МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

УТВЕРЖДАЮ
декан факультета _____С.А.Баркалов
«31» августа 2021 года

РАБОЧАЯ ПРОГРАММА
дисциплины

«Технологии защиты Web-контента»

Направление подготовки 38.03.05 БИЗНЕС-ИНФОРМАТИКА

Профиль Информационные системы в бизнесе

Квалификация выпускника бакалавр

Нормативный период обучения 4 года/4 года 11 м

Форма обучения очная/заочная

Год начала подготовки 2019

Автор программы _____/Сергеева Т.И./

Заведующий кафедрой
автоматизированных и
вычислительных систем _____/Барабанов В.Ф./

Руководитель ОПОП _____/ Наролина Т.С./

Воронеж 2021

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

освоение технологий защиты Web-контента.

1.2. Задачи освоения дисциплины

– ознакомление с методами и средствами защиты информации в сети Интернет;

– приобретение практических навыков применения стандартных программ для защиты Web-контента.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Технологии защиты Web-контента» относится к дисциплинам вариативной части (дисциплина по выбору) блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

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

ОПК-1 - способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ПК-9 - организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-1	**Знать**: – основные угрозы информационной безопасности в сети Интернет; – методы защиты информации; – средства обеспечения информационной безопасности компьютерных систем; – стандарты информационной безопасности.
	Уметь: – выбирать программные средства защиты Web-контента.
	Владеть: – методами построения системы защиты Web-контента.
ПК-9	**Знать**: – технологии защиты Web-контента.

	Уметь: – настраивать программное обеспечение для защиты Web-контента.
	Владеть: – навыками применения стандартных пакетов программ для защиты Web-контента.

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)	72	72
В том числе:		
Лекции	36	36
Лабораторные работы (ЛР)	36	36
Самостоятельная работа	72	72
Часы на контроль	36	36
Виды промежуточной аттестации - экзамен	+	+
Общая трудоемкость: академические часы зач.ед.	 180 5	 180 5

заочная форма обучения

Виды учебной работы	Всего часов	Семестры
		9
Аудиторные занятия (всего)	12	12
В том числе:		
Лекции	4	4
Лабораторные работы (ЛР)	8	8
Самостоятельная работа	159	159
Контрольная работа		
Часы на контроль	9	9
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	Введение в основы защиты информации в сети Интернет		**6**	**8**	**12**	**26**
		Информация как предмет защиты Определение информации и защищаемой информации, уровень важности информации, уровень секретности. Безопасность информации, конфиденциальность, целостность и доступность информации, угроза безопасности информации, несанкционированный доступ, политика безопасности, защита информации, информационная безопасность.	2		4	6
		Основные угрозы информационной безопасности в сети Интернет Классификация угроз информационной безопасности. Основные направления атак из сети Интернет	2	4	4	10
		Стандарты информационной безопасности Требования к комплексным системам защиты информации. Стандарты безопасности компьютерных систем. Государственные стандарты РФ по защите информации.	2	4	4	10
2	Методы и средства защиты информации в сети Интернет		**14**	**12**	**28**	**54**
		Классификация методов и средств защиты данных Понятие метода защиты, средства защиты, механизма защиты. Классификация методов защиты. Классификация средств защиты.	2		4	6
		Методы и средства обеспечения безопасности информационных систем в бизнесе. Классификация методов защиты. Классификация средств защиты.	2		4	6
		Защита компьютерных систем от вредоносных программ. Защита программных средств от несанкционированного использования и копирования Компьютерные вирусы и их свойства. Классификация вирусов. Основные виды компьютерных вирусов и схемы их функционирования. Обнаружение вирусов и меры по защите и профилактике.	2	4	4	10
		Криптографические методы защиты информации Основные определения (криптогра-	2	4	4	10

		фия, открытое сообщение, шифротекст, шифрование, шифр, ключ, криптоанализ, криптология). Симметричные и асимметричные системы шифрования. Классификация криптографических методов.	2	4	4	10
		Основные угрозы и принципы организации безопасности электронной коммерции Принципы организации безопасности. Методика построения системы безопасности. Основные угрозы безопасности и специфические риски электронной коммерции.	2		4	6
		Организация безопасности платежей в интернете Российские платежные системы. Направления обеспечения безопасности информации при организации платежей. Стандарты безопасности платежных систем.	2		4	6
		Электронная цифровая подпись Основные определения (ЭЦП, электронный документ, открытый и закрытый ключи, регистрационное свидетельство, удостоверяющий центр). Алгоритмы формирования ЭЦП. Стандарт цифровой подписи ГОСТ Р34.10-94. Новые отечественные стандарты ЭЦП.				
3	Организация защиты Web-контента		**16**	**16**	**32**	**64**
		Организация защиты информации в локальной сети Методы и средства защиты информации в сетях. Нарушение защиты информации через службы Интернет. Политика сетевой безопасности.	2	4	4	10
		Методы защиты контента Формирование входящих ссылок, оригинального контента, информации о защите контент. Блокирование копирования материала. Использование специализированных атрибутов для тегов.	2		4	6
		Системы безопасного управления контентом Технологии управления Web-контентом, контроля за обменом сообщениями, защиты от вирусов и вредоносных приложений из сети Интернет.	4		8	12
		Контролирующие системы и реализация их работы	4	4	8	16

		Системы контроля доступа сотрудников в Интернет. Контроль проникновения нелегального контента в корпоративную сеть. Контроль утечки конфиденциальной информации из корпоративной сети и фильтрация спама. Контроль проникновения вирусов. **Контентная фильтрация почтового трафика** Категории сообщений. Борьба со спамом. Контентный анализ Web-содержимого. **Обзор программных средств ведущих производителей в области контентной фильтрации**	2 2	8	4 4	14 6
Итого			**36**	**36**	**72**	**144**

заочная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Введение в основы защиты информации в сети Интернет	**Информация как предмет защиты** Определение информации и защищаемой информации, уровень важности информации, уровень секретности. Безопасность информации, конфиденциальность, целостность и доступность информации, угроза безопасности информации, несанкционированный доступ, политика безопасности, защита информации, информационная безопасность. **Основные угрозы информационной безопасности в сети Интернет** Классификация угроз информационной безопасности. Основные направления атак из сети Интернет **Стандарты информационной безопасности** Требования к комплексным системам защиты информации. Стандарты безопасности компьютерных систем. Государственные стандарты РФ по защите информации.			27 9 9 9	27 9 9 9
2	Методы и средства защиты информации в сети Интернет	**Классификация методов и средств защиты данных** Понятие метода защиты, средства защиты, механизма защиты. Классификация методов защиты. Классификация средств защиты. **Методы и средства обеспечения без-**			63 9 9	63 9 9

		опасности информационных систем в бизнесе. Классификация методов защиты. Классификация средств защиты. **Защита компьютерных систем от вредоносных программ. Защита программных средств от несанкционированного использования и копирования** Компьютерные вирусы и их свойства. Классификация вирусов. Основные виды компьютерных вирусов и схемы их функционирования. Обнаружение вирусов и меры по защите и профилактике. **Криптографические методы защиты информации** Основные определения (криптография, открытое сообщение, шифротекст, шифрование, шифр, ключ, криптоанализ, криптология). Симметричные и асимметричные системы шифрования. Классификация криптографических методов. **Основные угрозы и принципы организации безопасности электронной коммерции** Принципы организации безопасности. Методика построения системы безопасности. Основные угрозы безопасности и специфические риски электронной коммерции. **Организация безопасности платежей в интернете** Российские платежные системы. Направления обеспечения безопасности информации при организации платежей. Стандарты безопасности платежных систем. **Электронная цифровая подпись** Основные определения (ЭЦП, электронный документ, открытый и закрытый ключи, регистрационное свидетельство, удостоверяющий центр). Алгоритмы формирования ЭЦП. Стандарт цифровой подписи ГОСТ Р34.10-94. Новые отечественные стандарты ЭЦП.			9 9 9 9 9	9 9 9 9 9
3	Организация защиты Web-контента	**Организация защиты информации в локальной сети** Методы и средства защиты информа-	4 1	8 4	69 14	81 19

		ции в сетях. Нарушение защиты информации через службы Интернет. Политика сетевой безопасности.				
		Методы защиты контента Формирование входящих ссылок, оригинального контента, информации о защите контент. Блокирование копирования материала. Использование специализированных атрибутов для тегов.	1		14	15
		Системы безопасного управления контентом Технологии управления Web-контентом, контроля за обменом сообщениями, защиты от вирусов и вредоносных приложений из сети Интернет.	1		14	15
		Контролирующие системы и реализация их работы Системы контроля доступа сотрудников в Интернет. Контроль проникновения нелегального контента в корпоративную сеть. Контроль утечки конфиденциальной информации из корпоративной сети и фильтрация спама. Контроль проникновения вирусов.	1		14	15
		Контентная фильтрация почтового трафика Категории сообщений. Борьба со спамом. Контентный анализ Web-содержимого. **Обзор программных средств ведущих производителей в области контентной фильтрации**		4	13	17
Итого			**4**	**8**	**159**	**171**

5.2 Перечень лабораторных работ

Укажите перечень лабораторных работ

Неделя семестра	Наименование лабораторной работы	Объем часов	Виды контроля
7 семестр- очная форма обучения		**36**	
Введение в основы защиты информации в сети Интернет		**8**	
1	Лабораторная работа № 1. Обзор материалов об основных угрозах информационной безопасности в сети Интернет	4	Отчет
3	Лабораторная работа № 2. Создание презентации «Государственные стандарты РФ по защите информации»	4	Отчет
Методы и средства защиты информации в сети Интернет		**12**	
5	Лабораторная работа № 3. Сканирование состоя-	4	Демонстрация на

	ния безопасности компьютерной системы. Антивирусная проверка.		компьютере
7	Лабораторная работа № 4. Работа с программой шифрования электронных сообщений PGP. Формирование пары ключей, отправка открытого ключа получателям. Шифрование и расшифровка сообщений	4	Демонстрация на компьютере
9	Лабораторная работа № 5. Настройка и администрирование операционных систем для обеспечения информационной безопасности компьютерных систем	4	Демонстрация на компьютере
Организация защиты Web-контента		**16**	
11	Лабораторная работа № 6. Настройка и конфигурирование FireWall на примере бесплатно распространяемой версии. Управление доступом к ресурсам сети Интернет.	4	Демонстрация результата выполнения задания
13	Лабораторная работа № 7. Обеспечение безопасности использования WWW с помощью web-браузеров. Настройка браузера (создание зоны ограниченного доступа, формирование пароля-допуска, ограничение доступа).	4	Демонстрация на компьютере
15	Лабораторная работа № 8. Настройка работы почтовой системы. Определение данных отправителя. Обработка почты без участия пользователя. Создание правил для обработки сообщений.	4	Демонстрация на компьютере
17	Итоговое занятие. Приём отчетов. Опрос по контрольным вопросам.	4	Опрос
Итого часов по очной форме обучения		**36**	
9 семестр – заочная форма обучения		**8**	
В сессию	Лабораторная работа № 1. Настройка и конфигурирование FireWall на примере бесплатно распространяемой версии. Управление доступом к ресурсам сети Интернет.	2	Демонстрация на компьютере
В сессию	Лабораторная работа № 2. Обеспечение безопасности использования WWW с помощью web-браузеров. Настройка браузера (создание зоны ограниченного доступа, формирование пароля-допуска, ограничение доступа).	2	Демонстрация на компьютере
В сессию	Лабораторная работа № 3. Настройка работы почтовой системы. Определение данных отправителя. Обработка почты без участия пользователя. Создание правил для обработки сообщений.	2	Демонстрация на компьютере
В сессию	Итоговое занятие. Приём отчетов. Опрос по контрольным вопросам.	2	Опрос
Итого часов по заочной форме обучения		**8**	

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

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

Заочная форма обучения предусматривает выполнение контрольной работы в 9-ом семестре.

Контрольная работа состоит из двух частей: теоретическая часть и практическая часть.

Теоретическая часть включает по одному теоретическому вопросу из трех разделов учебной дисциплины.

Практическая часть включает реализацию трех заданий:

– сканирование состояния безопасности компьютерной системы; антивирусная проверка компьютера;

– работа с программой шифрования электронных сообщений PGP; формирование пары ключей, отправка открытого ключа получателям; шифрование и расшифровка сообщений;

– настройка и администрирование операционных систем для обеспечения информационной безопасности компьютерных систем.

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».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ОПК-1	Знать: - основные угрозы информационной безопасности в сети Интернет; - методы защиты информации; - средства обеспечения информационной безопасности компьютерных систем; - стандарты информационной безопасности.	Тест Решение стандартных практических задач	Выполнение теста на 60-100 % Выполнение лабораторных работ № 1-5 (лабораторной работы № 1 и контрольной работы для заочной формы обучения) в срок, предусмотренный в рабочих программах	Выполнение теста менее 60 % Невыполнение лабораторных работ (контрольной работы для заочников) в срок, предусмотренный в рабочих программах
	Уметь: - выбирать программные средства защиты Web-контента	Решение стандартных практических задач	Выполнение лабораторных работ № 1-5 (лабораторной работы № 1 и контрольной работы для заочной формы обучения) в срок, предусмотренный в рабочих программах	Невыполнение лабораторных работ (контрольной работы для заочников) в срок, предусмотренный в рабочих программах

	Владеть: - методами построения системы защиты Web-контента	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПК-9	Знать: технологии защиты Web-контента	Тест	Выполнение теста на 60-100 %	Выполнение теста менее 60 %
	Уметь: - настраивать программное обеспечение для защиты Web-контента	Решение стандартных практических задач	Выполнение лабораторных работ № 6-8 (лабораторных работ № 2-3 для заочной формы обучения) в срок, предусмотренный в рабочих программах	Невыполнение лабораторных работ в срок, предусмотренный в рабочих программах
	Владеть: - навыками применения стандартных пакетов программ для защиты Web-контента	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 7 семестре для очной формы обучения, 9 семестре для заочной формы обучения по четырехбалльной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компетенция	**Результаты обучения, характеризующие сформированность компетенции**	**Критерии оценивания**	**Отлично**	**Хорошо**	**Удовл.**	**Неудовл.**
ОПК-1	Знать: - основные угрозы информационной безопасности в сети Интернет; - методы защиты информации; - средства обеспечения информационной безопасности компьютерных систем; - стандарты 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: - выбирать программные средства защиты Web-контента	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: - методами построения системы защиты Web-контента	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-9	Знать: технологии защиты Web-контента	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	Уметь: - настраивать программное обеспечение для защиты Web-контента	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: - навыками применения стандартных пакетов программ для защиты Web-контента	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. Укажите правильный ответ

… является предметом собственности и подлежит защите в соответствии с требованиями правовых документов или требованиями, установленными собственником информации.

а) Правовая информация
б) Конфиденциальная информация
в) Защищаемая информация

2. Укажите правильный ответ

… - это административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю конкретной секретной информации.

а) Уровень секретности
б) Политика безопасности
в) Законодательные средства защиты

3. Укажите правильный ответ

… - это деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

а) Политика безопасности
б) Защита информации
в) Организационные средства защиты

4. Укажите правильный ответ

… - это неконтролируемое распространение защищаемой информации.

а) Разглашение

б) Несанкционированный доступ
в) Утечка

5. Укажите правильный ответ

… - это ситуация, когда защищаемая информация становится известной лицу, которое не должно иметь к ней доступ.

а) Угроза нарушения конфиденциальности
б) Угроза нарушения целостности
в) Угроза нарушения работоспособности

6. Укажите правильный ответ

… - это ситуация, когда происходит изменение или искажение защищаемой информации, приводящее к нарушению ее качества или полному уничтожению.

а) Угроза нарушения конфиденциальности
б) Угроза нарушения целостности
в) Угроза нарушения работоспособности

7. Укажите правильный ответ

… - это ситуация, когда происходит снижение скорости работы вычислительной системы, либо ее ресурсы становятся недоступными.

а) Угроза нарушения конфиденциальности
б) Угроза нарушения целостности
в) Угроза нарушения работоспособности

8. Укажите правильный ответ

Угрозы нарушения конфиденциальности, целостности и работоспособности – это …

а) Угрозы по предмету направленности
б) Угрозы по источнику возникновения
в) Каналы утечки
г) Воздействия

9. Укажите правильный ответ

Воздействия и каналы утечки – это ..

а) Угрозы по предмету направленности
б) Угрозы по источнику возникновения
в) Угрозы нарушения целостности информации

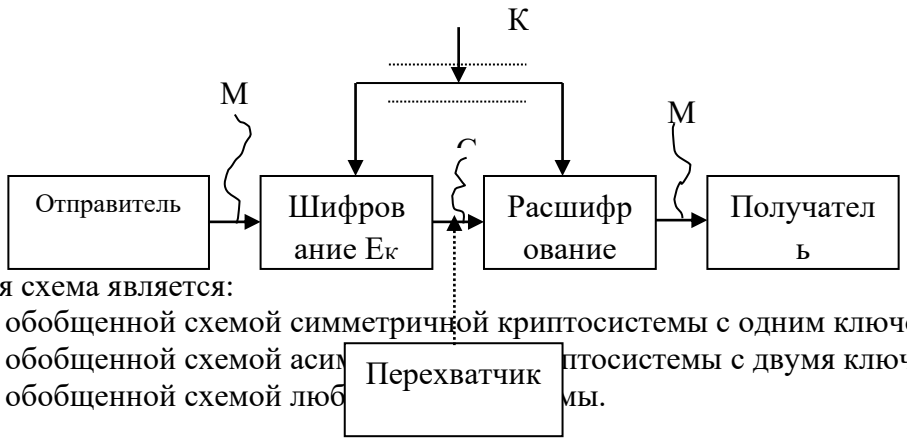
10. Укажите правильный ответ

… - воздействия природной среды (ураган, землетрясение, пожар, наводнение и т.п.).

а) Случайные воздействия
б) Природные воздействия
в) Целенаправленные воздействия
г) Внутрисистемные воздействия

7.2.2 Примерный перечень заданий для решения стандартных задач

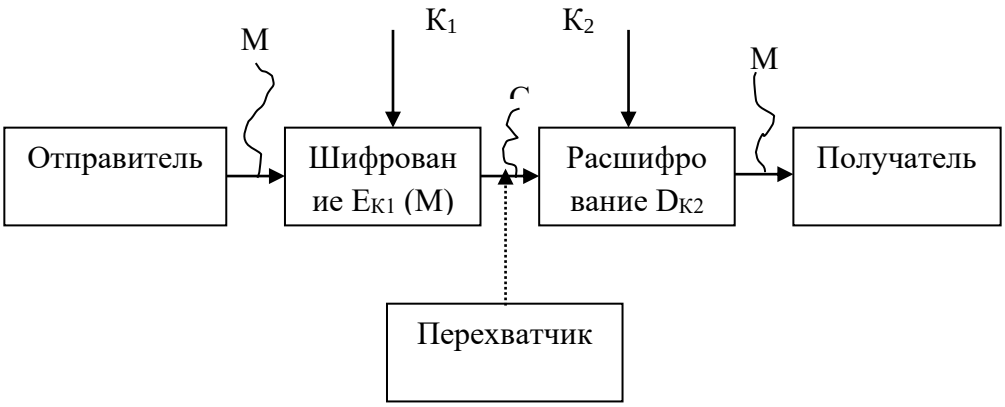
1. Представлена схема криптосистемы



Данная схема является:

а) обобщенной схемой симметричной криптосистемы с одним ключом;
б) обобщенной схемой асим птосистемы с двумя ключами;
в) обобщенной схемой люб мы.

2. Представлена схема криптосистемы



Данная схема является:

а) обобщенной схемой симметричной криптосистемы с закрытым ключом;
б) обобщенной схемой асимметричной криптосистемы;
в) обобщенной схемой любой криптосистемы.

3. Дана формула замены

$$Yi=k1*Xi+k2(mod\ N)$$

где Yi - i-й символ алфавита шифротекста (номер буквы в алфавите);
k1 и k2 - константы;
Xi - i-й символ открытого текста (номер буквы в алфавите);
N - длина используемого алфавита.

Данная формула реализует:

а) Гомофоническую замену;
б) Моноалфавитную замену;
в) Полиалфавитную замену;
г) Полиграммную замену.

4. Шифр, задаваемый формулой:

$yi=xi+ki(mod\ N)$,

где ki - i-ая буква ключа, в качестве которого используются слово или фраза, называется

а) шифром Вижинера;
б) шифром Бофора;
в) шифром Плейфера.

5. Шифр, задаваемый формулой:

$yi=ki-xi(mod\ n)$ *и*

$yi=xi-ki(mod\ n)$.

называется

а) шифром Вижинера;
б) шифром Бофора;
в) шифром Плейфера.

6. … означает, что одному символу открытого текста ставит в соответствие несколько символов шифротекста. Этот метод применяется для искажения статистических свойств шифротекста.

а) Моноалфавитная замена;

б) Гомофоническая замена;
в) Полиалфавитная замена.

7. … использует несколько алфавитов шифртекста.

Пусть используется k алфавитов. Тогда открытый текст: $X=X_1X_2...X_k\ X_{k+1}...X_{2k}\ X_{2k+1}...$ заменяется шифртекстом:

$Y=F1(X1)F2(X2)...Fk(Xk)\ F1(Xk+1)...Fk(X2k)\ F1(X2k+1)...$

где Fi(Xj) означает символ шифртекста алфавита i для символа открытого текста Xj.

а) Гомофоническая замена;
б) Полиалфавитная замена;
в) Моноалфавитная замена.

8. … формируется из одного алфавита с помощью специальных правил.

В качестве примера рассмотрим шифр Плэйфера.

В этом шифре алфавит располагается в матрице. Открытый текст разбивается на пары символов X_iX_{i+1}. Каждая пара символов открытого текста заменяется на пару символов из матрицы следующим образом:

1) если символы находятся в одной строке, то каждый из символов пары заменяется на стоящий правее его (за последним символом в строке следует первый);

2) если символы находятся в одном столбце, то каждый символ пары заменяется на символ, расположенный ниже его в столбце (за последним нижним символом следует верхний);

3) если символы пары находятся в разных строках и столбцах, то они считаются противоположными углами прямоугольника. Символ, находящийся в левом углу, заменяется на символ, стоящий в другом левом углу; замена символа, находящегося в правом углу, осуществляется аналогично;

4) если в открытом тексте встречаются два одинаковых символа подряд, то перед шифрованием между шали вставляется специальный символ (например, тире).

а) Полиалфавитная замена;
б) Полиграммная замена;
в) Гомофоническая замена.

9. … использует преобразование вида:

$Y=CX.$

где $Y=||y_1,y_2, ...,y_n||^T$.

$C=||C_{ij}||$

$X=||x_1,x_2, ...,x_n||$

а) Решение задачи об укладке ранца;
б) Вычисление значения полинома по модулю;
в) Метод умножения матриц.

10. … формулируется следующим образом.

Задан вектор $C=|c_1,c_2,...,c_n|$, который используется для шифрования сообщения, каждый символ s_i которого представлен последовательностью из n бит $s_i=|x_1,x_2,...,x_n|$, $x_k \in \{0,1\}$. Шифротекст получается как скалярное произведение $C \cdot s_i$.

а) Задача об укладке ранца;
б) Задача умножения матриц;
в) Задача вычисления значения полинома по модулю.

7.2.3 Примерный перечень заданий для решения прикладных задач

1. Как осуществить настройку уровня защиты для зоны безопасности Интернет?

а) Пуск, Панель управления, Свойства обозревателя, вкладка Безопасность, выбор зоны Интернет, переместить ползунок уровня безопасности;

б) Пуск, Панель управления, Брандмауэр Windows, выбор зоны Интернет, переместить ползунок уровня безопасности;

в) Пуск, Панель управления, Свойства обозревателя, вкладка Безопасность, кнопка Другой, выбор уровня безопасности из списка.

2. Как осуществить настройку уровня защиты для зоны ограниченных узлов?

а) Пуск, Панель управления, Свойства обозревателя, вкладка Безопасность, выбор Ограниченные узлы, переместить ползунок уровня безопасности;

б) Пуск, Панель управления, Свойства обозревателя, вкладка Безопасность, выбор Ограниченные узлы, кнопка Другой, выбор уровня безопасности из списка;

в) Пуск, Панель управления, Свойства обозревателя, вкладка Безопасность, кнопка Другой, выбор уровня безопасности из списка.

3. Как добавить web-узел в список зоны с ограничением доступа?

а) Пуск, Панель управления, Свойства обозревателя, вкладка Безопасность, выбрать из списка зон нужную зону (например, Ограниченные узлы), щелкнуть по кнопке Узлы, ввести в поле «Добавить узел в зону» адрес web-сайта и щелкнуть по кнопке «Добавить», ОК, ОК.

б) Пуск, Панель управления, Свойства обозревателя, вкладка Безопасность, ввести в поле «Добавить узел в зону» адрес web-сайта и щелкнуть по кнопке «Добавить», ОК, ОК.

в) Пуск, Панель управления, Свойства обозревателя, вкладка Подключение, ввести в поле «Добавить узел в зону» адрес web-сайта и щелкнуть по кнопке «Добавить», ОК, ОК.

4. Как осуществить ограничение доступа к информации, получаемой из Интернета?

а) Пуск, Панель управления, Свойства обозревателя, вкладка Содержание, кнопка Включить, в окне «Ограничения доступа» выбрать вкладку Оценки, выбрать категорию из списка (например, Насилие), установить бегунок на нужном уровне, кнопка Применить, ОК, будет предложено установить пароль-допуск, дважды ввести пароль-допуск, ОК.

б) Пуск, Панель управления, Свойства обозревателя, вкладка Безопасность, кнопка Включить, в окне «Ограничения доступа» выбрать вкладку Оценки, выбрать категорию из списка (например, Насилие), установить бегунок на нужном уровне, кнопка Применить, ОК, будет предложено установить пароль-допуск, дважды ввести пароль-допуск, ОК.

в) Пуск, Панель управления, Свойства обозревателя, вкладка Содержание, кнопка Добавить, в окне «Ограничения доступа» выбрать вкладку Общие, выбрать категорию из списка (например, Насилие), установить бегунок на нужном уровне, кнопка Применить, ОК, будет предложено установить пароль-допуск, дважды ввести пароль-допуск, ОК.

5. Как запретить посещение нежелательных web-страниц, не имеющих оценок?

а) Пуск, Панель управления, Свойства обозревателя, вкладка Содержание, кнопка Включить, перейти во вкладку «Разрешенные узлы», ввести в поле «Разрешить просмотр следующего узла» адрес web-сайта. Щелкнуть по кнопке «Всегда», если разрешить всегда посещать данный сайт, или щелкнуть по кнопке «Никогда», если запретить просмотр содержимого данного сайта независимо от оценок.

б) Пуск, Панель управления, Свойства обозревателя, вкладка Общие, кнопка Настройка, перейти во вкладку «Разрешенные узлы», ввести в поле «Разрешить просмотр следующего узла» адрес web-сайта. Щелкнуть по кнопке «Всегда», если разрешить всегда посещать данный сайт, или щелкнуть по кнопке «Никогда», если запретить просмотр содержимого данного сайта независимо от оценок.

в) Пуск, Панель управления, Свойства обозревателя, вкладка Безопасность, кнопка Настройка, перейти во вкладку «Разрешенные узлы», ввести в поле «Разрешить просмотр

следующего узла» адрес web-сайта. Щелкнуть по кнопке «Всегда», если разрешить всегда посещать данный сайт, или щелкнуть по кнопке «Никогда», если запретить просмотр содержимого данного сайта независимо от оценок.

6. Как определить адрес отправителя электронной почты?

а) Запустить почтового клиента MS Outlook Express, выбрать папку Входящие, выделить сообщение, вызвать контекстное меню, Свойства, вкладка Подробности, изучить заголовок письма. В заголовке письма записывается весь путь его прохождения через цепь почтовых серверов. В самом последнем абзаце, начинающимся словом Received, находится адрес первого сервера, на который отправлено письмо.

б) Запустить почтового клиента MS Outlook Express, выбрать папку Исходящие, выделить сообщение, вызвать контекстное меню, Свойства, вкладка Подробности, изучить заголовок письма. В заголовке письма записывается весь путь его прохождения через цепь почтовых серверов. В самом последнем абзаце, начинающимся словом Received, находится адрес первого сервера, на который отправлено письмо.

в) Запустить почтового клиента MS Outlook Express, выбрать папку Входящие, выделить сообщение, вызвать контекстное меню, Свойства, вкладка Общие, изучить заголовок письма. В заголовке письма записывается весь путь его прохождения через цепь почтовых серверов. В самом последнем абзаце, начинающимся словом Received, находится адрес первого сервера, на который отправлено письмо.

7. Как установить фильтр на анализ содержания входящей почты для удаления сообщения?

а) Запустить почтового клиента MS Outlook Express, Сервис, Правила для сообщений, Почта, в окне «Выбрать условие для данного правила» установить флажок «Искать сообщения, содержащие заданные слова», в окне «Выберите действия для данного правила» установить флажок Удалить, в списке «Описание правила» щелкнуть по ссылке «содержащие заданные слова». В раскрывшемся окне «Ввод ключевых слов» ввести ключевые слова и щелкнуть по кнопке Добавить. В этом же окне щелкнуть по кнопке Параметры, в открывшемся окне «Условия для правила» активировать переключатель «Имеются указанные слова» и щелкнуть по кнопке ОК, ОК.

б) Запустить почтового клиента MS Outlook Express, Сервис, Правила для сообщений, Почта, в окне «Выбрать условие для данного правила» установить флажок «Искать сообщения, содержащие заданные слова в поле «Тема», в окне «Выберите действия для данного правила» установить флажок Удалить, в списке «Описание правила» щелкнуть по ссылке «содержащие заданные слова». В раскрывшемся окне «Ввод ключевых слов» ввести ключевые слова и щелкнуть по кнопке Добавить. В этом же окне щелкнуть по кнопке Параметры, в открывшемся окне «Условия для правила» активировать переключатель «Имеются указанные слова» и щелкнуть по кнопке ОК, ОК.

в) Запустить почтового клиента MS Outlook Express, Сервис, Правила для сообщений, Почта, в окне «Выбрать условие для данного правила» установить флажок «Искать сообщения, содержащие заданные слова», в окне «Выберите действия для данного правила» установить флажок «Скопировать в заданную папку», в списке «Описание правила» щелкнуть по ссылке «содержащие заданные слова». В раскрывшемся окне «Ввод ключевых слов» ввести ключевые слова и щелкнуть по кнопке Добавить. В этом же окне щелкнуть по кнопке Параметры, в открывшемся окне «Условия для правила» активировать переключатель «Имеются указанные слова» и щелкнуть по кнопке ОК, ОК.

8. Как создать правило обработки входящих почтовых сообщений, согласно которому сообщения, включающие определенные слова, удаляются?

а) Запустить почтового клиента MS Outlook Express, Сервис, Правила для сообщений, Почта, в окне «Выбрать условие для данного правила» установить флажок «Искать сообще-

ния, содержащие заданные слова в поле «Тема», в окне «Выберите действия для данного правила» установить флажок Удалить, в списке «Описание правила» щелкнуть по ссылке «содержащие заданные слова». В раскрывшемся окне «Ввод ключевых слов» ввести ключевые слова и щелкнуть по кнопке Добавить. В этом же окне щелкнуть по кнопке Параметры, в открывшемся окне «Условия для правила» активировать переключатель «Имеются указанные слова» и щелкнуть по кнопке ОК, ОК.

б) Запустить почтового клиента MS Outlook Express, Сервис, Правила для сообщений, Почта, в окне «Выбрать условие для данного правила» установить флажок «Искать сообщения, содержащие заданные слова», в окне «Выберите действия для данного правила» установить флажок «Скопировать в заданную папку», в списке «Описание правила» щелкнуть по ссылке «содержащие заданные слова». В раскрывшемся окне «Ввод ключевых слов» ввести ключевые слова и щелкнуть по кнопке Добавить. В этом же окне щелкнуть по кнопке Параметры, в открывшемся окне «Условия для правила» активировать переключатель «Имеются указанные слова» и щелкнуть по кнопке ОК, ОК.

в) Запустить почтового клиента MS Outlook Express, Сервис, Правила для сообщений, Почта, в окне «Выбрать условие для данного правила» установить флажок «Искать сообщения, содержащие заданные слова», в окне «Выберите действия для данного правила» установить флажок Удалить, в списке «Описание правила» щелкнуть по ссылке «содержащие заданные слова». В раскрывшемся окне «Ввод ключевых слов» ввести ключевые слова и щелкнуть по кнопке Добавить. В этом же окне щелкнуть по кнопке Параметры, в открывшемся окне «Условия для правила» активировать переключатель «Имеются указанные слова» и щелкнуть по кнопке ОК, ОК.

9. Как установить фильтр на тему входящей почты?

а) Запустить почтового клиента MS Outlook Express, Сервис, Правила для сообщений, Почта, в окне «Выбрать условие для данного правила» установить флажок «Искать сообщения, содержащие заданные слова в поле «Тема», в окне «Выберите действия для данного правила» установить нужный флажок, в списке «Описание правила» щелкнуть по ссылке «содержащие заданные слова». В раскрывшемся окне «Ввод ключевых слов» ввести ключевые слова и щелкнуть по кнопке Добавить. В этом же окне щелкнуть по кнопке Параметры, в открывшемся окне «Условия для правила» активировать переключатель «Имеются указанные слова» и щелкнуть по кнопке ОК, ОК.

б) Запустить почтового клиента MS Outlook Express, Сервис, Правила для сообщений, Почта, в окне «Выбрать условие для данного правила» установить флажок «Искать сообщения, содержащие адресатов в поле «От», в окне «Выберите действия для данного правила» установить нужный флажок, в списке «Описание правила» щелкнуть по ссылке «содержащие заданные слова». В раскрывшемся окне «Ввод ключевых слов» ввести ключевые слова и щелкнуть по кнопке Добавить. В этом же окне щелкнуть по кнопке Параметры, в открывшемся окне «Условия для правила» активировать переключатель «Имеются указанные слова» и щелкнуть по кнопке ОК, ОК.

б) Запустить почтового клиента MS Outlook Express, Сервис, Правила для сообщений, Почта, в окне «Выбрать условие для данного правила» установить флажок «Искать сообщения, содержащие адресатов в поле «Кому», в окне «Выберите действия для данного правила» установить нужный флажок, в списке «Описание правила» щелкнуть по ссылке «содержащие заданные слова». В раскрывшемся окне «Ввод ключевых слов» ввести ключевые слова и щелкнуть по кнопке Добавить. В этом же окне щелкнуть по кнопке Параметры, в открывшемся окне «Условия для правила» активировать переключатель «Имеются указанные слова» и щелкнуть по кнопке ОК, ОК.

10 Как заблокировать сообщения, получаемые от отправителя с определенным адресом?

а) Запустить почтового клиента MS Outlook Express, Сервис, Правила для сообщений, Список блокируемых отправителей, во вкладке «Заблокированные отправители» в окне «Правила для сообщений» щелкнуть по кнопке Добавить. В окне «Добавить отправителя» ввести адрес электронной почты и установить флажок «Почтовые сообщения», ОК, ОК.

б) Запустить почтового клиента MS Outlook Express, Сервис, Правила для сообщений, Почта, во вкладке «Заблокированные отправители» в окне «Правила для сообщений» щелкнуть по кнопке Добавить. В окне «Добавить отправителя» ввести адрес электронной почты и установить флажок «Почтовые сообщения», ОК, ОК.

в) Запустить почтового клиента MS Outlook Express, Сервис, Правила для сообщений, Почта, в окне «Выбрать условие для данного правила» установить флажок «Искать сообщения, содержащие адресатов в поле «От», в окне «Выберите действия для данного правила» установить нужный флажок, в списке «Описание правила» щелкнуть по ссылке «содержащие заданные слова». В раскрывшемся окне «Ввод ключевых слов» ввести ключевые слова и щелкнуть по кнопке Добавить, ОК, ОК.

7.2.4 Примерный перечень вопросов для подготовки к зачету

Не предусмотрено учебным планом

7.2.5 Примерный перечень вопросов для подготовки к экзамену

1. Основные направления защиты компьютерной информации в сети Интернет
2. Информация как предмет защиты, конфиденциальная информация, защищаемая информация, уровень секретности, защита информации
3. Определения: безопасность информации, целостность информации, конфиденциальность информации
4. Определения: угроза безопасности информации, несанкционированный доступ к информации, политика безопасности
5. Основные угрозы информации по предмету направленности, по источнику возникновения
6. Виды воздействий, реализующие угрозу безопасности данных
7. Косвенные и прямые каналы утечки данных
8. Модель потенциального нарушителя
9. Определения: методы защиты, средства защиты, механизмы защиты
10. Определение метода защиты. Методы защиты: управление, препятствия, маскировка.
11. Определение метода защиты. Методы защиты: регламентация, побуждение, принуждение.
12. Классификация средств защиты
13. Физические средства защиты данных
14. Законодательные средства защиты компьютерной информации
15. Организационные средства защиты компьютерной информации
16. Аппаратные средства защиты
17. Программные средства защиты компьютерной информации
18. Требования к комплексным системам защиты компьютерной информации
19. Стандарты безопасности КС
20. Криптография. Шифрование. Шифр. Ключ. Криптоанализ. Криптология.
21. Симметричные системы шифрования.
22. Асимметричные системы шифрования.
23. Классификация криптографических методов.
24. Методы замены: моноалфавитная, гомофоническая, полиалфавитная, полиграммная.

25. Методы перестановки. Методы гаммирования
26. Обобщенная схема симметричной криптосистемы
27. Обобщенная схема асимметричной криптосистемы
28. Компьютерные вирусы и их свойства. Классификация вирусов.
29. Основные виды компьютерных вирусов и схемы их функционирования.
30. Обнаружение вирусов и меры по защите и профилактике.
31. Безопасность электронной коммерции. Информационная безопасность. Направления информационной безопасности.
32. Принципы защиты электронной коммерции (общие принципы, организационные, принципы реализации).
33. Методика построения системы безопасности электронной коммерции.
34. Основные угрозы информационной безопасности электронной коммерции.
35. Убытки. Прямые убытки. Косвенные убытки. Специфические риски электронной коммерции.
36. Направления обеспечения безопасности информации при организации электронных платежей.
37. Стандарты безопасности платежных систем.
38. Электронная цифровая подпись (ЭЦП). Электронный документ. Задачи, решаемые ЭЦП.
39. Открытый и закрытый ключи ЭЦП. Регистрационное свидетельство.
40. Формирование и проверка ЭЦП. Алгоритмы формирования ЭЦП.
41. Стандарт цифровой подписи ГОСТ Р34.10-94.
42. Нарушение защиты информации через службы Интернет. Политика сетевой безопасности.
43. Методы защиты контента: формирование входящих ссылок, оригинального контента, информации о защите контент.
44. Методы защиты контента: блокирование копирования материала. Использование специализированных атрибутов для тегов.
45. Системы безопасного управления контентом: технологии управления Web-контентом,
46. Системы безопасного управления контентом: технологии контроля за обменом сообщениями
47. Контролирующие системы и реализация их работы: системы контроля доступа сотрудников в Интернет.
48. Контролирующие системы и реализация их работы: контроль проникновения нелегального контента в корпоративную сеть.
49. Контролирующие системы и реализация их работы: контроль утечки конфиденциальной информации из корпоративной сети и фильтрация спама.
50. Контентная фильтрация почтового трафика: Категории сообщений. Борьба со спамом.
51. Контентная фильтрация почтового трафика: контентный анализ Web-содержимого.

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Экзамен проводится по билетам, включающим по два вопроса. Допуском к экзамену является выполнение всех лабораторных работ и положительное текущее тестирование по темам лекций первого и второго разделов.

Оценка на экзамене выставляется следующим образом.

1. Оценка «Неудовлетворительно» ставится в случае, если студент не ответил ни на один вопрос

2. Оценка «Удовлетворительно» ставится в случае, если студент ответил на один вопрос в полном объеме, изложив общие понятия и методики

3. Оценка «Хорошо» ставится в случае, если студент ответил на два вопроса в полном объеме, но не ответил на уточняющие вопросы по тематике вопросов билета.

4. Оценка «Отлично» ставится, если ответил на два вопроса в полном объеме, а также ответил на уточняющие вопросы по тематике вопросов ответа.

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Введение в основы защиты информации в сети Интернет	ОПК-1, ПК-9	Тест, контрольная работа (для заочников), защита лабораторных работ, экзамен, устный опрос
2	Методы и средства защиты информации в сети Интернет	ОПК-1, ПК-9	Тест, контрольная работа (для заочников), защита лабораторных работ, экзамен, устный опрос
3	Организация защиты Web-контента	ОПК-1, ПК-9	Тест, защита лабораторных работ, экзамен, устный опрос

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

Тестирование осуществляется по теоретическому материалу, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30- 45 мин. Затем осуществляется проверка теста преподавателем. Тест пройден, если количество правильных ответов составляет 60 – 100 %.

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 преподавателем. Тест пройден, если количество правильных ответов составляет 60 – 100 %.

Решение прикладных задач осуществляется на лабораторных работах и при тестировании. Разработанная программа или выполненное задание по настройке параметров стандартной программы должны отвечать заданным требованиям. Время выполнения лабораторной работы составляет 4 часа. Время тестирования составляет 30 мин. Тест пройден, если количество правильных ответов составляет 60 – 100 %.

Экзамен сдается по билетам из двух вопросов. Допуском к экзамену является выполнение всех лабораторных работ и положительное текущее тестирование по темам лекций первого и второго разделов.

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.
2. Анисимов, А. А. Менеджмент в сфере информационной безопасности : учебное пособие / А. А. Анисимов. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 211 с. — ISBN 978-5-4497-0328-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/89443.html (дата обращения: 30.01.2022). — Режим доступа: для авторизир. Пользователей
3. Аверченков, В. И. Аудит информационной безопасности : учебное пособие для вузов / В. И. Аверченков. — Брянск : Брянский государственный технический университет, 2012. — 268 с. — ISBN 978-89838-487-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/6991.html (дата обращения: 30.01.2022). — Режим доступа: для авторизир. пользователей

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:

Лицензионное ПО
LibreOffice

Ресурс 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
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/
Ekrost.ru - Информационная безопасность предприятия

Системное программное обеспечение:

Операционная система семейства Windows NT корпорации Microsoft

Лицензионное прикладное программное обеспечении:

Система программирования Visual Studio 2010 и выше; RAD Studio;

бесплатно распространяемые версии программ шифрования электронных сообщений, защиты компьютерных сетей, браузер.

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Лекционная аудитория и аудитории для практических занятий, оснащённые мультимедийным демонстрационным оборудованием (проектор, экран, звуковоспроизводящее оборудование), обеспечивающим демонстрацию мультимедиаматериалов.

Аудитории для лабораторных занятий, оснащенные компьютерами с лицензионным программным обеспечением с возможностью подключения к сети «Интернет» и доступом в электронную информационно образовательную среду университета.

Аудитории для самостоятельной работы, оборудованные техническими средствами обучения: персональными компьютерами с лицензионным программным обеспечением с возможностью подключения к сети «Интернет» и доступом в электронную информационно-образовательную среду университета

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; - работа над темами для самостоятельного изучения; - подготовка к лабораторным работам и оформление отчетов по лабораторным работам; - 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. Три дня перед экзаменом эффективнее всего использовать для повторения и систематизации материала.

6 Лист регистрации изменений

№ п/п	Перечень вносимых изменений	Дата внесения изменений	Подпись заведующего кафедрой, ответственной за реализацию ОПОП
1	Внесены изменения в рабочие программы дисциплин в части состава используемого лицензионного программного обеспечения, современных профессиональных баз данных и справочных информационных систем	31.08.2020	
2	Внесены изменения в рабочие программы дисциплин в части состава используемого лицензионного программного обеспечения, современных профессиональных баз данных и справочных информационных систем	31.08.2021	
3	Актуализирован перечень литературы, необходимой для освоения дисциплины	31.08.2021	