

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Минцва Милел Шаралович

Должность: Ректор

Дата подписания: 17.10.2019 11:04:32

Уникальный программный ключ:

236bcc35c296f119d6aafdc22836b21db52dbc07971a86865a5825f9fa4304cc

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

имени академика М.Д. Миллионщикова



РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЭКОНОМИЧЕСКИХ СИСТЕМ»

Направление подготовки

38.03.01 Экономика

Профиль

«Экономика предприятий и организаций (в строительстве)»

Квалификация

бакалавр

Грозный – 2019

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 программ; 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 курса: ознакомить студентов с тенденциями развития защиты информационной 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 базовой части профессионального цикла. Для изучения курса требуется освоение следующих дисциплин: «Информатика», «Мировая экономика и международные экономические отношения», «Информационные системы в экономике»,

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Общепрофессиональные (ОПК):

способностью осуществлять сбор, анализ и обработку данных, необходимых для решений профессиональных задач(ОПК-2);

Способностью использовать для решения коммуникативных задач современные технические средства и информационные технологии (ПК-10).

В результате освоения дисциплины студент должен.

знать:

- ✓ знать теоретические основы информационной безопасности и защиты информации.
- ✓ типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду.

уметь:

- ✓ проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе.

4. Объем дисциплины и виды учебной работы

Таблица 1.1

Вид учебной работы	Всего часов / зач. ед.		Семестр	Семестр
			7	7
	ОФО	ЗФО	ОФО	ЗФО
Контактная работа (всего)	68/1,9	16/0,44	68/1,9	16/0,44
В том числе:				
Лекции	34/0,94	8/0,22	34/0,94	8/0,22
Практические занятия	-		-	8/0,22
Семинары	34/0,94		34/0,94	
Лабораторные работы	-		-	-
Самостоятельная работа (всего)	76/2,22	128/3,55	76/2,22	128/3,55
В том числе:				
Курсовая работа (проект)	-	-	-	-
Расчетно-графические работы	-	-	-	-
ИТР	-	-	-	-
Рефераты	-	-	-	-
Доклады с презентациями	38/1,11	64/1,77	38/1,11	64/1,77
<i>И (или) другие виды самостоятельной работы:</i>				
Подготовка к лабораторным работам				
Подготовка к практическим занятиям	-		-	
Подготовка к зачету	38/1,11	64/1,77	38/1,11	64/1,77
Подготовка к экзамену	-		-	
Вид отчетности	зачет	зачет	зачет	зачет
Общая трудоемкость дисциплины	ВСЕГО в часах	144	144	144
	ВСЕГО в зач. единицах	4	4	4

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Таблица 2.1

ЗФО

№ п/п	Наименование раздела дисциплины по семестрам	Лекционные занятия	Практические занятия	Всего часов
1	Введение в информационную безопасность	2	2	4
2	Задачи и методы информационной безопасности	2	2	4
3	Угрозы информационной безопасности	2	2	4
4	Потенциальные противники и атаки	2	2	4
5	Стандарты обеспечения ИБ	-	-	-

Таблица 2.2

ОФО

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

5.2. Разделы дисциплины и виды занятий

Лекционные занятия

Таблица 3

№ п/п	Наименование раздела дисциплины	Содержание раздела
1.	Введение в информационную безопасность	Понятие "информационная безопасность" 1. Проблема информационной безопасности общества 2. Определение понятия "информационная безопасность" 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
15.	Сервисы управления доступом	Сервисы управления доступом
16.	Протоколирование и аудит	Протоколирование и аудит

5.3. Практические занятия

ОФО– 7 семестр, ЗФО-7 семестр

№	Наименование раздела	Наименование лабораторных работ
1.	Практическая работа №1. Установка и удаление сертификатов.	Работа со справкой: сертификаты, безопасные узлы. Установка и удаление сертификатов. Подготовка отчета
2.	Практическая 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.	Практическая работа №3. Анализ угроз и защищенности объекта.	Виды угроз и характер происхождения угроз
4.	Практическая работа №3. Анализ угроз и защищенности объекта.	Классы каналов несанкционированного получения информации, источники проявления угроз
5.	Практическая работа №3. Анализ угроз и защищенности объекта.	Причины нарушения целостности информации, потенциально возможные злоумышленные действия.
6.	Практическая работа №3. Анализ угроз и защищенности объекта.	Определить требования к защите Определить факторы, влияющие на требуемый уровень защиты информации
7.	Практическая работа №3. Анализ угроз и защищенности объекта.	Построить архитектуру систем защиты информации. Сформулировать предложения по увеличению защищенности информации
8.	Практическая работа №4 Создание самоподписанных сертификатов.	Работа со справкой: сертификаты, безопасные узлы. Создание самоподписанных сертификатов. сертификатов. Подготовка отчета
9	Практическая работа №5 Реализация политики безопасности в версиях операционной системы Windows	освоения средств администратора и аудитора версий операционной системы Windows, предназначенных для <ul style="list-style-type: none"> • определения параметров политики безопасности; • определения параметров политики аудита; • просмотра и очистки журнала аудита.
10.	Практическая работа №6 Разграничение доступа к ресурсам в версиях операционной системы Windows	освоение средств операционной системы Windows, предназначенных для: <ul style="list-style-type: none"> • 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.

5.4 Лабораторных занятий-нет

6. Самостоятельная работа студентов (СРС) по дисциплине

6.1. Вопросы для докладов+ презентация 7 семестр

№ п/п	Темы для самостоятельного изучения
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....)

7. Оценочные средства

В качестве оценочных средств используются средства контроля выполнения практических работ по дисциплине. Защита практической работы – ответ на контрольные вопросы после выполнения практической работы.

Средства текущего контроля: устный опрос (собеседование/опрос, разбор учебной ситуации на выбранную тему, подготовка устных сообщений и докладов), лабораторное задание (выполнение заданий в письменной форме, в электронной форме на ПК).

Текущий контроль

Практическая работа №1.

Установка и удаление сертификатов.

Практическая работа №2.

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

Практическая работа №3.

Анализ угроз и защищенности объекта.

Практическая работа №4

Создание самоподписанных сертификатов.

Практическая работа №5

Реализация политики безопасности в версиях операционной системы Windows

Практическая работа №6

Разграничение доступа к ресурсам в версиях операционной системы Windows

Образец практической работы

Практическая работа №4.

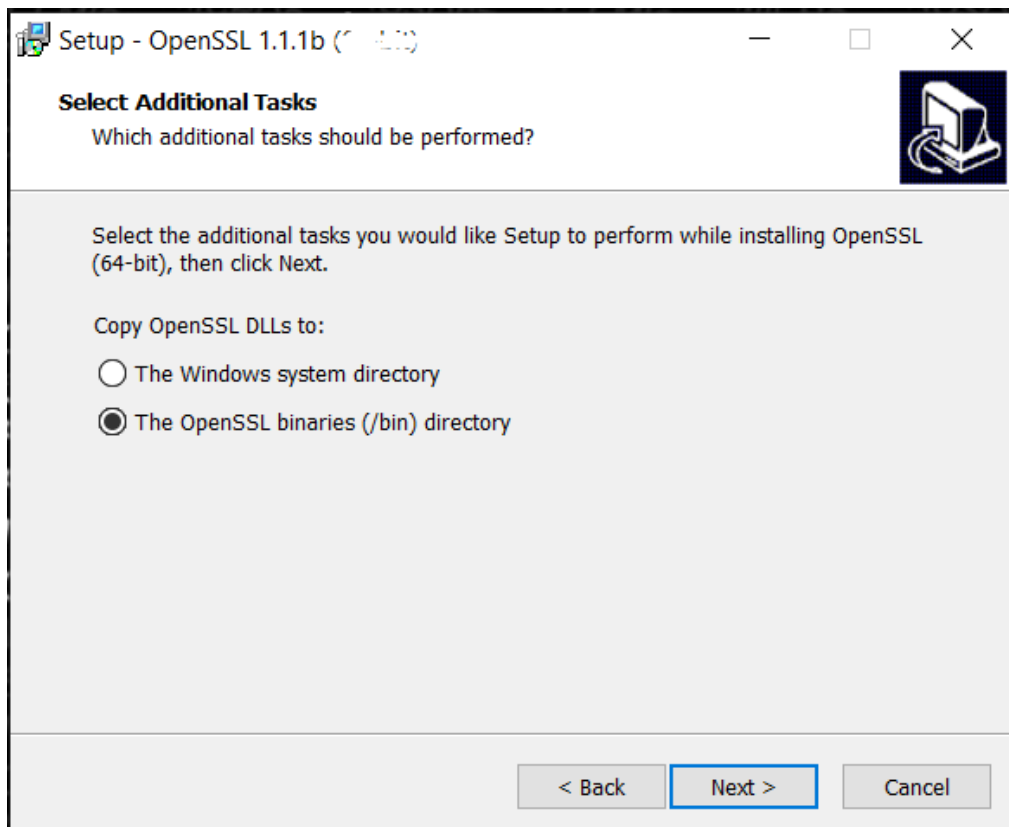
Создание самоподписанных сертификатов.

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 EXE MSI (experimental)	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:

- 2x 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.

Критерии оценки знаний студента на зачете

Оценка «зачтено» - выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации.

Оценка «незачтено» - выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении типовых практических задач.

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

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 к рубежной аттестации

Грозненский государственный нефтяной технический университет Институт цифровой экономики и технологического предпринимательства	
Кафедра «Экономика и управление в топливно-энергетическом комплексе» Дисциплина « Информационная безопасность экономических систем » БИЛЕТ № 1	
<ol style="list-style-type: none">1. Введение в информационную безопасность2. Стандарты обеспечения ИБ	
Преподаватель	
Зав. кафедрой «ЭиУП»	Т.В. Якубов

Образец билета ко 2-й рубежной аттестации

Грозненский государственный нефтяной технический университет Институт цифровой экономики и технологического предпринимательства	
Кафедра «Экономика и управление в топливно-энергетическом комплексе» Дисциплина « Информационная безопасность экономических систем » БИЛЕТ № 1	
<ol style="list-style-type: none">1. Законодательный уровень информационной безопасности2. Способы защиты операционных систем	
Преподаватель	
Зав. кафедрой «ЭиУП»	Т.В. Якубов

7.1. Вопросы к зачету

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

**ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**

БИЛЕТ № 1

Дисциплина «Информационная безопасность экономических систем»

Институт ИЦЭиТП ___ специальность ЭНГ 7 семестр

1. Законодательный уровень информационной безопасности
2. Способы защиты операционных систем
3. Введение в информационную безопасность
4. Стандарты обеспечения ИБ

УТВЕРЖДЕНО
на заседании кафедры
протокол № ___ от _____

Зав. кафедрой
Т.В. Якубов

Учебно-методическое и информационное обеспечение дисциплины

Основная литература:

1. Защита информации в корпоративных информационно-вычислительных сетях/ Игнатъев В.А.,2013 – Библиотека ГГНТУ;
2. Введение в информационную безопасность/Малюк А.А.-2011. – Библиотека ГГНТУ;
3. Информационная безопасность и защита информации/Громов Ю.Ю.,2010 – Библиотека ГГНТУ;
4. Васильев, В.И. Интеллектуальные системы защиты информации /Машиностроение, 2013 – ЭБС «Лань»;
5. Червяков, Н.И. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / Физматлит, 2012 – ЭБС «Лань»;
6. Фомин Д.В. Информационная безопасность [Электронный ресурс]: учебно-методическое пособие по дисциплине «Информационная безопасность» для студентов экономических специальностей заочной формы обучения/ Фомин Д.В.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2018.— 54 с.— Режим доступа: <http://www.iprbookshop.ru/77320.html>.— ЭБС «IPRbooks»
- 7.Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс]/ Анисимов А.А.— Электрон. текстовые данные. — М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 212 с.— Режим доступа: <http://www.iprbookshop.ru/52182.html>.— ЭБС «IPRbooks»
8. Кармановский Н.С. Организационно-правовое и методическое обеспечение информационной безопасности [Электронный ресурс]: учебное пособие/ Кармановский Н.С., Михайличенко О.В., Прохожев Н.Н.— Электрон. текстовые данные.— СПб.: Университет ИТМО, 2016.— 169 с.— Режим доступа: <http://www.iprbookshop.ru/67452.html>.— ЭБС «IPRbooks»

Дополнительная литература:

1. Моделирование системы защиты информации: Практикум/Баранова Е.К, 2015 – Библиотека ГГНТУ;
2. Защита информации в компьютерных системах и сетях/В.Ф.Шаньгин, 2012 – Библиотека ГГНТУ;
3. Коваленко, Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности / Горячая линия-Телеком, 2012. – ЭБС «Лань»;
4. Малюк, А.А. Введение в информационную / Горячая линия-Телеком, 2012. – ЭБС «Лань»;
5. Смирнов А.А. Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза [Электронный ресурс]: монография/ Смирнов А.А.— Электрон. текстовые данные.— М.: ЮНИТИ-ДАНА, 2017.— 159 с.— Режим доступа: <http://www.iprbookshop.ru/81515.html>.— ЭБС «IPRbooks»
6. Котов Ю.А., Криптографические методы защиты информации. Шифры: учебное пособие / Котов Ю.А. - Новосибирск: Изд-во НГТУ, 2016. - 59 с. - ISBN 978-5-7782-2959-4 - Текст: электронный // ЭБС "Консультант студента": сайт]. - URL: <http://www.studentlibrary.ru/book/ISBN9785778229594.html>

7. Ахмад Д.М., Защита от хакеров корпоративных сетей / Ахмад Д.М. и др.; Пер. с англ. А.А. Петренко. - Второе издание. - М.: ДМК Пресс, 2016. - 864 с. (Серия "Информационная безопасность") - ISBN 5-98453-015-5 - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: <http://www.studentlibrary.ru/book/ISBN5984530155.html> .

12. Материально-техническое обеспечение дисциплины «Информационная безопасность»

Технические средства обучения используются при выполнении студентами лабораторного практикума.

Технические средства обучения – сосредоточены в компьютерной лаборатории кафедры ИСЭ.

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

- 1 Internet explorer 6.0.
- 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 зачету.

Составитель

Асс. каф. «Информационные

системы в экономике»



М.К. Абдулаев

СОГЛАСОВАНО

Зав. каф. «Информационные

системы в экономике»



Л.Р. Магомаева

Зав. выпуск. каф. «Экономика

и управление на предприятии»



Т.В. Якубов

Директор ДУМР



М.А. Магомаева