МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ
Декан факультета информационных технологий и компьютерной безопасности
_____ /П.Ю. Гусев/
31.08.2021 г.

РАБОЧАЯ ПРОГРАММА
дисциплины (модуля)
«Информационная безопасность и защита информации»

Направление подготовки (специальность) 09.03.02 Информационные системы и технологии

Профиль (специализация) Системы автоматизации проектирования и разработки информационных систем

Квалификация выпускника бакалавр

Нормативный период обучения 4 года

Форма обучения Очная

Год начала подготовки 2021 г.

Автор(ы) программы _____ (подпись) А.В. Питолин

Заведующий кафедрой Системы автоматизированного проектирования и информационные системы _____ Я.Е. Львович

Руководитель ОПОП _____ (подпись) О.Г. Яскевич

Воронеж 2021

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

Целью изучения дисциплины является приобретение студентами теоретических знаний и практических навыков в области защиты информации и информационной безопасности; ознакомление студентов с современными системами информационной безопасности, технологическими приемами защиты информации; возможностями использования средств информационной безопасности при работе с информационными ресурсами.

1.2. Задачи освоения дисциплины

изучение теоретических основ, методов и средств организационно-правового и технического обеспечения защиты конфиденциальной информации и персональных данных;

- получение знаний и навыков в области оценки защищенности информации в автоматизированных системах;

освоение и использование в практической деятельности технологий информационной безопасности на основе применения специализированных аппаратных и программных средств.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Информационная безопасность и защита информации» относится к дисциплинам части, формируемой участниками образовательных отношений (дисциплина по выбору) блока Б1 учебного плана.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Информационная безопасность и защита информации» направлен на формирование следующих компетенций:

ПК-2 - Способен выполнять проектирование информационных систем и ресурсов для различных прикладных областей

ПК-6 - Способен проводить оценку осуществимости функционирования и сопровождения информационной системы

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-2	Знать: сущность и понятие информационной безопасности, характеристику ее составляющих; источники угроз информационной безопасности и меры по их предотвращению.
	Уметь: пользоваться средствами защиты информации при эксплуатации вычислительной техники, периферийных и мобильных устройств, других технических средств информатизации.
	Владеть: современными средствами и методы построения комплексных систем обеспечения

	информационной безопасности в автоматизированных системах
ПК-6	Знать: жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи; методы оценки эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности
	Уметь: использовать средства защиты информации от несанкционированного съема и утечки по техническим каналам; использовать средства охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения.
	Владеть: современными средствами и методы построения комплексных систем обеспечения информационной безопасности в автоматизированных системах

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Информационная безопасность и защита информации» составляет 3 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры
		7
Аудиторные занятия (всего)	72	72
В том числе:		
Лекции	36	36
Лабораторные работы (ЛР)	36	36
Самостоятельная работа	36	36
Виды промежуточной аттестации - зачет	+	+
Общая трудоемкость: академические часы зач.ед.	 108 3	 108 3

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Основы информационной безопасности	Понятие информационной безопасности. Основные концептуальные положения системы защиты информации. Угрозы конфиденциальной информации. Действия, приводящие к неправомерному овладению конфиденциальной информацией. Модель системы безопасности. Угрозы конфиденциальной информации.	4	6	6	16

		Классификация угроз.				
2	Направления обеспечения информационной безопасности	Направления обеспечения информационной безопасности. Организационная защита. Правовые основы информационной безопасности. Инженерно-техническая защита. Физические средства защиты Аппаратные средства защиты Программные средства защиты. Основные направления использования программной защиты информации.	8	6	6	20
3	Криптографические методы и средства защиты информации	Криптографические средства защиты. Общая технология шифрования. Методы шифрования с закрытым ключом. Алгоритмы шифрования DES, AES. Криптографические хеш-функции. Криптографические алгоритмы с открытым ключом и их использование. Электронная цифровая подпись. Шифрование, помехоустойчивое кодирование и сжатие информации	8	6	6	20
4	Стандарты и спецификации в области информационной безопасности	Стандарты и спецификации в области информационной безопасности. Стандарт «Критерии оценки доверенных компьютерных систем». Механизмы безопасности. Классы безопасности. Информационная безопасность распределенных систем. Рекомендации X.800. Сетевые сервисы безопасности. Стандарт ISO/IEC «Критерии оценки безопасности информационных технологий».	4	6	6	16
5	Защита информации от утечки по техническим каналам	Основные понятия в области технической защиты информации. Защита информации от утечки по техническим каналам. Структура канала утечки информации. Классификация каналов утечки информации. Аттестация объектов информатизации по требованиям безопасности.	8	6	6	20
6	Информационная безопасности в компьютерных сетях	Информационная безопасность в компьютерных сетях. Распределение функций безопасности по уровням модели. Классификация удаленных угроз в вычислительных сетях. Типовые удаленные атаки и их характеристики Компьютерные вирусы как угроза информационной безопасности. Классификация компьютерных вирусов. Антивирусные программы. Особенности функционирования и классификация	4	6	6	16
		Итого	**36**	**36**	**36**	**108**

5.2 Перечень лабораторных работ

1. Антивирусная защита информации. Работа с антивирусными пакетами.

2. Поточные шифры. Моделирование работы 8-ми (16-ти) разрядного скремблера

3. Программная реализация комбинированных криптографических алгоритмов

4. Программирование арифметических алгоритмов

5. Программирование алгоритмов криптосистем с открытым ключом.

6. Алгоритм шифрации двойным квадратом. Шифр Enigma.

7. Алгоритмы шифрования DES и ГОСТ 28147-89.

8. Алгоритм шифрования RSA

9. Алгоритм шифрования Эль Гамаля. Задачи и алгоритмы

электронной подписи.

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ПК-2	Знать: сущность и понятие информационной безопасности, характеристику ее составляющих; источники угроз информационной безопасности и меры по их предотвращению.	Выполнение, подготовка отчета и защита лабораторных работ, опрос по темам самостоятельного изучения	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь: пользоваться средствами защиты информации при эксплуатации вычислительной техники, периферийных и мобильных устройств, других технических средств информатизации.	Выполнение, подготовка отчета и защита лабораторных работ, опрос по темам самостоятельного изучения	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть: современными средствами и методы построения комплексных систем обеспечения информационной безопасности в автоматизированных системах	Выполнение, подготовка отчета и защита лабораторных работ, опрос по темам самостоятельного изучения	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-6	Знать: жизненные циклы конфиденциальной информации в процессе ее создания, обработки,	Выполнение, подготовка отчета и защита лабораторных работ, опрос по темам самостоятельного изучения	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	передачи; методы оценки эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности			
	Уметь: использовать средства защиты информации от несанкционированного съема и утечки по техническим каналам; использовать средства охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения.	Выполнение, подготовка отчета и защита лабораторных работ, опрос по темам самостоятельного изучения	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть: современными средствами и методы построения комплексных систем обеспечения информационной безопасности в автоматизированных системах	Выполнение, подготовка отчета и защита лабораторных работ, опрос по темам самостоятельного изучения	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 7 семестре для очной формы обучения по двухбалльной системе:

«зачтено»

«не зачтено»

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Не зачтено
ПК-2	Знать: сущность и понятие информационной безопасности, характеристику ее составляющих; источники угроз информационной безопасности и меры по их предотвращению.	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	Уметь: пользоваться средствами защиты информации при эксплуатации вычислительной техники, периферийных и мобильных устройств, других технических средств информатизации.	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	Владеть: современными средствами и методы построения	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены

	комплексных систем обеспечения информационной безопасности в автоматизированных системах			
ПК-6	Знать: жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи; методы оценки эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	Уметь: использовать средства защиты информации от несанкционированного съема и утечки по техническим каналам; использовать средства охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения.	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	Владеть: современными средствами и методы построения комплексных систем обеспечения информационной безопасности в автоматизированных системах	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1. Аутентификация на основе пароля, переданного по сети в зашифрованном виде и снабженного открытой временной меткой, плоха, потому что не обеспечивает защиты от:

перехвата

воспроизведения

атак на доступность

2. Криптография необходима для реализации следующих сервисов безопасности:

идентификация

экранирование

аутентификация

3. Системы анализа защищенности выявляют уязвимости путем:

диалогов с пользователями

пассивного анализа

активного опробования

4. В число возможных стратегий нейтрализации рисков входят:

переадресация риска

деноминация риска

декомпозиция риска

5. Для обеспечения информационной безопасности сетевых конфигураций следует руководствоваться следующими принципами:

выработка и проведение в жизнь единой политики безопасности

унификация аппаратно-программных платформ

минимизация числа используемых приложений

6. Согласно рекомендациям X.800, выделяются следующие сервисы безопасности:

управление квотами

управление доступом

экранирование

7. Реализация протоколирования и аудита преследует следующие главные цели:

обнаружение попыток нарушений информационной безопасности

недопущение попыток нарушений информационной безопасности

недопущение атак на доступность

8. Дублирование сообщений является угрозой:

доступности

конфиденциальности

целостности

9. Информационный сервис считается недоступным, если:

его эффективность не удовлетворяет наложенным ограничениям

подписка на него стоит слишком дорого

не удается найти подходящий сервис

10. В число этапов жизненного цикла информационного сервиса входят:

закупка

продажа

выведение из эксплуатации

7.2.2 Примерный перечень заданий для решения стандартных задач

1. Алгоритмы шифрования с открытым ключом по-другому называются:

симметричными алгоритмами шифрования

односторонними алгоритмами шифрования
помехоустойчивыми алгоритмами шифрования
асимметричными алгоритмами шифрования

2. Зашифруйте методом перестановки с фиксированным периодом d=6 с ключом 436215 сообщение КРИПТОГРАФИЯ

ПИОРКТФАЯРГИ

3. Вычислите последовательность из четырех чисел, генерируемую по методу Фибоначчи с запаздыванием, начиная с k_a, при следующих исходных данных: a = 4, b = 2, k_0=01; k_1=0.7; k_2=0.3; k_3=0.9

k_4=0.8; k_5=0.8; k_6=0.5; k_7=0.1

4. Чему равна сумма по модулю 2^8 шестнадцатеричных чисел 9E и 0A3? Варианты ответов представлены в двоичной системе счисления Примечание: десятичные или шестнадцатеричные числа необходимо сначала перевести в двоичный вид

01110110
11101100
10111010
01010011
01000001
11111111

5. Расшифруйте сообщение, зашифрованное методом перестановки по таблице 4x4 (символ подчеркивания заменяет пробел) Ключ указывает порядок считывания столбцов при шифровании. Ответ запишите прописными русскими буквами; в качестве пробела используйте символ подчеркивания Сообщение: НАНЩ_ЕОЯТАМАНН Ключ: 4321

МОЩНАЯ_АНТЕННА

6. Известно, что для некоторого источника сообщений количество информации по Хартли, приходящееся на 1 символ, равно 6 битам Чему равно количество символов в алфавите источника сообщений?

12
3
2
32
128
6
64
256

7. Определите последовательность из первых четырех чисел, вырабатываемых линейным конгруэнтным генератором псевдослучайных

чисел для следующих параметров генератора: a =11, b =7 и c = 16 (k_0 принять равным 0)

$k_1 = 7; k_2 = 4; k_3=2; k_4= 8$

$k_1 = 7; k_2 = 4; k_3=3; k_4= 8$

$k_1 = 4; k_2=3; k_3= 8; k_4 = 15$

$k_1 = 7; k_2 = 4; k_3=3; k_4= 9$

8. На сколько блоков будет разбито сообщение размером 512 байт для шифрования алгоритмом по ГОСТ 28147-89? Ответ запишите в виде одного числа

64

9. Какие простейшие операции не используются для вычисления хеш-функции по алгоритму ГОСТ 3411-94?

возведение в степень

перестановка

получение остатка от деления на большое простое число

сложение по модулю 2

сдвиги бит

10. Какая наука разрабатывает методы «вскрытия» шифров?

линейная алгебра

криптоанализ

криптография

теория чисел

тайнопись

7.2.3 Примерный перечень заданий для решения прикладных задач

1. Какой орган исполнительной власти проводит лицензирование деятельности по оказанию услуг в области защиты государственной тайны в части, касающейся противодействия техническим разведкам и/или технической защиты информации?

ФСТЭК России

ФСБ России

МВД России

Роскомнадзор

2. Какие программы позволяют реализовать DOS-атаки нескольких типов одновременно?

TFN

TFN2K

Smurf

Trinoo

3. Какое программное обеспечение в комплекте сканирующего приемника Winradio 1000 является основной программой управления работой приемника (устанавливает частоту настройки и режим работы приемника, задает параметры сканирования и отображает его результаты, обеспечивает ведение базы данных по результатам работы)?

базовое программное обеспечение
дополнительное программное обеспечение
программное обеспечение в соответствии со спецификацией XRS

4. Как называется принцип контроля доступа, который предполагает назначение каждому объекту списка контроля доступа, элементы которого определяют права доступа к объекту конкретных пользователей или групп?

комбинированный доступ
дискреционный доступ
регистрируемый доступ
мандатный доступ

5. Каналы, в которых утечка информации носит случайный разовый характер, называются:

постоянные
эпизодические
периодические

6. Как называется программное или программно-аппаратное средство, которое разграничивает информационные потоки на границе защищаемой системы?

межсетевой экран
IDS
антивирус
СКД

7. Как называется вредоносная программа, распространяющаяся по сетевым каналам, способная к автономному преодолению систем защиты автоматизированных и компьютерных сетей, а также к созданию и дальнейшему распространению своих копий?

троянский конь
вирус
сетевой червь
макровирус

8. Какие из приведенных ниже документов можно отнести к организационным?

федеральные законы
доктрины
уставы

инструкции
указы Президента
распоряжения Президента

9. Как называется атака на систему, целью которой является довести её до отказа?

отказ в обслуживании
атака на уровне приложений
анализ сетевого трафика
сканирование сети
подмена доверенного объекта в сети

10. Рассчитайте приблизительное значение ослабления акустического сигнала частотой f=2000 Гц в сплошной однородной стене массой 1000 кг.

78.5 Дб
100.5 Дб
40.3 Дб
50.5 Дб

11. Какова эффективность помехоподавляющего фильтра, если напряжение опасного сигнала на входе фильтра 100В, а на выходе 10В?

10 Дб
100 Дб
3 Дб
20 Дб

7.2.4 Примерный перечень вопросов для подготовки к зачету

1. Понятие информационной безопасности. Основные определения.
2. Основные концептуальные положения системы защиты информации.
3. Модель системы безопасности.
4. Угрозы конфиденциальной информации. Классификация угроз.
5. Действия, приводящие к неправомерному овладению конфиденциальной информацией.
6. Направления обеспечения информационной безопасности.
7. Организационная защита.
8. Инженерно-техническая защита.
9. Физические средства защиты.
10. Аппаратные средства защиты.
11. Программные средства защиты. Основные направления использования программной защиты информации.
12. Защита информации от несанкционированного доступа.
13. Криптографические средства защиты. Общая технология шифрования.
14. Правовые основы информационной безопасности.
15. Защита информации от утечки по техническим каналам. Структура канала утечки информации.

16. Классификация каналов утечки информации.
17. Стандарты и спецификации в области информационной безопасности.
18. Стандарт «Критерии оценки доверенных компьютерных систем». Механизмы безопасности. Классы безопасности.
19. Информационная безопасность распределенных систем. Рекомендации X.800. Сетевые сервисы безопасности.
20. Стандарт ISO/IEC «Критерии оценки безопасности информационных технологий». Основные понятия.
21. Информационная безопасность в компьютерных сетях.
22. Распределение функций безопасности по уровням модели.
23. Классификация удаленных угроз в вычислительных сетях.
24. Типовые удаленные атаки и их характеристики.
25. Компьютерные вирусы как угроза информационной безопасности. Классификация компьютерных вирусов.
26. Антивирусные программы. Особенности функционирования и классификация.

7.2.5 Примерный перечень заданий для подготовки к экзамену

Не предусмотрено учебным планом

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Зачет проводится по билетам, каждый из которых содержит 2 вопроса и 10 тестовых практических тест-заданий. Каждый правильный ответ на вопрос оценивается в 5 баллов. Правильный ответ на практическое тест-задание оценивается 1 баллом. Максимальное количество набранных баллов – 20. Оценка «Незачтено» ставится в случае, если студент набрал менее 10 баллов. Оценка «Зачтено» ставится в случае, если студент набрал не менее 10 баллов.

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Основы информационной безопасности	ПК-2, ПК-6	Тест, защита лабораторных работ
2	Направления обеспечения информационной безопасности	ПК-2, ПК-6	Тест, защита лабораторных работ
3	Криптографические методы и средства защиты информации	ПК-2, ПК-6	Тест, защита лабораторных работ
4	Стандарты и спецификации в области информационной безопасности	ПК-2, ПК-6	Тест, защита лабораторных работ
5	Защита информации от утечки по техническим каналам	ПК-2, ПК-6	Тест, защита лабораторных работ
6	Информационная безопасности в	ПК-2, ПК-6	Тест, защита

	компьютерных сетях		лабораторных работ

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

1. Мельников, В.П. Информационная безопасность : Учеб. пособие / под ред. С. А. Клейменова. - 8-е изд., испр. - М. : Академия, 2013. - 336 с. - ISBN 978-5-7695-9954-5 : 797-00.

2. Чопоров О.Н. Защита информации и информационная безопасность [Электронный ресурс] : Учеб. пособие. - Электрон. текстовые, граф. дан. (1,8 Мб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2012.

3. Шаньгин, В.Ф. Информационная безопасность и защита информации [Электронный ресурс] : учебное пособие / В.Ф. Шаньгин. - Информационная безопасность и защита информации ; 2019-04-19. - Саратов : Профобразование, 2017. - 702 с. - ISBN 978-5-4488-0070-2. URL: http://www.iprbookshop.ru/63594.html

4. Прохорова, О. В. Информационная безопасность и защита информации: учебник / О.В. Прохорова. – Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 с. – ISBN 978-5-9585-0603-3. URL: http://biblioclub.ru/index.php?page=book&id=438331

5. Голиков, А.М. Защита информации от утечки по техническим каналам [Электронный ресурс] : учебное пособие / А.М. Голиков. - Томск : Томский государственный университет систем управления и

радиоэлектроники, 2015. - 256 c. URL: http://www.iprbookshop.ru/72090.html
6. Гатченко, Н. А. Криптографическая защита информации / Н. А. Гатченко, А. С. Исаев, А. Д. Яковлев. — СПб. : Университет ИТМО, 2012. — 142 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/68658.html

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

Программное обеспечение:
Microsoft Visual C++
Microsoft Visual Studio

Ресурсы информационно-телекоммуникационной сети Интернет:
http://www.edu.ru/
Образовательный портал ВГТУ

Информационная справочная система
http://window.edu.ru
https://wiki.cchgeu.ru/

Современные профессиональные базы данных
Information Security Информационная безопасность
http://www.itsec.ru/
Securitylab.ru by Positive Technologies
https://www.securitylab.ru/
Anti-Malware.ru
https://www.anti-malware.ru/news
Iso27000.ru Искусство управления информационной безопасностью
http://www.iso27000.ru/
SecurityPolicy.ru Документы по информационной безопасности
http://securitypolicy.ru/
SearchInform – Информационная безопасность
https://searchinform.ru/informatsionnaya-bezopasnost/

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Специализированная лекционная аудитория, компьютерный класс, оснащенный программным обеспечением лабораторных работ

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО

ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Информационная безопасность и защита информации» читаются лекции, проводятся лабораторные работы.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом три дня эффективнее всего использовать для повторения и систематизации материала.

11 ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Перечень вносимых изменений	Дата внесения	Подпись заведующего кафедрой,

		изменений	ответственной за реализацию ОПОП
1	Актуализирован раздел 8.1 Перечень учебной литературы, необходимой для освоения дисциплины	31.08.2020	
2	Актуализирован раздел 8.2 в части состава используемого лицензионного программного обеспечения, современных профессиональных баз данных и справочных информационных систем	31.08.2020	
3	Актуализирован раздел 8.1 Перечень учебной литературы, необходимой для освоения дисциплины	31.08.2021	