МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

УТВЕРЖДАЮ

И.о. декана факультета информационных технологий и компьютерной безопасности

_____ / А.В. Бредихин /

19.03.2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Технологии защиты Web-контента»

Направление подготовки 09.03.02 Информационные системы и технологии

Профиль Технологии искусственного интеллекта

Квалификация выпускника бакалавр

Нормативный период обучения 4 года

Форма обучения очная

Год начала подготовки 2024

Автор программы _____ А.В. Питолин

И.о. заведующего кафедрой систем автоматизированного проектирования и информационных систем _____ П.Ю. Гусев

Руководитель ОПОП _____ Д.В. Иванов

Воронеж 2024

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

приобретение обучающимися теоретических знаний и практических навыков в области защиты web-контента; ознакомление обучающихся с современными системами информационной безопасности, технологическими приемами защиты web-контента; возможностями использования средств информационной безопасности при работе с интернет-ресурсами

1.2. Задачи освоения дисциплины

- изучение теоретических основ, методов и средств организационно-правового и технического обеспечения защиты web-контента;
- получение знаний и навыков в области оценки защищенности web-контента в сетевых системах;
- 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.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Технологии защиты Web-контента» направлен на формирование следующих компетенций:

ПК-1 - Способен анализировать предметную область, определять современные подходы и стандарты автоматизации в процессе проектирования и разработки информационных систем;

ПК-6 - Способен выполнять работы по созданию (модификации), развертыванию и сопровождению информационных систем и ресурсов для различных прикладных областей.

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-1	знать: сущность и понятие защищенности web-контента, характеристику ее составляющих; источники угроз интернет-ресурсам и меры по их предотвращению.
	уметь: пользоваться средствами защиты web-контента при эксплуатации вычислительной техники, периферийных и мобильных устройств, других технических средств информатизации.
	владеть: современными средствами и методы построения комплексных систем обеспечения защиты

	web-контента в телекоммуникационных системах
ПК-6	знать: жизненные циклы web-контента в процессе его создания, обработки, передачи; методы оценки эффективности применяемых программно-аппаратных средств обеспечения защищенности web-ресурсов
	уметь: использовать средства защиты web-ресурса 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 (защиты web-контента) в телекоммуникационных системах

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Технологии защиты Web-контента» составляет 5 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	90	90
Часы на контроль	36	36
Виды промежуточной аттестации - экзамен	+	+
Общая трудоемкость: академические часы зач.ед.	 180 5	 180 5

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	Понятие информационной безопасности при работе с web-контентом. Основные концептуальные положения системы защиты web-контента. Угрозы конфиденциальной информации. Действия, приводящие к неправомерному овладению конфиденциальной информацией. Модель системы безопасности. Угрозы конфиденциальной информации. Классификация угроз.	4	6	14	24

2	Направления обеспечения защищенности web-контента	Направления обеспечения защищенности web-контента. Организационная защита. Правовые основы информационной безопасности. Инженерно-техническая защита. Физические средства защиты Аппаратные средства защиты Программные средства защиты. Основные направления использования программной защиты web-контента. .	4	6	14	24
3	Криптографические методы и средства защиты интернет-ресурсов	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	4	6	14	24
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».	2	6	16	24
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	6	16	24
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	2	6	16	24
		Итого	**18**	**36**	**90**	**144**

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-1	знать: сущность и понятие защищенности web-контента, характеристику ее составляющих; источники угроз интернет-ресурсам 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 web-контента 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 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
ПК-6	знать: жизненные циклы web-контента в процессе его создания, обработки, передачи; методы оценки эффективности применяемых программно-аппаратных средств обеспечения защищенности 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

	уметь: использовать средства защиты web-ресурса 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 (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

7.1.2 Этап промежуточного контроля знаний

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

7.1.2 Этап промежуточного контроля знаний

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

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ПК-1	знать: сущность и понятие информационной безопасности, характеристику ее составляющих; источники угроз информационной безопасности и меры по их предотвращению.	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь: пользоваться средствами защиты информации при эксплуатации вычислительной техники, периферийных и мобильных устройств, других технических средств информатизации.	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован 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	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
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 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	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	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован 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	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован 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

Не предусмотрено учебным планом

7.2.5 Примерный перечень заданий для подготовки к экзамену

1. Понятие информационной безопасности при работе с интернет-ресурсами (web-контентом). Основные определения.
2. Основные концептуальные положения системы защиты web-контента.
3. Модель системы безопасности.
4. Угрозы конфиденциальной информации. Классификация угроз.
5. Действия, приводящие к неправомерному овладению конфиденциальной информацией.
6. Направления обеспечения информационной защищенности web-контента.
7. Организационная защита.
8. Инженерно-техническая защита.
9. Физические средства защиты.
10. Аппаратные средства защиты.
11. Программные средства защиты. Основные направления использования программной защиты web-контента.
12. Защита информации от несанкционированного доступа.
13. Криптографические средства защиты. Общая технология шифрования.
14. Правовые основы информационной защищённости web-контента.
15. Защита Интернет-ресурсов 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.

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Экзамен проводится по билетам, каждый из которых содержит 20 тестовых вопросов. Каждый правильный ответ на вопрос оценивается в 1 балл. Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 10 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 10 до 15 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 16 до 18 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 19 до 20 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-1, ПК-6	Тест, защита лабораторных работ
2	Направления обеспечения защищенности web-контента	ПК-1, ПК-6	Тест, защита лабораторных работ
3	Криптографические методы и средства защиты интернет-ресурсов	ПК-1, ПК-6	Тест, защита лабораторных работ
4	Стандарты и спецификации в области информационной безопасности	ПК-1, ПК-6	Тест, защита лабораторных работ
5	Защита информации от утечки по техническим каналам	ПК-1, ПК-6	Тест, защита лабораторных работ
6	Информационная безопасности в компьютерных сетях	ПК-1, 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. 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

5. 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.

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	31.01.2025