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

УТВЕРЖДАЮ
Директор института ЭИТУС
_____ А.В. Белоусов
«20» 05 2021 г.

РАБОЧАЯ ПРОГРАММА
дисциплины

Информационная безопасность

Направление подготовки

18.05.02 Химическая технология материалов современной энергетики

Направленность программы

Ядерная и радиационная безопасность на объектах использования ядерной энергии

Квалификация

Инженер

Форма обучений

очная

Институт: Энергетики, информационных технологий и управляющих систем

Кафедра: Информационных технологий

Белгород – 2021

Образовательная программа составлена на основании с требованиями:

- Федерального государственного образовательного стандарта высшего образовани - специалитет по специальности 18.05.02 Химическая технология материало современной энергетики, утвержденного приказом Минобрнауки России с 07.08.2020 г. № 913;

- Учебного плана, утвержденного ученым советом БГТУ им. Шухова в 2021 г.

Составитель (составители): _____ (Е.П. Коломыцева)
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа обсуждена на заседании кафедры

«30» 04 2021 г., протокол № 6

и.о. заведующий кафедрой: к.т.н., доцент _____ (Д.Н. Старченко)
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа согласована с выпускающей кафедрой теоретической и прикладной химии
Зав. кафедрой: доктор техн.наук, профессор _____(В.И. Павленко)

«13» мая 2021г., протокол № 9

Рабочая программа одобрена методической комиссией института

«20» 05 2021 г., протокол № 9

Председатель к.т.н., доцент _____(А.Н. Семернин)
(ученая степень и звание, подпись) (инициалы, фамилия)

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Категория (группа) компетенций	Код и наименования компетенции	Код и наименование индикатора достижения компетенции	Наименование показателя оценивания
Общепрофессиональные	ОПК-6. Способен использовать информацию, полученную при осуществлении своей профессиональной деятельности, с учетом основных требований информационной безопасности в том числе защиты государственной тайны	ОПК-6.1 Использует информацию, полученную при осуществлении профессиональной деятельности с учетом требований информационной безопасности	Понимает: технические и программные средств реализации информационных процессов; методы и процессы сбора, передачи, обработки и накопления информации; Умеет: использовать возможности вычислительной техники и программного обеспечения; выполнять обобщение и систематизацию технических данных; осуществлять выбор наиболее эффективных методов, способов и средств получения, хранения и переработки информации в зависимости от конкретных целей и задач профессиональной деятельности; использовать возможностиглобальных компьютерныхсетей;
		ОПК-6.2 Применяет методы информационной безопасности при подготовке проектной и технической документации в сфере профессиональной деятельности	Понимает: теоретические основы изучаемых алгоритмов шифрования, формы защиты информации в сети Интернет, требования к защите информации, критерии оценки угроз. Умеет: проводить анализ необходимой информации, технических данных, показателей и результатов работы; работать с различными источниками информации, используя разные формы защиты информации, выявлять программы – шпионы, «вирусы».

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Компетенция ОПК-6. Способен использовать информацию, полученную при осуществлении своей профессиональной деятельности, с учетом основных требований информационной безопасности в том числе защиты государственной тайны.

Данная компетенция формируется следующими дисциплинами.

Стадия	Наименование дисциплины
1	Информационная безопасность
2	Выполнение, подготовка к процедуре защиты и защита Выпускной квалификационной работы

3. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 4 зач. единиц, 144 часа.

Вид учебной работы	Всего часов	Семестр № 8
Общая трудоемкость дисциплины, час	144	144
Контактная работа (аудиторные занятия), в т.ч.:	51	51
лекции	17	17
лабораторные		
практические	34	34
Самостоятельная работа студентов, в том числе:	93	
Подготовка к лекциям	14	14
Подготовка к практическим занятиям	34	34
Выполнение ИДЗ	9	9
Подготовка к экзамену	36	36
Форма промежуточная аттестация (зачет, экзамен)		Экзамен

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Наименование тем, их содержание и объем

№ п/п	Наименование раздела (краткое содержание)	Объем на тематический раздел по видам учебной нагрузки, час			
		Лекции	Лабораторные занятия	Практические занятия	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. КриптоалгоритмыAES, ГОСТ 28147-89 и ГОСТ Р 34.12-2015.Основные принципы шифрования с открытым ключом. Области применения криптосистем с открытым ключом. КриптоалгоритмRSA. Управление ключами. Алгоритм Диффи-Хеллмана-Меркла.	6		22	28
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	4		6	10

	создания и верификацииэлектронных подписей: DSA,ECDSA, ГОСТ Р 34.10-94, 2001, 2012. Протоколы 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	8
6.	**Раздел 6. Системы защиты электронной почты**				
	Назначение и принцип работы систем PGPи S/MIME.	2			3
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	53

4.2. Содержание лабораторных занятий

Не предусмотрено учебным планом

4.3. Содержание практических (семинарских) занятий

№ п/п	Наименование раздела дисциплины	Тема лабораторного занятия	К-вочасов	К-во часов СРС
семестр № 8				
1	Криптографические средства защиты информации	Потоковое шифрование данных	4	4
2		Алгоритм блочного шифрования данных ГОСТ 28147-89	6	6
3		Симметричное шифрование данных с использованием криптографических интерфейсов MicrosoftCryptoAPI и Cryptography API: NextGeneration	6	6
4		Симметричное и асимметричное шифрование данных средствами криптографического пакета OpenSSL	6	6

5	Электронная подпись и аутентификация	Создание криптографических сообщений с использованием интерфейса MicrosoftCryptoAPI и цифровых сертификатов X.509	6	6
6	Защита распределенных систем и корпоративных сетей	Реализация защищенной передачи данных по протоколу TLS средствами криптографического пакета OpenSSL	6	6
		ИТОГО:	34	34
			ВСЕГО:	68

4.4. Содержание курсового проекта/работы

Не предусмотрено учебным планом

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

5.1. Реализация компетенции

Компетенция ОПК-6. Способен использовать информацию, полученную при осуществлении своей профессиональной деятельности, с учетом основных требований информационной безопасности в том числе защиты государственной тайны.

Наименование индикатора (показателя оценивания)	Используемые средства оценивания
ОПК-6.1 Использует информацию, полученную при осуществлении профессиональной деятельности с учетом требований информационной безопасности	Собеседование, защита лабораторной работы, тестовый контроль, устный опрос.
ОПК-6.2 Применяет методы информационной безопасности при подготовке проектной и технической документации в сфере профессиональной деятельности	Собеседование, защита лабораторной работы, тестовый контроль, устный опрос.

5.2. Типовые контрольные задания для промежуточной аттестации

5.2.1. Перечень контрольных вопросов (типовых заданий) для экзамена

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 вГОСТ 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) Чтотакое 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 MicrosoftCryptoAPI для управления хранилищами сертификатов вы знаете?
59) Какие функции MicrosoftCryptoAPI для работы с сертификатами вы знаете?
60) Как определить имена всех сертификатов в хранилище?
61) Как верифицировать сертификат?
62) Какие функции MicrosoftCryptoAPI 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) Чтотакое 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 напроведение 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		КриптоалгоритмAES. 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 хэшированияMD5, 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	информационных систем
25	корпоративных сетей	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	Система защиты электронной почты PGP
29	электронной почты	Система защиты электронной почты S/MIME
30	Организационное обеспечение информационной безопасности	Организационное обеспечение информационной безопасности

5.2.2. Перечень контрольных материалов для защиты курсового проекта/курсовой работы

Не предусмотрено учебным планом

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

Написать реферат по предложенным темам.

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

5.5. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

5.5.1. 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.

5.5.2. 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. Организационная защита информации [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И., Рытов М.Ю.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 184 с.— Режим доступа: http://www.iprbookshop.ru/7002.html.— ЭБС «IPRbooks»
3. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособиеУчебное 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 c. 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 c. 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.

5.5.3. Перечень интернет ресурсов

1. Портал по информационной безопасности [Электронный ресурс]. Режим доступа: https://www.securitylab.ru/
2. Математическая криптография [Электронный ресурс]. Режим доступа: http://cryptography.ru/
3. Сервер компании НИП "Информзащита" [Электронный ресурс]. Режим доступа: https://infosec.ru/
4. Портал по информационной безопасности[Электронный ресурс]. Режим доступа: http://bugtraq.ru

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

1. Лекционная аудитория с интерактивной доской.
2. Компьютерный класс с ПК, имеющими организационные и технические возможности для установки требуемого программного обеспечения, выход в глобальную сеть Интернет.
3. Операционная система WindowsXP или новее, пакет MSOffice 2007 или новее, среда программирования VisualStudio 2010 или новее.
4. Система компьютерного тестирования знаний VeralTest (доступ по локальной сети университета по адресу http://veraltest.bstu.ru)

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Утверждение рабочей программы без изменений

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

Протокол № 8 заседания кафедры ИТ от «24» мая 2018 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 утверждена на 2019/2020 учебный год.

Протокол №_10_ заседания кафедры информационных технологий от "_25_" _06_ 2019 г.

Зав. кафедрой _____ (Д.Н. Старченко)

Директор института _____ (А.В. Белоусов)

УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Утверждение рабочей программы без изменений.

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

Протокол № 8 заседания кафедры от «17» 05 2020 г.

И.о.заведующий кафедрой _____ (к.т.н., доцент Д.Н. Старченко)

Директор института энергетики,
информационных технологий и
управляющих систем _____ (к.т.н.,доцент А.В. Белоусов)