МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

имени академика М.Д. Миллионщикова

«УТВЕРЖДАЮ»

Первый проректор

И.Г. Гайрабеков

«01» 09 2022 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Информационная безопасность в цифровой экономике»

Направление подготовки

09.03.03 Прикладная информатика

Направленность (профиль)

«Прикладная информатика в экономике»

Квалификация

бакалавр

Год начала подготовки: 2022

Грозный - 2022

1. Цели и задачи освоения дисциплины

Целью изучения дисциплины является ознакомление студентов с основными понятиями и определениями информационной безопасности; источниками, рисками и формами атак на информацию; угрозами, которыми подвергается информация; вредоносными программами; защитой от компьютерных вирусов и других вредоносных программам; методами и средствами защиты информации; политикой безопасности компании в области информационной безопасности; стандартами информационной безопасности; криптографическими методами и алгоритмами шифрования информации; алгоритмами аутентификации пользователей; защитой информации в сетях; требованиям к системам защиты информации.

Задача дисциплины: ознакомить студентов с тенденциями развития защиты информации с моделями возможных угроз, терминологией и основными понятиями теории защиты информации, а так же с нормативными документами и методами защиты компьютерной информации.

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к блоку 1. Часть, формируемая участниками образовательных отношений. Для изучения дисциплины требуется освоение следующих дисциплин: «Информатика», «Программирование», «Экономико-правовые основы рынка ПО», «Вычислительные системы, сети и телекоммуникации», «Операционные системы», «Теория экономических информационных систем», «Проектирование информационных систем».

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Таблица 1

Код по ФГОС	Индикаторы достижения	Планируемые результаты обучения по дисциплине (ЗУВ)
Общепрофессиональные		

ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1. Формулирует принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности	Знать виды угроз ИС и методы обеспечения информационной безопасности; правовые основы защиты компьютерной информации; стандарты; Уметь выявлять и оценивать угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС; Владеть навыками работы с различными источниками информации;
	ОПК-3.2 Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности	Знать требования информационных систем; Уметь проводить анализ информационной безопасности объектов информатизации на соответствие требованиям стандартов в области информационной безопасности; Владеть навыками построения системы информационной безопасности в условиях действующих угроз, формирования комплекса средств защиты;
Профессиональные		
ПК-2 Способен разрабатывать и адаптировать прикладное программное обеспечение	ПК-2.1. Проектирует и разрабатывает прототипы ИС	Знать методы идентификации; модели и методы криптографии; Уметь применять методы защиты компьютерной информации при использовании и проектировании ИС в различных областях; Владеть навыками работы с программно-инструментальными средствами
ПК-5 Способен принимать участие	ПК-5.3 Обеспечивает управление доступом к данным с учетом	Знать требования информационных систем и методы обеспечения информационной безопасности;

в организации ИТ-инфраструктуры и управлении информационной безопасностью	требований организации ИТ-инфраструктуры.	Уметь проводить обследования, выявлять информационные потребности пользователей, формировать требования к информационной системе; Владеть навыками эксплуатирования и сопровождения информационных систем и сервисов

4. Объем дисциплины и виды учебной работы

Таблица 2

Вид учебной работы		**Всего часов/з.ед.**		**Семестры**			
				ОФО	**ОФО**	**ЗФО**	**ЗФО**
		ОФО	**ЗФО**	**7**	**8**	**8**	**9**
Контактная работа (всего)		**104/2.8**	**36/1**	**68/1.8**	**36/13**	**16/0.4**	**20/0.5**
В том числе:							
Лекции		46/1.2	20/0.5	34/0.9	12/0.3	8/0.2	12/0.3
Лабораторные работы (ЛР)		58/1.6	16/0.4	34/0.9	24/0.6	8/0.2	8/0.2
Практические занятия (ПР)		0	0	0	0	0	0
Самостоятельная работа (всего)		**256/7**	**324/9**	**40/1.1**	**216/6**	**128/**	**196/5.4**
В том числе:							
Реферат		102/2.8	98/2.8	30/0.8	72/2	64/3.5	34/0.94
Курсовой проект		**72/2**	128/3.5		72/2	0	128/3.5
Темы для самостоятельного изучения		**10/0.2**	66/1.8	10/0.2		32/0.8	34/0.94
Подготовка к лабораторным работам и к экзаменам		**72/2**	32/0.8		72/2	32/0.8	
Вид отчетности		Зач/экз	Зач/экз	Зачет	экзамен	Зачет	экзамен
Общая трудоемкость дисциплины	**ВСЕГО в часах**	**360**	**360**	**108**	**252**	**144**	**216**
	ВСЕГО в зач. единицах	**10**	**10**	**3**	**7**	**4**	**6**

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Таблица 2.1

ЗФО

№ п/п	**Наименование раздела дисциплины по семестрам**	**Лекционные занятия**	**Лабораторные занятия**	**Всего часов**

1	Введение в информационную безопасность Задачи и методы информационной безопасности	4	4	8
2	Угрозы информационной безопасности Потенциальные противники и атаки	**4**	**4**	**8**
3	Стандарты обеспечения ИБ Организационно-правовые методы информационной безопасности	4	4	8
4	Законодательный уровень информационной безопасности Административный уровень информационной безопасности	4	2	6
5	Основные положения теории информационной безопасности информационных систем Управление рисками	4	2	6

Таблица 2.2

ОФО

№ п/п	**Наименование раздела дисциплины по семестрам**	**Лекционные занятия**	**Лабораторные занятия**	**Всего часов**
1	Введение в информационную безопасность	2	4	6
2	Задачи и методы информационной безопасности	**4**		**8**
3	Угрозы информационной безопасности	4	4	8
4	Потенциальные противники и атаки	4		8
5	Стандарты обеспечения ИБ	2	4	6
6	Организационно-правовые методы информационной безопасности	2	4	6
7	Законодательный уровень информационной безопасности	2	4	6
8	Административный уровень информационной безопасности	2	4	6
9	Основные положения теории информационной безопасности информационных систем	2	4	6
10	Основные технологии построения защищенных экономических информационных систем.	2	2	4
11	Управление рисками	2	2	4
12	Процедурный уровень информационной безопасности	2	2	4
13	Программно-технические методы защиты	2	2	4
14	Идентификация и аутентификация	2	2	4
15	Сервисы управления доступом	2	2	4
16	Протоколирование и аудит	2	2	4
17	Экранирование и анализ защищенности	2	2	4
18	Тунелирование и управление	2	2	4
19	Обеспечение высокой доступности	2	2	4
20	Криптографические методы защиты	2	2	4

5.2. Разделы дисциплины и виды занятий

Лекционные занятия

Таблица 3

№ п/п	**Наименование раздела дисциплины**	**Содержание раздела**
7 семестр		

1.	Введение в информационную безопасность	Понятие "Информационная безопасность в цифровой экономике" 1. Проблема информационной безопасности общества 2. Определение понятия "Информационная безопасность в цифровой экономике" 3. Составляющие информационной безопасности
2.	Задачи и методы информационной безопасности	1. Задачи информационной безопасности общества 2. Уровни формирования режима информационной безопасности
3.	Угрозы информационной безопасности	Угрозы информационной безопасности
4.	Потенциальные противники и атаки	Потенциальные противники и атаки
5.	Стандарты обеспечения ИБ	Стандарты информационной безопасности 1. Общие критерии 2. Стандарты информационной безопасности распределенных систем 3. Стандарты информационной безопасности в РФ
6.	Организационно-правовые методы информационной безопасности	Организационно-правовые методы информационной безопасности
7.	Законодательный уровень информационной безопасности	1. Правовые основы информационной безопасности общества 2. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации Ответственность за нарушения в сфере информационной безопасности
8.	Административный уровень информационной безопасности	1. Цели, задачи и содержание административного уровня 2. Разработка политики информационной безопасности
9.	Основные положения теории информационной безопасности информационных систем	Основные положения теории информационной безопасности информационных систем
10.	Основные технологии построения защищенных экономических информационных систем.	Основные технологии построения защищенных экономических информационных систем.
11.	Управление рисками	Управление рисками
12.	Процедурный уровень информационной безопасности	Процедурный уровень информационной безопасности
13.	Программно-технические методы защиты	Программно-технические методы защиты
14.	Идентификация и аутентификация	Идентификация и аутентификация
8 семестр		
15.	Сервисы управления доступом	Сервисы управления доступом
16.	Протоколирование и аудит	Протоколирование и аудит

17.	Экранирование и анализ защищенности	Экранирование и анализ защищенности
18.	Тунелирование и управление	Тунелирование и управление
19.	Обеспечение высокой доступности	Обеспечение высокой доступности
20.	Криптографические методы защиты	Криптографические методы защиты

5.3. Практических занятий- нет

5.4 Лабораторный практикум

ОФО– 7семестр, ЗФО-8 семестр

№	Наименование раздела	Наименование лабораторных работ
1.	**Лабораторная работа №1.** Установка и удаление сертификатов.	Работа со справкой: сертификаты, безопасные узлы.Установка и удаление сертификатов. Подготовка отчета
2.	**Лабораторная работа №2.** Настройка уровня безопасности, конфиденциальности и эффективности работы программы INTERNET EXPLORER.	**Первичные настройки обозревателя, назначение веб-узлу зоны безопасности, настройки автозаполнения, средств безопасности**
3.	**Лабораторная работа №3. Анализ угроз и защищенности объекта.**	Виды угроз и характер происхождения угроз
4.	**Лабораторная работа №3. Анализ угроз и защищенности объекта.**	Классы каналов несанкционированного получения информации, источники проявления угроз
5.	**Лабораторная работа №3. Анализ угроз и защищенности объекта.**	Причины нарушения целостности информации, потенциально возможные злоумышленные действия.
6.	**Лабораторная работа №3. Анализ угроз и защищенности объекта.**	Определить требования к защите Определить факторы, влияющие на требуемый уровень защиты информации
7.	**Лабораторная работа №3. Анализ угроз и защищенности объекта.**	Построить архитектуру систем защиты информации. Сформулировать предложения по увеличению защищенности информации

ОФО - 8 семестр, ЗФО – 9 семестр

№ п/п	Наименование раздела	Наименование лабораторных работ
1	**Лабораторная работа №4** **Разграничение прав пользователей в защищенных версиях операционной системы Windows**	освоение средств администратора операционной системы Windows.
2	**Лабораторная работа №5** **Реализация политики безопасности в версиях операционной системы Windows**	освоения средств администратора и аудитора версий операционной системы Windows, предназначенных для • определения параметров политики безопасности; • определения параметров политики аудита; • просмотра и очистки журнала аудита.

3	**Лабораторная работа №6** **Разграничение доступа к ресурсам в версиях операционной системы Windows**	освоение средств операционной системы Windows, предназначенных для: • разграничения доступа субъектов к папкам и файлам; • разграничения доступа субъектов к принтерам; • разграничения доступа к разделам реестра; • обеспечения конфиденциальности папок и файлов с помощью шифрующей файловой системы.

6. Самостоятельная работа студентов по дисциплине

6.1. Темы для рефератов 7, 8 семестр

№ п/п	Темы для рефератов
1.	Обеспечение информационной безопасности в банковских и финансовых структурах
2.	Анализ мирового рынка биометрических систем, используемых в системах обеспечения информационной безопасности
3.	Анализ мирового рынка антивирусного программного обеспечения
4.	Электронная цифровая подпись.
5.	Компьютерная преступность в России
6.	Модель угроз информации на территории РФ
7.	Алгоритмы цифровой подписи
8.	Способы защиты операционных систем
9.	Экономические основы защиты конфиденциальной информации
10.	Анализ мирового рынка антивирусного программного обеспечения
11.	Аудит безопасности корпоративных информационных систем
12.	Безопасность электронной почты и Интернет
13.	Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний
14.	Виды аудита информационной безопасности
15.	Выбор показателей защищенности от несанкционированного доступа к информации
16.	Государственная система защиты информации РФ
17.	Методы защиты аудио и визуальных документов
18.	Методы защиты документов на бумажных носителях
19.	Методы и средства обеспечения безопасности ПО
20.	Методы скрытой передачи информации
21.	Методы экономического анализа систем информационной безопасности
22.	Проблемы безопасности и пути их решения в современных компьютерных сетях
23.	Современные технологии архивирования данных
24.	Технологии резервного копирования данных
25.	Управление безопасностью приложений (на примере компании….)

6.2. Вопросы для самостоятельного изучения 8, 9 семестр

№ п/п	Темы для самостоятельного изучения

1.	Проблемы безопасности в локальных сетях
2.	Технологии защиты Web-ресурсов от взлома и хакерских атак
3.	Проблемы безопасности в глобальных сетях
4.	Политика информационной безопасности в РФ
5.	Политика информационной безопасности в США
6.	Концепция электронного документа и проблемы правового регулирования электронно-цифровой подписи
7.	Стандарты шифрования
8.	Методы защиты речевой информации
9.	Виды компьютерных правонарушений.
10.	Методы защиты аудио и визуальных документов
11.	Методы защиты документов на бумажных носителях
12.	Методы внедрения программных закладок
13.	Методы защиты информации в Интернет.
14.	Методы защиты от макро-вирусов
15.	Методы защиты программ от несанкционированных изменений
16.	Методы защиты речевой информации
17.	Методы и средства борьбы со спамом
18.	Методы и средства обеспечения безопасности ПО
19.	Методы перехвата и навязывания информации
20.	Методы поиска и сбора информации.
21.	Методы скрытой передачи информации
22.	Методы экономического анализа систем информационной безопасности
23.	Методы защиты аудио и визуальных документов
24.	Методы защиты документов на бумажных носителях
25.	Методы внедрения программных закладок
26.	Методы защиты информации в Интернет.

6.3. Темы курсовых проектов

№	**Темы курсовых проектов**
1.	Сравнительный и оценочный анализ международных стандартов в области информационной безопасности и управления рисками.
2.	Анализ методов и средств анализа защищенности беспроводных сетей.
3.	Анализ зарубежного рынка средств обеспечения информационной безопасности беспроводных сетей.
4.	Разработка комплексной защиты информации на предприятии
5.	Анализ российского рынка средств обеспечения информационной безопасности беспроводных сетей
6.	Анализ средств защиты от спама.
7.	Разработка системы защиты персональных данных в предприятии
8.	Сравнительный анализ методов перехвата паролей пользователей компьютерных систем и методов противодействия им
9.	Анализ схем мошенничества в сети Интернет
10.	Оценочный анализ методов и средств тестирования системы защиты

	вычислительных сетей (аудита информационной безопасности).
11.	Разработка мер по технической защите конфиденциальной информации в организации
12.	Анализ безопасности ОС Linux
13.	Сравнительный анализ средств защиты электронной почты
14.	Разработка комплексной системы защиты коммерческой информации
15.	Анализ внедрения технологий цифровой подписи в РФ
16.	Анализ возможности применения средств защиты информации на предприятиях
17.	Разработка системы управления кадровой безопасностью организации
18.	Разработка типового проекта защиты локальной вычислительной сети предприятия
19.	Разработка политики информационной безопасности.
20.	Анализ основных угроз электронного документооборота
21.	Анализ критических характеристик линий связи с точки зрения обеспечения защиты информации
22.	Сравнительный анализ систем обнаружения атаки
23.	Сравнительный анализ программных средств, реализующих стеганографические методы защиты информации.
24.	Сравнительный анализ международных стандартов в области информационной безопасности и управления рисками
25.	Разработка системы информационной безопасности банка
26.	Сравнительный анализ способов информационного воздействия в сети Интернет
27.	Анализ современных средств анализа защищенности
28.	Сравнительный анализ методов аутентификации пользователей.
29.	Разработка мероприятий защиты персональных данных в организации.
30.	Анализ средств защиты компакт-дисков от несанкционированного копирования.
31.	Сравнительный анализ инструментальные средства анализа рисков информационной безопасности.
32.	Анализ основных угроз электронного документооборота - фундамент электронного бизнеса.

7. Оценочные средства

7.1 Вопросы к рубежным аттестациям

Вопросы к первой рубежной аттестации 7 семестр

1. Введение в информационную безопасность
2. Задачи и методы информационной безопасности
3. Угрозы информационной безопасности
4. Потенциальные противники и атаки
5. Стандарты обеспечения ИБ
6. Организационно-правовые методы информационной безопасности

Образец билета к первой рубежной аттестации (7 семестр)

Грозненский государственный нефтяной технический университет
Институт цифровой экономики и технологического предпринимательства

Кафедра «Информационные системы в экономике»
Группа "ПИ-21" Семестр "7"
Дисциплина "Информационная безопасность в цифровой экономике"
Билет № 3

1. Управление рисками
2. Экранирование и анализ защищенности

Преподаватель ***Абдулаев М.К.***

Зав. кафедрой «ИСЭ» ***Л.Р. Магомаева***

Вопросы ко второй рубежной аттестации 7 семестр

1. Законодательный уровень информационной безопасности
2. Административный уровень информационной безопасности
3. Основные положения теории информационной безопасности информационных систем
4. Основные технологии построения защищенных экономических информационных систем.
5. Модель угроз информации на территории РФ
6. Способы защиты операционных систем
7. Анализ мирового рынка антивирусного программного обеспечения
8. Компьютерная преступность в России

Образец билета ко второй рубежной аттестации (7 семестр)

Грозненский государственный нефтяной технический университет
Институт цифровой экономики и технологического предпринимательства

Кафедра «Информационные системы в экономике»
Группа "ПИ-21" Семестр "7"
Дисциплина "Информационная безопасность в цифровой экономике"
Билет № 3

1. Основные технологии построения защищенных экономических информационных систем.
2. Модель угроз информации на территории РФ

Преподаватель ***Абдулаев М.К.***

Зав. кафедрой «ИСЭ» ***Л.Р. Магомаева***

Вопросы к первой рубежной аттестации 8 семестр

1. Управление рисками
2. Процедурный уровень информационной безопасности
3. Программно-технические методы защиты
4. Идентификация и аутентификация
5. Сервисы управления доступом

Образец билета к первой рубежной аттестации (8 семестр)

Грозненский государственный нефтяной технический университет
Институт цифровой экономики и технологического предпринимательства

Кафедра «Информационные системы в экономике»
Группа "ПИ-21" Семестр "8"
Дисциплина "Информационная безопасность в цифровой экономике"
Билет № 3

1. Процедурный уровень информационной безопасности
2. Программно-технические методы защиты

Преподаватель ***Абдулаев М.К.***

Зав. кафедрой «ИСЭ» ***Л.Р. Магомаева***

Вопросы ко второй рубежной аттестации 8 семестр

1. Протоколирование и аудит
2. Экранирование и анализ защищенности
3. Тунелирование и управление
4. Обеспечение высокой доступности
5. Криптографические методы защиты

Образец билета ко второй рубежной аттестации (8 семестр)

Грозненский государственный нефтяной технический университет
Институт цифровой экономики и технологического предпринимательства

Кафедра «Информационные системы в экономике»
Группа "ПИ-21" Семестр "8"
Дисциплина "Информационная безопасность в цифровой экономике"
Билет № 3

1. Обеспечение высокой доступности
2. Криптографические методы защиты

Преподаватель ***Абдулаев М.К.***

Зав. кафедрой «ИСЭ» ***Л.Р. Магомаева***

7.2 Вопросы к зачету (7семестр)

1. Введение в информационную безопасность
2. Задачи и методы информационной безопасности
3. Угрозы информационной безопасности
4. Потенциальные противники и атаки
5. Стандарты обеспечения ИБ
9. Законодательный уровень информационной безопасности
10. Административный уровень информационной безопасности
11. Основные положения теории информационной безопасности информационных систем
12. Основные технологии построения защищенных экономических информационных систем.
13. Модель угроз информации на территории РФ
14. Способы защиты операционных систем
15. Анализ мирового рынка антивирусного программного обеспечения
16. Компьютерная преступность в России

Образец билета к зачету (7 семестр)

Грозненский государственный нефтяной технический университет
Институт цифровой экономики и технологического предпринимательства

Кафедра «Информационные системы в экономике»
Группа "ПИ-21" Семестр "8"
Дисциплина "Информационная безопасность в цифровой экономике"
Билет № 3

1. Угрозы информационной безопасности
2. Потенциальные противники и атаки

Преподаватель ***Абдулаев М.К.***

Зав. кафедрой «ИСЭ» ***Л.Р. Магомаева***

Вопросы к экзамену

1. Управление рисками
2. Процедурный уровень информационной безопасности
3. Программно-технические методы защиты
4. Идентификация и аутентификация
5. Сервисы управления доступом
6. Протоколирование и аудит
7. Экранирование и анализ защищенности
8. Тунелирование и управление
9. Обеспечение высокой доступности
10. Криптографические методы защиты
11. Протоколирование и аудит
12. Экранирование и анализ защищенности

Образец билета к экзамену (8 семестр)

Грозненский государственный нефтяной технический университет
Институт цифровой экономики и технологического предпринимательства

Кафедра «Информационные системы в экономике»
Группа "ПИ-21" Семестр "8"
Дисциплина "Информационная безопасность в цифровой экономике"
Билет № 3

1. Криптографические методы защиты
2. Протоколирование и аудит

Преподаватель ***Абдулаев М.К.***

Зав. кафедрой «ИСЭ» ***Л.Р. Магомаева***

7.3 Текущий контроль

7 семестр

Лабораторная работа №1.

Установка и удаление сертификатов.

Лабораторная работа №2.

Настройка уровня безопасности, конфиденциальности и эффективности работы программы INTERNET EXPLORER.

Лабораторная работа №3.

8 семестр

Анализ угроз и защищенности объекта.

Лабораторная работа №4

Создание самоподписанных сертификатов.

Лабораторная работа №5

Реализация политики безопасности в версиях операционной системы Windows

Лабораторная работа №6

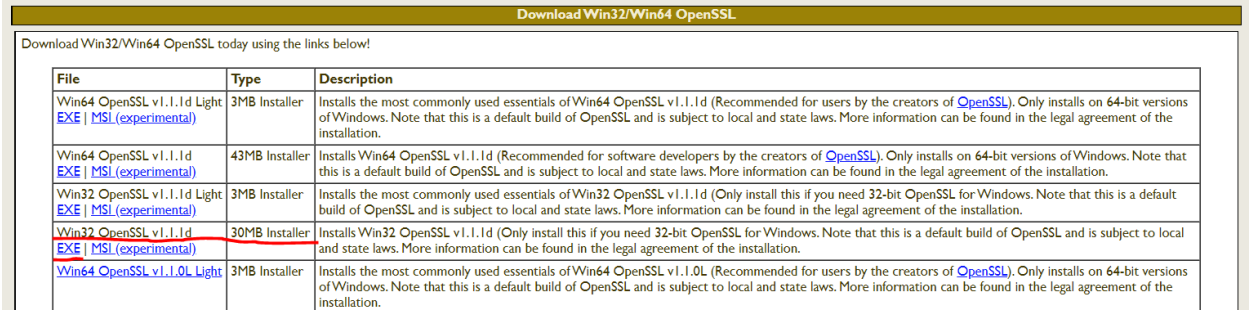
Разграничение доступа к ресурсам в версиях операционной системы Windows

Образец лабораторной работы

Лабораторная работа №4.
Создание самоподписанных сертификатов.

1. Расписать: Описание SSL-сертификатов, для чего они применяются, каких видов бывают. Описание .pem, .crt, .cer, .key, .csr ключей.
2. Найти в сети Интернет 3 ресурса для покупки Wildcard SSL-сертификатов с наиболее низкой ценой. В отчет внести скриншоты с указанием цен.
3. Скачать и установить полную 32-битную или 64-битную версию OpenSSL (EXE) в зависимости от разрядности вашей ОС.

Ссылка на скачивание https://slproweb.com/products/Win32OpenSSL.html

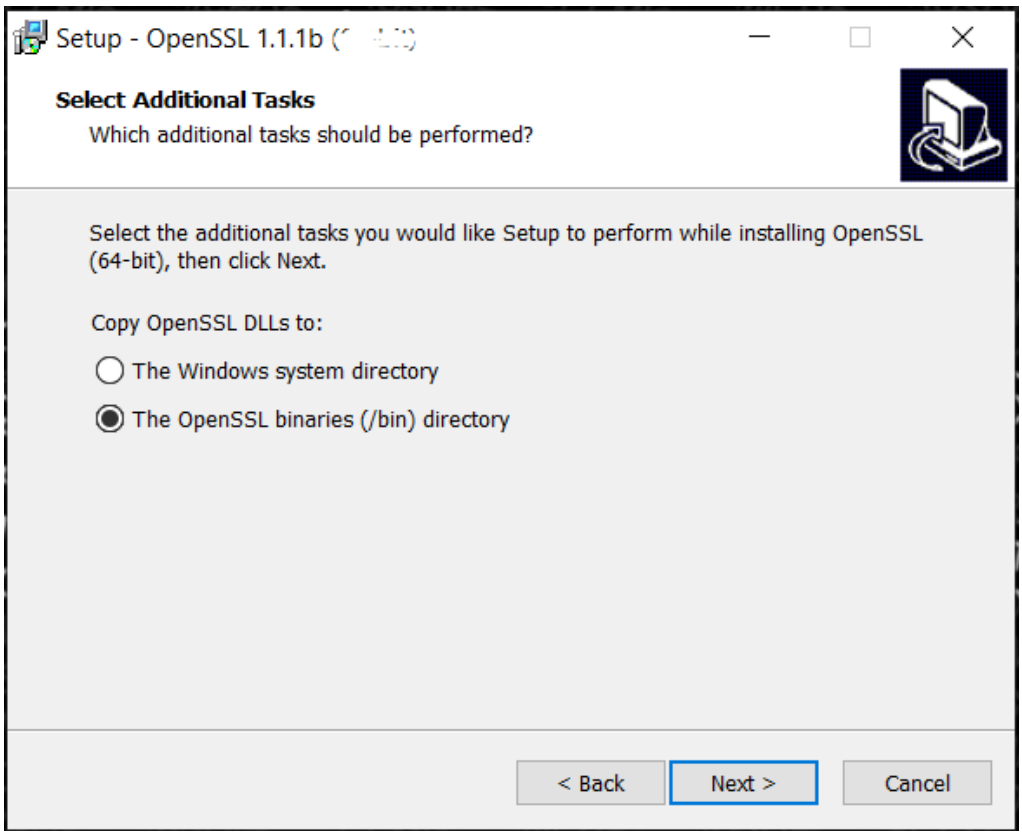


Download Win32/Win64 OpenSSL

Download Win32/Win64 OpenSSL today using the links below!

File	Type	Description
Win64 OpenSSL v1.1.1d Light EXE | MSI (experimental)	3MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v1.1.1d (Recommended for users by the creators of OpenSSL). Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v1.1.1d EXE | MSI (experimental)	43MB Installer	Installs Win64 OpenSSL v1.1.1d (Recommended for software developers by the creators of OpenSSL). Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win32 OpenSSL v1.1.1d Light EXE | MSI (experimental)	3MB Installer	Installs the most commonly used essentials of Win32 OpenSSL v1.1.1d (Only install this if you need 32-bit OpenSSL for Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win32 OpenSSL v1.1.1d EXE | MSI (experimental)	30MB Installer	Installs Win32 OpenSSL v1.1.1d (Only install this if you need 32-bit OpenSSL for Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v1.1.0L Light	3MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v1.1.0L (Recommended for users by the creators of OpenSSL). Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.

При установке на пункте выбора места копирования DLL-файлов, ОБЯЗАТЕЛЬНО выбрать директорию /bin



Запустить программу openssl.exe от имени администратора из папки C:\Program Files\OpenSSL-Win32\bin (в 64-битной версии возможно расположение C:\Program Files (x86)\OpenSSL-Win32\bin).

4. Создать самоподписанный сертификат следуя инструкциям. В отчет внести скриншоты по каждому выполняемому шагу. В наименовании файлов вместо “domain” использовать вашу фамилию латинскими буквами.

Создание закрытого ключа и запроса на подпись.

Чтобы создать закрытый ключ и запрос на подпись открытого ключа выполните такую команду:

После чего необходимо указать следующие сведения на латинице:

- *2х буквенное обозначение страны*
- *Республику*
- *Населенный пункт*
- *Название организации – Свою фамилию*
- *Отдел – IT*
- *Доменное имя, вида «имя».ru*
- *Свой email*
- *Указать какой-либо пароль*
- *Дополнительно название компании – Свое имя.*

```
req -newkey rsa:2048 -nodes -keyout domain.key -out domain.csr
```

```
Country Name (2 letter code) [AU]:RU
State or Province Name (full name) [Some-State]:Chechen Republic
Locality Name (eg, city) []:Grozny
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Zaurbekov
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:rizvan.ru
Email Address []:rizvan@mail.ru

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:12345678
An optional company name []:Rizvan
OpenSSL>
```

Подпись сертификатов.
Выполните команду для подписания сертификата сроком 365 дней:
Внести в отчет скриншот содержания папки C:\Program Files\OpenSSLWin32\
bin , где по умолчанию создаются ключи.

7.4. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания.

Таблица 7

Планируемые результаты освоения компетенции	**Критерии оценивания результатов обучения**				**Наименование оценочного средства**
	менее 41 баллов (неудовлетворительно)	**41-60 баллов (удовлетворительно**	**61-80 баллов (хорошо)**	**81-100 баллов (отлично)**	
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности					
Знать: виды угроз ИС и методы обеспечения информационной безопасности; правовые основы защиты компьютерной информации; стандарты;	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	*задания для контрольной работы, тестовые задания, билеты рубежных аттестаций, темы рефератов*
Уметь: выявлять и оценивать угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть: навыками работы с различными источниками информации	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ПК-2 Способен разрабатывать и адаптировать прикладное программное обеспечение					
Знать: методы идентификации; модели и методы криптографии,	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	*задания для контрольной работы, тестовые задания, билеты рубежных аттестаций, темы рефератов*
Уметь: применять методы защиты компьютерной информации при использовании и проектировании ИС в различных областях	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	

Владеть: навыками работы с программно-инструментальными средствами	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ПК-5 Способен принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью					
Знать: требования информационных систем и методы обеспечения информационной безопасности;	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	*задания для контрольной работы, тестовые задания, билеты рубежных аттестаций, темы рефератов*
Уметь: проводить обследования, выявлять информационные потребности пользователей, формировать требования к информационной системе	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть: навыками эксплуатирования и сопровождения информационных систем и сервисов	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	

8. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации обучающихся созданы фонды оценочных средств, адаптированные для инвалидов и лиц с ограниченными возможностями здоровья и позволяющие оценить достижение ими запланированных в основной образовательной программе результатов обучения и уровень сформированности всех компетенций, заявленных в образовательной программе. Форма проведения текущей аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). При тестировании для слабовидящих студентов используются фонды оценочных средств с укрупненным шрифтом. На экзамен приглашается сопровождающий, который обеспечивает техническое сопровождение студенту. При необходимости студенту-инвалиду предоставляется дополнительное время для подготовки ответа на экзамене (или зачете). Обучающиеся с ограниченными возможностями здоровья и обучающиеся инвалиды обеспечиваются печатными и электронными образовательными ресурсами (программы, учебные пособия для самостоятельной работы и т.д.) в формах, адаптированных к ограничениям их здоровья и восприятия информации:

1) для инвалидов и лиц с ограниченными возможностями здоровья **по зрению:**

- для слепых: задания для выполнения на семинарах и практических занятиях оформляются рельефно-точечным шрифтом Брайля или в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением для слепых, либо зачитываются ассистентом; письменные задания выполняются на бумаге рельефно-точечным шрифтом Брайля или на компьютере со специализированным программным обеспечением для слепых либо надиктовываются ассистенту; обучающимся для выполнения задания при необходимости предоставляется комплект письменных принадлежностей и бумага для письма рельефно-точечным шрифтом Брайля, компьютер со специализированным программным обеспечением для слепых;

- для слабовидящих: обеспечивается индивидуальное равномерное освещение не менее 300 люкс; обучающимся для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; задания для выполнения заданий оформляются увеличенным шрифтом;

2) для инвалидов и лиц с ограниченными возможностями здоровья **по слуху:**

- **для глухих и слабослышащих:** обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающимся предоставляется звукоусиливающая аппаратура индивидуального пользования; предоставляются услуги сурдопереводчика;

- **для слепоглухих** допускается присутствие ассистента, оказывающего услуги

тифлосурдопереводчика (помимо требований, выполняемых соответственно для слепых и глухих);

3) для лиц с тяжелыми нарушениями речи, глухих, слабослышащих лекции и семинары, проводимые в устной форме, проводятся в письменной форме;

4) для инвалидов и лиц с ограниченными возможностями здоровья, **имеющих нарушения опорно-двигательного аппарата:**

- для лиц с нарушениями опорно-двигательного аппарата, нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей: письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту; выполнение заданий (тестов, контрольных работ), проводимые в письменной форме, проводятся в устной форме путем опроса, беседы с обучающимся.

9. Учебно-методическое и информационное обеспечение дисциплины

9.1 Литература

1. Защита информации в корпоративных информационно-вычислительных сетях/ Игнатьев В.А.,2018 – Библиотека ГГНТУ;

2. Введение в информационную безопасность/Малюк А.А.-2017. – Библиотека ГГНТУ;

3. Информационная безопасность в цифровой экономике и защита информации/Громов Ю.Ю.,2018 – Библиотека ГГНТУ;

4. Васильев, В.И. Интеллектуальные системы защиты информации /Машиностроение, 2019 – ЭБС «Лань»;

5. Фомин Д.В. Информационная безопасность в цифровой экономике [Электронный ресурс]: учебно-методическое пособие по дисциплине «Информационная безопасность в цифровой экономике» для студентов экономических специальностей заочной формы обучения/ Фомин Д.В.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2018.— 54 c.— Режим доступа: http://www.iprbookshop.ru/77320.html.— ЭБС «IPRbooks»

6.Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс]/ Анисимов А.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 212 c.— Режим доступа: http://www.iprbookshop.ru/52182.html.— ЭБС «IPRbooks»

1. http://internetsecure.ru/ InternetSecure.ru — безопасность в интернет — набор технологий и программ для работы в сети и с компьютером

2. http://www.securityportal.ru/ Security Portal .RU — сведения по защите информации, защите приватности, безопасным сетевым взаимодействиям, криптографии.

3. http://www.oszone.net/6213/ Обеспечение безопасности детей при работе в Интернет (статья, ссылки, материалы)

9.2. Методические указания для обучающихся для освоения дисциплины (приложение)

10. Материально-техническое обеспечение дисциплины «Информационная безопасность в цифровой экономике»

10.1

Для проведения качественного обучения в лаборатории используется предоставленное ведущими фирмами-разработчиками современного уровня программное обеспечение.

1 Google Chrome.
2 Правовая ИС «Гарант +», «Консультант»
3 Электронный замок "Соболь"
4 СЗИ от НСД Secret Net

В лаборатории содержатся электронные версии методических указаний к лабораторным работам, вопросы к экзамену.

10.2

Помещение для самостоятельной работы (Главный учебный корпус ФГБОУ ВО «Грозненский государственный нефтяной технический университет» 364902, Чеченская республика, г. Грозный, проспект им. Х.А. Исаева, 100.

Аудитория оснащена необходимой компьютерной техникой, в наличии есть необходимое ПО:

WinPro 10 RUS Uprgrd OLP NL Acdmc;

OfficeStd RUS OLP NL Acdmc (право на использование согласно Контракту № 267-ЭА/19 от 15.09.2019 г.) Система ГАРАНТ (пропиетарная лицензия)

Visual Studio-(Freemium)

1С Предприятие договор от 02.12.2020 регистрационные номера продуктов (9334859; 9334952) Sublime Text- (открытый доступ)

Notepad++ (открытый доступ

Приложение

Методические указания по освоению дисциплины «Информационная безопасность в цифровой экономике»

1. Методические указания для обучающихся по планированию и организации времени, необходимого для освоения дисциплины.

Изучение рекомендуется начать с ознакомления с рабочей программой дисциплины, ее структурой и содержанием разделов (модулей), фондом оценочных средств, ознакомиться с учебно-методическим и информационным обеспечением дисциплины.

Дисциплина «Информационная безопасность в цифровой экономике» состоит из 20 связанных между собою тем, обеспечивающих последовательное изучение материала.

Обучение по дисциплине «Информационная безопасность в экономике» осуществляется в следующих формах:

1. Аудиторные занятия (лекции, лабораторные занятия).
2. Самостоятельная работа студента (подготовка к лекциям, лабораторным занятиям, рефератам и иным формам письменных работ, индивидуальная консультация с преподавателем).
3. Интерактивные формы проведения занятий (лекция-дискуссия, групповое решение кейса и др. формы).

Учебный материал структурирован и изучение дисциплины производится втематической последовательности. Каждому лабораторному занятию и самостоятельному изучению материала предшествует лекция по данной теме. Обучающиеся самостоятельно проводят предварительную подготовку к занятию, принимают активное и творческое участие в обсуждении теоретических вопросов, разборе проблемных ситуаций и поисков путей их решения. Многие проблемы, изучаемые в курсе, носят дискуссионный характер, что предполагает интерактивный характер проведения занятий на конкретных примерах.

Описание последовательности действий обучающегося:

При изучении курса следует внимательно слушать и конспектировать материал, излагаемый на аудиторных занятиях. Для его понимания и качественного усвоения рекомендуется следующая последовательность действий:

1. После окончания учебных занятий для закрепления материала просмотреть и обдумать текст лекции, прослушанной сегодня, разобрать рассмотренные примеры (10 – 15 минут).
2. При подготовке к лекции следующего дня повторить текст предыдущей лекции, подумать о том, какая может быть следующая тема (10 - 15 минут).
3. В течение недели выбрать время для работы с литературой в библиотеке (по 1 часу).
4. При подготовке к лабораторному занятию повторить основные понятия по теме, изучить примеры. Решая конкретную ситуацию, - предварительно понять, какой теоретический материал нужно использовать. Наметить план решения, попробовать на его основе решить 1 - 2 практические ситуации.

2. Методические указания по работе обучающихся во время проведения лекций.

Лекции дают обучающимся систематизированные знания по дисциплине, концентрируют их внимание на наиболее сложных и важных вопросах. Лекции обычно излагаются в традиционном или в проблемном стиле. Для студентов в большинстве случаев в проблемном стиле. Проблемный стиль позволяет стимулировать активную познавательную деятельность обучающихся и их интерес к дисциплине, формировать творческое мышление, прибегать к противопоставлениям и сравнениям, делать обобщения, активизировать внимание обучающихся путем постановки проблемных вопросов, поощрять дискуссию.

Во время лекционных занятий рекомендуется вести конспектирование учебного материала, обращать внимание на формулировки и категории, раскрывающие суть того или иного явления, или процессов, выводы и практические рекомендации.

Конспект лекции лучше подразделять на пункты, соблюдая красную строку. Этому в

большой степени будут способствовать вопросы плана лекции, предложенные преподавателям. Следует обращать внимание на акценты, выводы, которые делает преподаватель, отмечая наиболее важные моменты в лекционном материале замечаниями
«важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек, подчеркивая термины и определения.

Целесообразно разработать собственную систему сокращений, аббревиатур и символов. Однако при дальнейшей работе с конспектом символы лучше заменить обычными словами для быстрого зрительного восприятия текста.

Работая над конспектом лекций, необходимо использовать не только основную литературу, но и ту литературу, которую дополнительно рекомендовал преподаватель. Именно такая серьезная, кропотливая работа с лекционным материалом позволит глубоко овладеть теоретическим материалом.

Тематика лекций дается в рабочей программе дисциплины.

3. Методические указания обучающимся по подготовке к практическим/семинарским занятиям.

На практических занятиях приветствуется активное участие в обсуждении конкретных ситуаций, способность на основе полученных знаний находить наиболее эффективные решения поставленных проблем, уметь находить полезный дополнительный материал по тематике семинарских занятий.

Студенту рекомендуется следующая схема подготовки к семинарскому занятию:

1. Ознакомление с планом практического занятия, который отражает содержание предложенной темы;

2. Проработать конспект лекций;

3. Прочитать основную и дополнительную литературу.

В процессе подготовки к практическим занятиям, необходимо обратить особое внимание на самостоятельное изучение рекомендованной литературы. При всей полноте конспектирования лекции в ней невозможно изложить весь материал из-за лимита аудиторных часов. Поэтому самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов отношение к конкретной проблеме. Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса;

4. Ответить на вопросы плана практического занятия;

5. Выполнить домашнее задание;

6. Проработать тестовые задания и задачи;

7. При затруднениях сформулировать вопросы к преподавателю.

Результат такой работы должен проявиться в способности студента свободно ответить на теоретические вопросы практикума, выступать и участвовать в коллективном обсуждении вопросов изучаемой темы, правильно выполнять практические задания и иные задания, которые даются в фонде оценочных средств дисциплины.

3. Методические указания обучающимся по организации самостоятельной работы.

Цель организации самостоятельной работы по дисциплине «Информационная безопасность в экономике» - это углубление и расширение знаний в области гуманитарных наук; формирование навыка и интереса к самостоятельной познавательной деятельности.

Самостоятельная работа обучающихся является важнейшим видом освоения содержания дисциплины, подготовки к практическим занятиям и к контрольной работе. Сюда же относятся и самостоятельное углубленное изучение тем дисциплины. Самостоятельная работа представляет собой постоянно действующую систему, основу образовательного процесса и носит исследовательский характер, что послужит в будущем основанием для написания выпускной квалификационной работы, практического применения полученных знаний.

Организация самостоятельной работы обучающихся ориентируется на активные методы овладения знаниями, развитие творческих способностей, переход от поточного к индивидуализированному обучению, с учетом потребностей и возможностей личности.

Правильная организация самостоятельных учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет студентам развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивать высокий уровень успеваемости в период обучения, получить навыки повышения профессионального уровня.

Подготовка к практическому занятию включает, кроме проработки конспекта и презентации лекции, поиск литературы (по рекомендованным спискам и самостоятельно), подготовку заготовок для выступлений по вопросам, выносимым для обсуждения по конкретной теме. Такие заготовки могут включать цитаты, факты, сопоставление различных позиций, собственные мысли. Если проблема заинтересовала обучающегося, он может подготовить реферат и выступить с ним на практическом занятии. Практическое занятие - это, прежде всего, дискуссия, обсуждение конкретной ситуации, то есть предполагает умение внимательно слушать членов малой группы и модератора, а также стараться высказать свое мнение, высказывать собственные идеи и предложения, уточнять и задавать вопросы коллегам по обсуждению.

При подготовке к контрольной работе обучающийся должен повторять пройденный материал в строгом соответствии с учебной программой, используя конспект лекций и литературу, рекомендованную преподавателем. При необходимости можно обратиться за консультацией и методической помощью к преподавателю.

Самостоятельная работа реализуется:

– непосредственно в процессе аудиторных занятий - на лекциях, практических занятиях;

– в контакте с преподавателем вне рамок расписания - на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.

– в библиотеке, дома, на кафедре при выполнении обучающимся учебных и практических задач.

Виды СРС и критерии оценок

(по балльно-рейтинговой системе ГГНТУ, СРС оценивается в 15 баллов)

1. Реферат

Темы для самостоятельной работы прописаны в рабочей программе дисциплины. Эффективным средством осуществления обучающимся самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям электронных библиотечных систем.

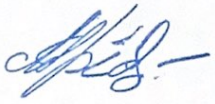
Составитель:

Ассистент  /Абдулаев М.К. /

СОГЛАСОВАНО:

Зав.кафедрой «ИСЭ»  /Магомаева Л.Р./

Зав. выпускающей каф. «ИСЭ»  /Магомаева Л.Р./

Директор ДУМР  /Магомаева М.А./