. Изд-во БГТУ 2015

6.2. Перечень дополнительной литературы

1. Смышляев А. Г. Информационная безопасность и защита информации : методические указания к выполнению лабораторных работ Метод. указ. БГТУ им. в. Г. Шухова 2008 https://elib.bstu.ru/Reader/Book/2013040917423620565600001204
2. Максим М. Безопасность беспроводных сетей / Мерритт Максим, Дэвид Поллино Учебное пособие М.: Компания АйТи; ДМК Пресс 2008 http://e.lanbook.com/view/book/1115/
3. Петренко С. А., Петренко А. А. Аудит безопасности Intranet Учебное пособие М.: ДМК Пресс 2010 http://e.lanbook.com/view/book/1113/
4. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. Учебное пособие. М.: ДМК Пресс. 2008. http://e.lanbook.com/view/book/3027/

5. Аверченков В.И. Организационная защита информации : учеб.пособие для вузов Учебное пособие М. : ФЛИНТА 2011. http://www.knigafund.ru/books/116220/read
6. А.Ю. Щербаков Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие Учебное пособие М.: Книжный мир 2009 http://www.knigafund.ru/books/88712/read
7. Сердюк В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие Учебное пособие М.: Издательский дом Государственного университета — Высшей школы экономики 2011 http://www.knigafund.ru/books/149149/read
8. Спицын В.Г. Информационная безопасность вычислительной техники Учебное пособие. Эль Контент, Томский государственный университет систем управления и радиоэлектроники 2011. http://www.iprbookshop.ru/13936.html
9. Афанасьев А.А., Веденьев Л.Т., Воронцов А А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие Горячая линия – Телеком. 2012. http://www.iprbookshop.ru/11978.html
10. Федин Ф.О., Офицеров В.П., Федин Ф.Ф. Информационная безопасность. Учебное пособие Московский городской педагогический университет 2011 http://www.iprbookshop.ru/26486.html
11. Лапонина О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия, 2-е изд., испр. Учебное пособие М.: Интернет-Университет Информационных Технологий; М.: БИНОМ 2007
12. Платонов В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей Учебное пособие М.: Издательский центр "Академия" 2006

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

7. 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
- 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. Защита информации в компьютерных системах и сетях : учебное пособие. М.: ДМК Пресс, 2014. Режим доступа: http://www.iprbookshop.ru/63594.html?replacement=1/
2. Скрипник Д.А. Общие вопросы технической защиты информации : учебное пособие. Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. Режим доступа: 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. Режим доступа: http://www.iprbookshop.ru/7002.html
4. Гашков С. Б., Применк С. Б., Черепнев М. А. Криптографические методы защиты информации : учебное пособие. М.: Издательский центр "Академия", 2010.
5. Смышляев А. Г. Информационная безопасность и защита информации. Учебное пособие : учебное пособие. Белгород: Изд-во БГТУ, 2012.
6. 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.
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. Смышляев А. Г. Информационная безопасность и защита информации : методические указания к выполнению лабораторных работ : метод. указ. БГТУ им. в. Г. Шухова, 2008. Режим доступа: https://elib.bstu.ru/Reader/Book/2013040917423620565600001204
2. Федин Ф.О., Офицеров В.П., Федин Ф.Ф. Информационная безопасность : учебное пособие. Московский городской педагогический университет, 2011. Режим доступа: http://www.iprbookshop.ru/26486.html
3. Петренко С.А., Курбатов В.А. Политики безопасности компании при работе в Интернет : учебное пособие. Саратов: Профобразование, 2017. Режим доступа: http://www.iprbookshop.ru/63807
4. Аверченков В.И. Организационная защита информации Учебное пособие Брянск: Брянский государственный технический университет 2012 http://www.iprbookshop.ru/7002
5. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие : учебное пособие. М.: Книжный мир, 2009. Режим доступа: http://biblioclub.ru/index.php?page=book&id=89798
6. Авдошин С. М. Савельева А. А., Сердюк В. А.Технологии и продукты Microsoft в обеспечении информационной безопасности : учебное пособие. Москва : Интернет-Университет Информационных Технологий, 2010. Режим доступа: http://biblioclub.ru/index.php?page=book&id=233684
7. Спицын В.Г. Информационная безопасность вычислительной техники : учебное пособие. Эль Контент, Томский государственный университет систем управления и радиоэлектроники, 2011. Режим доступа: http://www.iprbookshop.ru/13936.html
8. Лапонина О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учебное пособие. М.: Интернет-Университет Информационных Технологий; М.: БИНОМ, 2007.

9. Платонов В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учебное пособие. М.: Издательский центр "Академия", 2006.

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 _____ (Л.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)