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)
«Технологии защиты Web-контента»

Направление подготовки (специальность) 09.03.02 Информационные системы и технологии

Профиль (специализация) Информационные системы и технологии цифровизации

Квалификация выпускника бакалавр

Нормативный период обучения 4 года

Форма обучения Очная

Год начала подготовки 2019 г.

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

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

Руководитель ОПОП _____ О.Г. Яскевич
подпись

Воронеж 2021

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

формирование у обучающихся знаний о методах, моделях, системах обеспечения и управления защитой web-контента; изучение математических основ защиты web-контента, методов, средств и инструментов шифрования, применяемых в сфере информационно-коммуникационных технологий

1.2. Задачи освоения дисциплины

- изучение основных методов и систем защиты информации, различных направлений обеспечения информационной безопасности в Интернет-среде;
- систематизация, формализация и расширение знаний по основным положениям теории информации, информационной безопасности и стандартами шифрования;
- освоение и использование в практической деятельности технологий защиты интернет-ресурсов на основе применения специализированных аппаратных и программных средств.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Технологии защиты Web-контента» 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 «Технологии защиты Web-контента» 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: задачи информационной безопасности в области защиты web-контента, основные тенденции и направления формирования и функционирования комплексной системы защиты информационных ресурсов сети интернет
	Уметь: применять методы и системы защиты информации для обеспечения информационной безопасности web-ресурсов
	Владеть: современными средствами и методами построения комплексных систем обеспечения защиты web-контента в телекоммуникационных системах
ПК-6	Знать: основные принципы

	административно-правовой защиты web-контента в телекоммуникационных системах
	Уметь: уметь выбирать, адаптировать и применять необходимые алгоритмы при решении профессиональных задач защиты web-контента
	Владеть: навыками использования средства защиты web-контента от несанкционированного съема и утечки по техническим каналам; использовать средства охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения.

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Технологии защиты Web-контента» составляет 3 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры
		7
Аудиторные занятия (всего)	54	54
В том числе:		
Лекции	18	18
Лабораторные работы (ЛР)	36	36
Самостоятельная работа	54	54
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 при работе с web-контентом	Основные понятия информационной безопасности при работе с web-контентом. Классификация угроз. Классификация средств защиты информации. Методы и средства организационно-правовой защиты информации. Методы и средства инженерно-технической защиты. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности	2	6	8	16
2	Криптографические методы и средства защиты интернет-ресурсов	Введение в основы современных шифров с симметричным ключом. Модульная арифметика. Сравнения и матрицы. Традиционные шифры с симметричным ключом. Алгебраические структуры. Поля. Усовершенствованный стандарт шифрования	6	8	10	24

		(AES — Advanced Encryption Standard). Простые числа. Квадратичное сравнение. Криптографическая система RSA. Криптосистемы. Простые криптосистемы. Шифрование методом замены (подстановки). Одноалфавитная подстановка. Многоалфавитная одноконтурная обыкновенная подстановка. Таблицы Вижинера. Многоалфавитная одноконтурная монофоническая подстановка. Многоалфавитная многоконтурная подстановка. Шифрование методом перестановки. Простая перестановка. Перестановка, усложненная по таблице. Перестановка, усложненная по маршрутам. Шифрование методом гаммирования. Шифрование с помощью аналитических преобразований. Комбинированные методы шифрования. Стандарты шифрования. Стандарт шифрования данных Data Encryption Standard. Режимы работы алгоритма DES. Алгоритм шифрования данных IDEA. Общая схема алгоритма IDEA				
3	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».	2	6	10	18
4	Информационная безопасности в компьютерных сетях	Защита информации в локальных сетях и глобальных сетях. Основы построения локальной компьютерной сети. Уровни антивирусной защиты. Уровень защиты рабочих станций сетевых серверов. Уровень защиты почты. Уровень защиты шлюзов. Централизованное управление антивирусной защитой. Логическая сеть. Схема сбора статистики в системе антивирусной защиты. Управление ключами шифрования и безопасность сети. Целостность сообщения и установление подлинности сообщения. Криптографические хэш-функции. Цифровая подпись. Установление подлинности объекта. Управление ключами. Безопасность на прикладном уровне: PGP и S/MIME. Безопасность на транспортном уровне: SSL и TLS. Безопасность на сетевом уровне:IP SEC. Брандмауэры. Определение типов брандмауэров. Разработка конфигурации межсетевого экрана. Построение набора правил межсетевого экрана. Система обнаружения вторжений (IDS). Узловые IDS. Анализаторы журналов. Датчики признаков. Анализаторы системных вызовов. Анализаторы поведения приложений. Контроллеры целостности файлов. Сетевые IDS. Установка IDS. Определение целей применения IDS.	6	8	16	30
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.	2	8	10	20
		Итого	**18**	**36**	**54**	**108**

5.2 Перечень лабораторных работ

1. Разработка программных средств криптографической защиты web-контента. Алгоритмы симметричного шифрования.
2. Разработка программных средств криптографической защиты web-контента. Базовые алгоритмы теории чисел.
3. Разработка программных средств криптографической защиты web-контента. Алгоритмы шифрования с открытым ключом.
4. 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: задачи информационной безопасности в области защиты web-контента, основные тенденции и направления формирования и функционирования комплексной системы защиты информационных ресурсов сети интернет	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: применять методы и системы защиты информации для обеспечения информационной безопасности web-ресурсов	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 методами построения комплексных систем обеспечения защиты web-контента в телекоммуникационных	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

	системах			
ПК-6	Знать: основные принципы административно-правовой защиты web-контента в телекоммуникационных 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
	Уметь: выбирать, адаптировать и применять необходимые алгоритмы при решении профессиональных задач защиты web-контента	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: навыками использования средства защиты web-контента 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

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: задачи информационной безопасности в области защиты web-контента, основные тенденции и направления формирования и функционирования комплексной системы защиты информационных ресурсов сети интернет	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	Уметь: применять методы и системы защиты информации для обеспечения информационной безопасности web-ресурсов	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	Владеть современными средствами и методами построения комплексных систем обеспечения защиты web-контента в телекоммуникационных системах	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
ПК-6	Знать: основные принципы административно-правовой	Тест	Выполнение теста на 70-100%	Выполнение менее 70%

	защиты web-контента в телекоммуникационных системах			
	Уметь: уметь выбирать, адаптировать и применять необходимые алгоритмы при решении профессиональных задач защиты web-контента	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	Владеть: навыками использования средства защиты web-контента от несанкционированного съема и утечки по техническим каналам; использовать средства охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения.	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. Какой метод обнаружения вирусов базируется на применении программ-ревизоров, которые следят за изменениями файлов и дисковых секторов на компьютере?

обнаружение изменений

использование резидентных сторожей

эвристический анализ

сканирование

2. Какое требование к системе защиты информации предполагает организацию единого управления по обеспечению защиты информации?

универсальность

централизованность

адекватность

непрерывность

3. Как называется это метод выбора маршрута в сетях с коммутацией каналов, учитывающий динамическое состояние выходных каналов хоста или сети?

пассивная маршрутизация

активная маршрутизация

статическая маршрутизация

динамическая маршрутизация

4. Суть какого метода криптографического преобразования информации заключается в замене исходного смысла сообщения

сочетаниями букв, цифр и знаков?

стеганография
шифрование
сжатие
кодирование

5. На каком уровне модели OSI создают туннели протоколы L2TP и PPTP?

транспортный
прикладной
канальный
сетевой

6. Как называется логическая группа устройств, имеющих возможность взаимодействовать между собой напрямую на канальном уровне, хотя физически при этом они могут быть подключены к разным сетевым коммутаторам?

виртуальная локальная сеть
виртуальная канальная сеть
защищенная магистральная сеть
виртуальная частная сеть

7. Как называется процедура проверки идентификационных данных пользователя при доступе к информационной системе?

авторизация
аутентификация
идентификация

8. Если сетевой администратор самостоятельно заполняет таблицы маршрутизации, то в сети используется…

пассивная маршрутизация
активная маршрутизация
динамическая маршрутизация
статическая маршрутизация

9. Недостатком какого метода обнаружения вирусов является большое количество ложных срабатываний антивирусных средств?

использование резидентных сторожей
эвристический анализ
сканирование
обнаружение изменений

10. Если сетевой администратор самостоятельно заполняет таблицы маршрутизации, то в сети используется…

пассивная маршрутизация

активная маршрутизация
динамическая маршрутизация
статическая маршрутизация

7.2.2 Примерный перечень заданий для решения стандартных задач

1. Для чего используется вектор инициализации?
для начала процесса расшифровки
для сжатия пакета
для аутентификации
для маршрутизации пакета

2. Как называется атака, при которой злоумышленник генерирует большое количество сообщений с разных источников для почтового сервера, чтобы реализовать ограничение доступа (или полный отказ) к этому почтовому серверу?
SYN-flood
Mailbombing
ICMP-flood
UDP-flood

3. Какие из нижеперечисленных угроз относятся к внешним угрозам?
использование сотрудниками слабых паролей для доступа к информационным системам
перехват информации с использованием радиоприемных устройств
распространение вредоносного программного обеспечения
передача сотрудниками конфиденциальной информации конкурентам
преднамеренное удаление конфиденциальной информации сотрудниками
атаки из Интернета

4. Какие системы предназначены для обеспечения сетевого мониторинга, анализа, оповещения в случае обнаружения сетевой атаки, а также способны ее блокировать?
IPS
AV
IDP
WCF

5. Как называется вредоносная программа-троян, предназначенная для скрытого удаленного управления злоумышленником пораженного компьютера?
Trojan-Mailfinder
Rootkit

Exploit
Backdoor

6. Для чего предназначены системы IDS?
для обеспечения защиты от вредоносного кода во время загрузки файлов
для обнаружения и предотвращения сетевых атак
для проверки сетевого трафика на вирусы, троянские и другие вредоносные программы
для контроля использования доступа пользователей локальной сети к интернет-ресурсам

7. Для чего при удаленном доступе к CLI применяется протокол SSH?
для преобразования IP-адресов в текстовые имена
для определения интерфейса управления
для балансировки нагрузки на сеть
для обеспечения безопасного соединения

8. Какие механизмы аутентификации беспроводных клиентов предусматривает стандарт IEEE 802.11 с традиционной безопасностью?
открытая аутентификация
аутентификация с общим ключом
назначение идентификатора беспроводной локальной сети
аутентификация клиента по MAC-адресу

9. Какой из нижеперечисленных вариантов реализации EAP основан на паролях?
PEAP
EAP-TLS
EAP-LEAP
EAP-MD5

10. Какой механизм фильтрации интернет-трафика в межсетевых экранах NetDefend помогает защитить пользователей от потенциально опасного контента веб-страниц – объектов ActiveX, Java-скриптов и т.п.?
динамическая фильтрация
статическая фильтрация
работа с активным содержимым

7.2.3 Примерный перечень заданий для решения прикладных задач
1. Как называется стандарт для виртуальных локальных сетей?
802.1ad
IEEE 802.11i
IEEE 802.1Q
IEEE 802.11

2. На каком уровне модели OSI работает proxy-служба?

сетевой

физический

сеансовый

прикладной

3. Какая функция межсетевых экранов D-Link автоматически изолирует инфицированные компьютеры локальной сети и предотвращает распространение ими вредоносного трафика?

Threshold Rules

Server Load Balancing

ZoneDefense

Traffic Shaping

4. Какой протокол поддерживает взаимную аутентификацию на базе сертификатов?

EAP-LEAP

EAP-TLS

PEAP

EAP-MD5

5. Какой протокол предназначен для того, чтобы хосты автоматически получали IP-адреса и другие параметры, необходимые для работы в сети TCP/IP?

BGP

DHCP

RIP

OSPF

6. Какой протокол использует технология ZoneDefense для блокировки трафика зараженного компьютера?

IPSec

SNMP

SSH

UDP

7. Для чего применяется параметр DPD Expire Time в межсетевых экранах D-Link?

для того чтобы задать время, по истечении которого меняется алгоритм шифрования VPN-туннеля

для того чтобы задать время, по истечении которого меняется ключ шифрования VPN-туннеля

для того чтобы исключить существование VPN «туннелей-призраков»

для того чтобы задать время, по истечении которого происходит взаимная переидентификация узлов в VPN-туннеле

8. Какой метод шифрования является наиболее стойким?
WEP
TKIP
CCMP

9. Как называется функция DIR-100, которая позволяет фильтровать нежелательные URL-адреса Web-сайтов, блокировать домены и управлять расписанием по использованию выхода в Интернет?
пограничный контроль
родительский контроль
полный контроль
прозрачный контроль

10. Для чего применяется HA-кластер?
для динамического распределения IP-адресов
для балансировки нагрузки в сети
для обеспечения отказоустойчивости сети
для обеспечения целостности передаваемых данных

11. Что такое Pipe-канал?
канал между маршрутизатором и коммутатором
объект для управления полосой пропускания
объект для управления длиной передаваемых пакетов
канал, предоставляемый поставщиком услуг

7.2.4 Примерный перечень вопросов для подготовки к зачету

1. Основные понятия информационной безопасности при работе с web-контентом. Классификация угроз. Классификация средств защиты информации.
2. Методы и средства организационно-правовой защиты информации.
3. Методы и средства инженерно-технической защиты.
4. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности
5. Введение в основы современных шифров с симметричным ключом. Модульная арифметика. Сравнения и матрицы.
6. Традиционные шифры с симметричным ключом.
7. Алгебраические структуры. Поля. Усовершенствованный стандарт шифрования (AES — Advanced Encryption Standard). Простые числа. Квадратичное сравнение.
8. Криптографическая система RSA. Криптосистемы. Простые

криптосистемы.

9. Шифрование методом замены (подстановки). Одноалфавитная подстановка. Многоалфавитная одноконтурная обыкновенная подстановка.

10. Таблицы Вижинера. Многоалфавитная одноконтурная монофоническая подстановка. Многоалфавитная многоконтурная подстановка.

11. Шифрование методом перестановки. Простая перестановка. Перестановка, усложненная по таблице.Перестановка, усложненная по маршрутам.

12. Шифрование методом гаммирования.

13. Шифрование с помощью аналитических преобразований.

14. Комбинированные методы шифрования. Стандарты шифрования.

15. Стандарт шифрования данных Data Encryption Standard. Режимы работы алгоритма DES.

16. Алгоритм шифрования данных IDEA. Общая схема алгоритма IDEA

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».

21. Защита информации в локальных сетях и глобальных сетях. Основы построения локальной компьютерной сети.

22. Уровни антивирусной защиты. Уровень защиты рабочих станций сетевых серверов. Уровень защиты почты. Уровень защиты шлюзов.

23. Централизованное управление антивирусной защитой. Логическая сеть. Схема сбора статистики в системе антивирусной защиты.

24. Управление ключами шифрования и безопасность сети. Целостность сообщения и установление подлинности сообщения.

25. Криптографические хэш-функции. Цифровая подпись. Установление подлинности объекта.

26. Управление ключами. Безопасность на прикладном уровне: PGP и S/MIME.

27. Безопасность на транспортном уровне: SSL и TLS. Безопасность на сетевом уровне:IP SEC.

28. Брандмауэры. Определение типов брандмауэров. Разработка конфигурации межсетевого экрана.

29. Построение набора правил межсетевого экрана. Система обнаружения вторжений (IDS). Узловые IDS.

30. Анализаторы журналов. Датчики признаков. Анализаторы системных вызовов. Анализаторы поведения приложений. Контроллеры целостности файлов.

31. Сетевые IDS. Установка IDS. Определение целей применения IDS.

32. Основные понятия в области технической защиты информации.

33. Защита информации от утечки по техническим каналам. Структура канала утечки информации. Классификация каналов утечки информации.

34. Аттестация объектов информатизации по требованиям безопасности.

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 при работе с web-контентом	ПК-2, ПК-6	Тест, защита лабораторных работ
2	Криптографические методы и средства защиты интернет-ресурсов	ПК-2, ПК-6	Тест, защита лабораторных работ
3	Стандарты и спецификации в области информационной безопасности	ПК-2, ПК-6	Тест, защита лабораторных работ
4	Информационная безопасности в компьютерных сетях	ПК-2, ПК-6	Тест, защита лабораторных работ
5	Защита информации от утечки по техническим каналам	ПК-2, ПК-6	Тест, защита 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 с. 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 «Технологии защиты Web-контента» 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 изменений	Подпись заведующего кафедрой, 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	31.08.2020	

	систем		
3	Актуализирован раздел 8.1 Перечень учебной литературы, необходимой для освоения дисциплины	31.08.2021	
4	Внесены изменения в связи с вступлением в силу приказа № 403-ФЗ от 2.12.2019 «О внесении изменений в Федеральный закон об образовании в Российской Федерации» и отдельные законодательные акты Российской Федерации	31.08.2021	