МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФИЛИАЛ В г. ХАСАВЮРТЕ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направление: 40.03.01 - юриспруденция (уровень бакалавриата)

Профиль подготовки: «Уголовно-правовой"
Квалификация: бакалавр

Форма обучения: очная, очно-заочная

Хасавюрт – 2022

Рабочая программа дисциплины «**Информационная безопасность**» составлена в 2022 году в соответствии с требованиями ФГОС ВО по направлению подготовки 40.03.01. Юриспруденция (уровень бакалавриата) от 1 декабря 2016 г. № 1511

Разработчик (и):

Дадаев Динислам Хайбулаевич - кандидат физико-математических наук, доцент кафедры гуманитарных, естественнонаучных и социальных дисциплин филиала ДГУ в г. Хасавюрте.

Рабочая программа дисциплины одобрена:
на заседании кафедры юридических дисциплин от 31 марта 2022 г. протокол № 7.

Зав. кафедрой _____ Касумов Р. М.
(подпись)

на заседании учебно-методической комиссии филиала ДГУ в г. Хасавюрте от 31 марта 2022 г. протокол № 7.

Председатель _____ Шахбанов А. М.
(подпись)

Аннотация рабочей программы «Информационная безопасность»

Дисциплина «Информационная безопасность» является дисциплиной по выбору вариативной части образовательной программы бакалавриата по направлению 40.03.01. – Юриспруденция.

Дисциплина реализуется кафедрой юридических дисциплин.

Содержание дисциплины охватывает круг вопросов, связанных с изучением основных понятий, категорий, концепций, теорий, существующих в отрасли информационного права, рассматривается содержание основных норм права в отрасли информационного права, основные угрозы информационной безопасности, актуальные способы защиты информации, виды тайн, защищаемых законом.

Дисциплина нацелена на формирование следующих компетенций выпускника: профессиональных – ОК-3, ПК-6, ПК-15, ПК-16.

Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: лекции, практические занятия, самостоятельная работа.

Рабочая программа дисциплины предусматривает проведение итогового контроля успеваемости в форме зачета.

Объем дисциплины 1 зачетная единица, в том числе в академических часах по видам учебных занятий (1 зачетная единица, 36 часов).

Очная форма

Семестр	Всего	Учебные занятия				СР	Форма промежуточной аттестации
		в том числе					
		Контактная работа обучающихся с преподавателем					
		из них					
		Лекции	Лабораторные занятия	Практические занятия	Консультации		
6	36	14	-	12	-	10	Зачет

Очно-заочная форма

Семестр	Всего	Учебные занятия				СР	Форма промежуточной аттестации
		в том числе					
		Контактная работа обучающихся с преподавателем					
		из них					
		Лекции	Лабораторные занятия	Практические занятия	Консультации		
8	36	12	-	12	-	12	Зачет

1. Цели освоения дисциплины.

Основной целью дисциплины является ознакомление студентов с тенденцией развития информационной безопасности, с моделями возможных угроз, терминологией и основными понятиями теории безопасности информации, а так же с нормативными документами России, по данному вопросу и правилами получения соответствующих лицензий.

Изучение дисциплины «Информационная безопасность» направлено на решение следующих *задач:*

- получения студентами знаний по существующим угрозам безопасности информации, подбору и применению современных методов и способов защиты информации;
- формирование навыков, необходимых студентам по защите информации.

2. Место дисциплины «Информационная безопасность» в структуре основной профессиональной образовательной программы бакалавриата.

Дисциплина «Информационная безопасность» является дисциплиной по выбору вариативной части образовательной программы бакалавриата по направлению 40.03.01. – Юриспруденция.

Нормативно-правовой базой для изучения данной дисциплины являются статьи Конституции Российской Федерации, статьи Уголовного Кодекса, КОАП, международные договоры в сфере информационной безопасности.

Освоение дисциплины «Информационная безопасность» позволяет обучающимся максимально полно интегрировать полученные в ходе обучения профильным дисциплинам в условиях быстро развивающейся компьютеризации. В ходе изучения данной дисциплины студентами будут получены те навыки и умения, которые помогут им расширить свои знания в юриспруденции за счет использования современной теории и методов работы с информацией.

Дисциплина дополняет технические навыки пользования компьютерной техникой, полученные обучающимися в ходе освоения такой общеобразовательной дисциплины как «Информатика», теоретическими и технологическими знаниями в области автоматизированного управления (кибернетики) и связанных с ней естественнонаучных концепций, выступая своего рода «высшей информатикой».

Их изучение в особенности необходимо юристу как представителю профессии, в значительной степени связанной с управлением - нормативным регулированием и организацией локальных и глобальных социальных групп и общностей. В этой связи дисциплина в программе образования юриста методологически и технологически дополняет «управленческий» блок дисциплин.

Знание теории и механизмов общественных отношений, в большинстве своем складывающихся как коммуникации (информационное

взаимодействие) позволит бакалавру более полно понять объект и предмет всех профильных общетеоретических и конкретно-отраслевых юридических дисциплин.

Наконец, изучение технических и технологических средств защиты информации и правоохраны в области информационных отношений методологически дополняет блок криминологических и криминалистических дисциплин.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины (перечень планируемых результатов обучения).

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код компетенции из ФГОС ВО	Наименование компетенции из ФГОС ВО	Планируемые результаты обучения
ОК-3	владением основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией	**Знать:** сущность и содержание основных методов, способов и средств получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией **Уметь:** Работать с компьютером как средством управления информацией **Владеть:** владением основными методами, способами и средствами получения, хранения, переработки информации
ПК-6	способность юридически правильно квалифицировать факты и обстоятельства	**Знать**: понятие, виды и способы квалификации фактов и обстоятельств, этапы юридической квалификации, содержание источников информационной безопасности, с точки зрения разных авторов на проблемные вопросы **Уметь:** правильно давать юридическую оценку фактам и обстоятельствам, обоснованно применять нормы права при правовой квалификации обстоятельств. **Владеть:** юридической терминологией отраслей права, позволяющей юридически правильно квалифицировать факты и

		обстоятельства
ПК-15	Способность толковать нормативные правовые акты	**Знать:** понятие, виды и способы толкования правовых норм **Уметь:** анализировать содержание правовых норм, использовать различные приемы толкования для уяснения точного смысла нормы при квалификации фактов и обстоятельств **Владеть:** навыками работы по толкованию правовых норм.
ПК-16	способность давать квалифицированные юридические заключения и консультации в конкретных видах юридической деятельности	**Знать:** понятие, виды и способы квалификации фактов и обстоятельств, правовые явления и методы их анализа **Уметь:** оценивать правовые явления и формулировать выводы и предложения на основе их анализа, давать разъяснения по правовым вопросам в рамках своей профессиональной деятельности **Владеть**: навыками работы по толкованию правовых норм, навыками общения, методами аргументированного, обоснованного убеждения

4.Объем, структура и содержание дисциплины.

4.1. Объем дисциплины

Очная форма обучения

Объем дисциплины составляет 1 зачетную единицу, - 36 часов.

4.2. Структура дисциплины

Очная форма обучения

Раздел дисциплины (модуля)	Всего	Виды учебной работы, включая самостоятельную работу студентов и трудоёмкость (в часах)			Формы текущего контроля успеваемости (по неделям семестра) Форма промежуточной аттестации (по семестрам)
		Лекции	Практические занятия	СР	
Модуль 1					
Понятие "информационная безопасность". Проблема информационной безопасности общества. Составляющие информационной безопасности.	3	1	1	1	Контрольный опрос
Система формирования режима информационной безопасности. Уровни формирования режима информационной безопасности Нормативно-правовые основы информационной безопасности в РФ.	3	1	1	1	Контрольный опрос
Стандарты информационной безопасности: "Общие критерии". Требования безопасности к информационным системам. Функциональные требования, требования доверия	4	2	1	1	Контрольный опрос
Стандарты информационной безопасности в РФ. Федеральная служба по техническому и экспортному контролю и ее роль в обеспечении информационной безопасности в РФ. Документы по оценке защищенности автоматизированных систем в РФ	4	2	1	1	Контрольный опрос
Административный уровень обеспечения информационной безопасности. Разработка политики информационной безопасности. Классификация угроз "информационной безопасности". Каналы несанкционированного доступа к информации.	5	2	2	1	Контрольный опрос
Вирусы как угроза информационной безопасности. Характерные черты компьютерных вирусов. Классификация компьютерных вирусов	5	2	2	1	Контрольный опрос
Антивирусные программы, особенности их работы. Классификация антивирусных программ, факторы, определяющие их качество.	6	2	2	2	Контрольный опрос
Классификация удаленных угроз в вычислительных сетях, их характеристика. Механизмы обеспечения "информационной безопасности».	6	2	2	2	Контрольный опрос
Всего:	36	**14**	**12**	**10**	

*** - занятия проводятся в активной и интерактивной формах**

Очно-заочная форма обучения

Раздел дисциплины (модуля)	Всего	Виды учебной работы, включая самостоятельную работу студентов и трудоёмкость (в часах)			Формы текущего контроля успеваемости (по неделям семестра) Форма промежуточной аттестации (по семестрам)
		Лекции	Практические занятия	СР	
Модуль 1					
Понятие "информационная безопасность". Проблема информационной безопасности общества. Составляющие информационной безопасности.	3	1	1	1	Контрольный опрос
Система формирования режима информационной безопасности. Уровни формирования режима информационной безопасности Нормативно-правовые основы информационной безопасности в РФ.	3	1	1	1	Контрольный опрос
Стандарты информационной безопасности: "Общие критерии". Требования безопасности к информационным системам. Функциональные требования, требования доверия	4	2	1	1	Контрольный опрос
Стандарты информационной безопасности в РФ. Федеральная служба по техническому и экспортному контролю и ее роль в обеспечении информационной безопасности в РФ. Документы по оценке защищенности автоматизированных систем в РФ	4	2	1	1	Контрольный опрос
Административный уровень обеспечения информационной безопасности. Разработка политики информационной безопасности. Классификация угроз "информационной безопасности". Каналы несанкционированного доступа к информации.	5	1	2	2	Контрольный опрос
Вирусы как угроза информационной безопасности. Характерные черты компьютерных вирусов. Классификация компьютерных вирусов	5	1	2	2	Контрольный опрос
Антивирусные программы, особенности их работы. Классификация антивирусных программ, факторы, определяющие их качество.	6	2	2	2	Контрольный опрос
Классификация удаленных угроз в вычислительных сетях, их характеристика. Механизмы обеспечения "информационной безопасности».	6	2	2	2	Контрольный опрос
Всего:	36	**12**	**12**	**12**	

*** - занятия проводятся в активной и интерактивной формах**

4.3. Содержание дисциплины, структурированное по темам

4.3.1. Содержание лекционных занятий по дисциплине.

Тема 1. Введение в дисциплину «Информационная безопасность». Составляющие информационной безопасности.

Информационная безопасность является одной из проблем, с которой столкнулось современное общество в процессе массового использования автоматизированных средств ее обработки.
Проблема информационной безопасности обусловлена возрастающей ролью информации в общественной жизни.
Информационная безопасность – это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.
Согласно ГОСТу 350922-96 защита информации - это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.
В ряде случаев понятие "информационная безопасность" подменяется термином "компьютерная безопасность". В этом случае информационная безопасность рассматривается очень узко, поскольку компьютеры только одна из составляющих информационных систем.
Обеспечение информационной безопасности в большинстве случаев связано с комплексным решением трех задач:

- Обеспечением доступности информации.
- Обеспечением целостности информации.
- Обеспечением конфиденциальности информации.

Именно доступность, целостность и конфиденциальность являются равнозначными составляющими информационной безопасности.
Доступность – это гарантия получения требуемой информации или информационной услуги пользователем за определенное время.
Целостность информации условно подразделяется на статическую и динамическую. Статическая целостность информации предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации. Динамическая целостность информации включает вопросы корректного выполнения сложных действий с информационными потоками, например, анализ потока сообщений для выявления некорректных, контроль правильности передачи сообщений, подтверждение отдельных сообщений и др.

Целостность – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений.
Конфиденциальность – гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена.
Нарушение каждой из трех категорий приводит к нарушению информационной безопасности в целом.

Тема 2. Система формирования режима информационной безопасности.
Нормативно-правовые основы информационной безопасности в РФ.
Обеспечение безопасности является комплексной задачей. С одной стороны режима информационной, информационная безопасность предполагает, как минимум, обеспечение трех ее составляющих - доступность, целостность и конфиденциальность данных. И уже с учетом этого проблему информационной безопасности следует рассматривать комплексно. С другой стороны, информацией и информационными системами в буквальном смысле "пронизаны" все сферы общественной деятельности и влияние информации на общество все нарастает, поэтому обеспечение информационной безопасности также требует комплексного подхода.
В этой связи основными задачами информационной безопасности в широком смысле являются:

1. защита государственной тайны, т. е. секретной и другой конфиденциальной информации, являющейся собственностью государства, от всех видов несанкционированного доступа, манипулирования и уничтожения;
2. защита прав граждан на владение, распоряжение и управление принадлежащей им информацией;
3. защита прав предпринимателей при осуществлении ими коммерческой деятельности;
4. защита конституционных прав граждан на тайну переписки, переговоров, личную тайну.

Рассматривая проблему информационной безопасности в узком смысле, отметим, что в этом случае речь идет о совокупности методов и средств защиты информации и ее материальных носителей, направленных на обеспечение целостности, конфиденциальности и доступности информации.
Исходя из этого, выделим следующие задачи информационной безопасности:

- защита технических и программных средств информатизации от ошибочных действий персонала и техногенных воздействий, а также стихийных бедствий;
- защита технических и программных средств информатизации от преднамеренных воздействий.

Выделим три уровня формирования режима информационной безопасности:

- законодательно-правовой;
- административный (организационный);
- программно-технический.

Законодательная база в сфере информационной безопасности включает пакет Федеральных законов, Указов Президента РФ, постановлений Правительства РФ, межведомственных руководящих документов и стандартов.
Основополагающими документами по информационной безопасности в РФ являются Конституция РФ и Концепция национальной безопасности.

- Закон Российской Федерации от 21 июля 1993 года №5485-1 "О государственной тайне" с изменениями и дополнениями, внесенными после его принятия, регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.
- Закон РФ "Об информации, информатизации и защите информации" от 20 февраля 1995 года №24-ФЗ – является одним из основных базовых законов в области защиты информации, который регламентирует отношения, возникающие при формировании и использовании информационных ресурсов Российской Федерации на основе сбора, накопления, хранения, распространения и предоставления потребителям документированной информации, а также при создании и использовании информационных технологий, при защите информации и прав субъектов, участвующих в информационных процессах и информатизации.

В принятом в 1996 году Уголовном кодексе Российской Федерации, как наиболее сильнодействующем законодательном акте по предупреждению преступлений и привлечению преступников и нарушителей к уголовной ответственности, вопросам безопасности информации посвящены следующие главы и статьи:

1. Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.
2. Статья 140. Отказ в предоставлении гражданину информации.
3. Статья 183. Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну.
4. Статья 237. Сокрытие информации об обстоятельствах, создающих опасность для жизни и здоровья людей.
5. Статья 283. Разглашение государственной тайны.
6. Статья 284. Утрата документов, содержащих государственную тайну.

Особое внимание уделяется компьютерным преступлениям, ответственность за которые предусмотрена в специальной 28 главе кодекса "Преступления в сфере компьютерной информации".

Тема 3. Стандарты информационной безопасности: "Общие критерии".
Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий" (издан 1 декабря 1999 года) относится к оценочным стандартам. Этот международный стандарт стал итогом почти десятилетней работы специалистов нескольких стран. Он вобрал в себя опыт существовавших к

тому времени документов национального и межнационального масштаба. Именно поэтому этот стандарт очень часто называют "Общими критериями".
"Общие критерии" содержат два основных вида требований безопасности:

1. функциональные – соответствуют активному аспекту защиты – предъявляемые к функциям безопасности и реализующим их механизмам;
2. требования доверия – соответствуют пассивному аспекту – предъявляемые к технологии и процессу разработки и эксплуатации.

Все функциональные требования объединены в группы на основе выполняемой ими роли или обслуживаемой цели безопасности. Всего в "Общих критериях" представлено 11 функциональных классов, 66 семейств, 135 компонентов.
Вторая форма требований безопасности в "Общих критериях" – требования доверия безопасности.
Установление доверия безопасности основывается на активном исследовании объекта оценки.
Форма представления требований доверия, та же, что и для функциональных требований (класс – семейство – компонент).
Всего в "Общих критериях" 10 классов, 44 семейства, 93 компонента требований доверия безопасности.

Тема 4. Стандарты информационной безопасности распределенных систем. Стандарты информационной безопасности в РФ.

В последнее время с развитием вычислительных сетей и в особенности глобальной сети Интернет вопросы безопасности распределенных систем приобрели особую значимость. Важность этого вопроса косвенно подчеркивается появлением чуть позже "Оранжевой книги" стандарта, получившего название "Рекомендации X.800", который достаточно полно трактовал вопросы информационной безопасности распределенных систем, т. е. вычислительных сетей.
В X.800 определены следующие сетевые механизмы безопасности:

- шифрование;
- электронная цифровая подпись;
- механизм управления доступом;
- механизм контроля целостности данных;
- механизм аутентификации;
- механизм дополнения трафика;
- механизм управления маршрутизацией;
- механизм нотаризации (заверения).

В рекомендациях X.800 рассматривается понятие администрирование средств безопасности, которое включает в себя распространение информации, необходимой для работы сервисов и механизмов безопасности, а также сбор и анализ информации об их функционировании. Например, распространение криптографических ключей.

Согласно рекомендациям X.800, усилия администратора средств безопасности должны распределяться по трем направлениям:

- администрирование информационной системы в целом;
- администрирование сервисов безопасности;
- администрирование механизмов безопасности.

В 1987 г. Национальным центром компьютерной безопасности США была опубликована интерпретация "Оранжевой книги" для сетевых конфигураций. Данный документ состоит из двух частей. Первая содержит собственно интерпретацию, во второй рассматриваются сервисы безопасности, специфичные или особенно важные для сетевых конфигураций.

В Российской Федерации информационная безопасность обеспечивается соблюдение указов Президента, федеральных законов, постановлений Правительства Российской Федерации, руководящих документов Гостехкомиссии России и других нормативных документов.

Гостехкомиссия разработала и довела до уровня национальных стандартов десятки документов, среди которых:

- Руководящий документ "Положение по аттестации объектов информатизации по требованиям безопасности информации" (Утверждено Председателем Гостехкомиссии России 25.11.1994 г.).
- Руководящий документ "Автоматизированные системы (АС). Защита от несанкционированного доступа (НСД) к информации. Классификация АС и требования к защите информации" (Гостехкомиссия России, 1997 г.).
- Руководящий документ "Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации" (Гостехкомиссия России, 1992 г.).
- Руководящий документ "Концепция защиты средств вычислительной техники от НСД к информации" (Гостехкомиссия России, 1992 г.).
- Руководящий документ "Защита от НСД к информации. Термины и определения" (Гостехкомиссия России, 1992 г.).
- Руководящий документ "Средства вычислительной техники (СВТ). Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации" (Гостехкомиссия России, 1997 г.).
- Руководящий документ "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей" (Гостехкомиссия России, 1999 г.).
- Руководящий документ "Специальные требования и рекомендации по технической защите конфиденциальной информации" (Гостехкомиссия России, 2001 г.).

Тема 5. Административный уровень обеспечения информационной безопасности.

Административный уровень является промежуточным между законодательно-правовым и программно-техническим уровнями формирования режима информационной безопасности. Законы и стандарты в области информационной безопасности являются лишь отправным нормативным базисом информационной безопасности. Основой практического построения комплексной системы безопасности является административный уровень, определяющий главные направления работ по защите информационных систем.

Задачей административного уровня является разработка и реализация практических мероприятий по созданию системы информационной безопасности, учитывающей особенности защищаемых информационных систем.

Политика безопасности – это комплекс предупредительных мер по обеспечению информационной безопасности организации.

Основные направления разработки политики безопасности:

1. определение объема и требуемого уровня защиты данных;
2. определение ролей субъектов информационных отношений.

В состав автоматизированной информационной системы входят следующие компоненты:

- аппаратные средства – компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства – дисководы, принтеры, контроллеры), кабели, линии связи и т. д.;
- программное обеспечение – приобретенные программы, исходные, объектные, загрузочные модули; операционные системы и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т. д.;
- данные – хранимые временно и постоянно, на магнитных носителях, печатные, архивы, системные журналы и т. д.;
- персонал – обслуживающий персонал и пользователи.

Тема 6. Классификация угроз "информационной безопасности". Вирусы как угроза информационной безопасности

Угроза информационной безопасности – это потенциальная возможность нарушения режима информационной безопасности. Преднамеренная реализация угрозы называется атакой на информационную систему. Лица, преднамеренно реализующие угрозы, являются злоумышленниками.

Угрозы информационной безопасности классифицируются по нескольким признакам:

- по составляющим информационной безопасности (доступность, целостность, конфиденциальность), против которых, в первую очередь, направлены угрозы;
- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, персонал);
- по характеру воздействия (случайные или преднамеренные, действия природного или техногенного характера);

- по расположению источника угроз (внутри или вне рассматриваемой информационной системы).

Одним из наиболее распространенных и многообразных способов воздействия на информационную систему, позволяющим нанести ущерб любой из составляющих информационной безопасности является несанкционированный доступ.

Современный компьютерный вирус – это практически незаметный для обычного пользователя "враг", который постоянно совершенствуется, находя все новые и более изощренные способы проникновения на компьютеры пользователей.

Приведем одно из общепринятых определений вируса, содержащееся в ГОСТе Р 51275-99 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения".

Программный вирус – это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах.

По среде "обитания" вирусы делятся на:

- файловые;
- загрузочные;
- макровирусы;
- сетевые.

Файловые вирусы внедряются в выполняемые файлы (наиболее распространенный тип вирусов), либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы).

Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик жесткого диска (Master Boot Record), либо меняют указатель на активный boot-сектор.

Макровирусы заражают файлы-документы и электронные таблицы популярных офисных приложений.

Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

Существует большое количество сочетаний – например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные сектора дисков.

К "троянским" программам относятся программы, наносящие какие-либо разрушительные действия в зависимости от каких-либо условий. Утилиты скрытого администрирования являются разновидностью "логических бомб" ("троянских программ"), которые используются злоумышленниками для удаленного администрирования компьютеров в сети. Полиморфик-генераторы, как и конструкторы вирусов, не являются вирусами в прямом смысле этого слова, поскольку в их алгоритм не закладываются функции

размножения, т. е. открытия, закрытия и записи в файлы, чтения и записи секторов и т. д. Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика.

Тема 7. Антивирусные программы, особенности их работы. Особенности обеспечения информационной безопасности в компьютерных сетях.

Антивирусная программа – программа, предназначенная для поиска, обнаружения, классификации и удаления компьютерного вируса и вирусоподобных программ.

Самыми популярными и эффективными антивирусными программами являются антивирусные сканеры, CRC-сканеры (ревизоры). Существуют также антивирусы блокировщики и иммунизаторы.
Качество антивирусной программы определяется несколькими факторами. Перечислим их по степени важности:

- Надежность и удобство работы – отсутствие "зависаний" антивируса и прочих технических проблем, требующих от пользователя специальной подготовки.
- Качество обнаружения вирусов всех распространенных типов, сканирование внутри файлов-документов/таблиц, упакованных и архивированных файлов. Отсутствие "ложных срабатываний". Возможность лечения зараженных объектов.
- Существование версий антивируса под все популярные платформы (DOS, Windows, Linux и т. д.).
- Возможность сканирование "налету".
- Существование серверных версий с возможностью администрирования сети.
- Скорость работы.

Сетевые системы характерны тем, что наряду с локальными угрозами, осуществляемыми в пределах одной компьютерной системы, к ним применим специфический вид угроз, обусловленный распределенностью ресурсов и информации в пространстве. Это так называемые сетевые или удаленные угрозы.

Особенности вычислительных сетей и, в первую очередь, глобальных, предопределяют необходимость использования специфических методов и средств защиты, например:

- защита подключений к внешним сетям;
- защита корпоративных потоков данных, передаваемых по открытым сетям;
- защита потоков данных между клиентами и серверами;
- обеспечение безопасности распределенной программной среды;
- защита важнейших сервисов (в первую очередь – Web-сервиса);
- аутентификация в открытых сетях.

Тема 8. Классификация удаленных угроз в вычислительных сетях, их характеристика. Механизмы обеспечения "информационной безопасности».

Цели сетевой безопасности могут меняться в зависимости от ситуации, но основные цели обычно связаны с обеспечением составляющих "информационной безопасности":

1. целостности данных;
2. конфиденциальности данных;
3. доступности данных.

Удаленная угроза – потенциально возможное информационное разрушающее воздействие на распределенную вычислительную сеть, осуществляемая программно по каналам связи.

Удаленные угрозы можно классифицировать по следующим признакам.

- По характеру воздействия:
  - пассивные (класс 1.1);
  - активные (класс 1.2).
- По цели воздействия:
  - нарушение конфиденциальности информации (класс 2.1);
  - нарушение целостности информации (класс 2.2);
  - нарушение доступности информации (работоспособности системы) (класс 2.3).
- По условию начала осуществления воздействия

  Удаленное воздействие, также как и любое другое, может начать осуществляться только при определенных условиях. В вычислительных сетях можно выделить три вида условий начала осуществления удаленной атаки:
  - атака по запросу от атакуемого объекта (класс 3.1);
  - атака по наступлению ожидаемого события на атакуемом объекте (класс 3.2);
  - безусловная атака (класс 3.3).
- По наличию обратной связи с атакуемым объектом:
  - с обратной связью (класс 4.1);
  - без обратной связи (однонаправленная атака) (класс 4.2).
- По расположению субъекта атаки относительно атакуемого объекта:
  - внутрисегментное (класс 5.1);
  - межсегментное (класс 5.2).
- По уровню модели ISO/OSI, на котором осуществляется воздействие:
  - физический (класс 6.1);
  - канальный (класс 6.2);
  - сетевой (класс 6.3);
  - транспортный (класс 6.4);
  - сеансовый (класс 6.5);
  - представительный (класс 6.6);
  - прикладной (класс 6.7).

Общая процедура идентификации и аутентификации пользователя при его доступе в защищенную информационную систему заключается в следующем.

Пользователь предоставляет системе свой личный идентификатор (например, вводит пароль или предоставляет палец для сканирования отпечатка). Далее система сравнивает полученный идентификатор со всеми хранящимися в ее базе идентификаторами. Если результат сравнения успешный, то пользователь получает доступ к системе в рамках установленных полномочий. В случае отрицательного результата система сообщает об ошибке и предлагает повторно ввести идентификатор. В тех случаях, когда пользователь превышает лимит возможных повторов ввода информации (ограничение на количество повторов является обязательным условием для защищенных систем) система временно блокируется и выдается сообщение о несанкционированных действиях (причем, может быть, и незаметно для пользователя).

Если в процессе аутентификации подлинность субъекта установлена, то система защиты информации должна определить его полномочия (совокупность прав). Это необходимо для последующего контроля и разграничения доступа к ресурсам.

В целом аутентификация по уровню информационной безопасности делится на три категории:

1. Статическая аутентификация.
2. Устойчивая аутентификация.
3. Постоянная аутентификация.

В ГОСТе Р 50739-95 "Средства вычислительной техники. Защита от несанкционированного доступа к информации" и в документах Гостехкомиссии РФ определены два вида (принципа) разграничения доступа:

1. дискретное управление доступом;
2. мандатное управление доступом.

Дискретное управление доступом представляет собой разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту. Данный вид организуется на базе методов разграничения по спискам или с помощью матрицы.

Мандатное управление доступом основано на сопоставлении меток конфиденциальности информации, содержащейся в объектах (файлы, папки, рисунки) и официального разрешения (допуска) субъекта к информации соответствующего уровня конфиденциальности.

При внимательном рассмотрении можно заметить, что дискретное управление доступом есть ничто иное, как произвольное управление доступом (по "Оранжевой книге США"), а мандатное управление реализует принудительное управление доступом.

Тема 9. Определение и содержание регистрации и аудита информационных систем. Межсетевое экранирование.

Регистрация является еще одним механизмом обеспечения защищенности информационной системы. Этот механизм основан на подотчетности системы обеспечения безопасности, фиксирует все события, касающиеся безопасности, такие как:

- вход и выход субъектов доступа;
- запуск и завершение программ;
- выдача печатных документов;
- попытки доступа к защищаемым ресурсам;
- изменение полномочий субъектов доступа;
- изменение статуса объектов доступа и т. д.

Для сертифицируемых по безопасности информационных систем список контролируемых событий определен рабочим документом Гостехкомиссии РФ: "Положение о сертификации средств и систем вычислительной техники и связи по требованиям безопасности информации".

Аудит – это анализ накопленной информации, проводимый оперативно в реальном времени или периодически (например, раз в день). Регистрационный журнал – это хронологически упорядоченная совокупность записей результатов деятельности субъектов системы, достаточная для восстановления, просмотра и анализа последовательности действий, окружающих или приводящих к выполнению операций, процедур или совершению событий при транзакции с целью контроля конечного результата.

Под подозрительной активностью понимается поведение пользователя или компонента информационной системы, являющееся злоумышленным (в соответствии с заранее определенной политикой безопасности) или нетипичным (согласно принятым критериям).

Организация регистрации событий, связанных с безопасностью информационной системы включает как минимум три этапа:

- Сбор и хранение информации о событиях.
- Защита содержимого журнала регистрации.
- Анализ содержимого журнала регистрации.

Статистические методы основаны на накоплении среднестатистических параметров функционирования подсистем и сравнении текущих параметров с ними. Наличие определенных отклонений может сигнализировать о возможности появления некоторых угроз.

Эвристические методы используют модели сценариев несанкционированных действий, которые описываются логическими правилами или модели действий, по совокупности приводящие к несанкционированным действиям.

Одним из эффективных механизмом обеспечения информационной безопасности распределенных вычислительных сетях является экранирование, выполняющее функции разграничения информационных потоков на границе защищаемой сети.

Межсетевое экранирование повышает безопасность объектов внутренней сети за счет игнорирования неавторизованных запросов из

внешней среды, тем самым, обеспечивая все составляющие информационной безопасности. Кроме функций разграничения доступа, экранирование обеспечивает регистрацию информационных обменов.

Межсетевые экраны разделяют на четыре типа:

1. межсетевые экраны с фильтрацией пакетов;
2. шлюзы сеансового уровня;
3. шлюзы прикладного уровня;
4. межсетевые экраны экспертного уровня.

4.3.2. Содержание практических занятий по дисциплине.

Тема 1. Введение в дисциплину «Информационная безопасность».
Составляющие информационной безопасности.

1. В чем заключается проблема информационной безопасности?
2. Дайте определение понятию "информационная безопасность".
3. Какие определения информационной безопасности приводятся в "Концепции информационной безопасности сетей связи общего пользования Российской Федерации"?
4. Что понимается под "компьютерной безопасностью"?
5. Составляющие информационной безопасности.
6. Перечислите составляющие информационной безопасности.
7. Приведите определение доступности информации.
8. Приведите определение целостности информации.
9. Приведите определение конфиденциальности информации.
10. Каким образом взаимосвязаны между собой составляющие информационной безопасности?

Тема 2. Система формирования режима информационной безопасности.
Нормативно-правовые основы информационной безопасности в РФ.

11. Перечислите задачи информационной безопасности общества.
12. Перечислите уровни формирования режима информационной безопасности.
13. Дайте краткую характеристику законодательно-правового уровня.
14. Какие подуровни включает программно-технический уровень?
15. Что включает административный уровень?
16. В чем особенность морально-этического подуровня?
17. Перечислите основополагающие документы по информационной безопасности.
18. Понятие государственной тайны.
19. Что понимается под средствами защиты государственной тайны?
20. Основные задачи информационной безопасности в соответствии с Концепцией национальной безопасности РФ.

21. Какие категории государственных информационных ресурсов определены в Законе "Об информации, информатизации и защите информации"?
22. Какая ответственность в Уголовном кодексе РФ предусмотрена за создание, использование и распространение вредоносных программ для ЭВМ?

Тема 3. Стандарты информационной безопасности: "Общие критерии".

23. Какие виды требований включает стандарт ISO/IEC 15408?
24. Чем отличаются функциональные требования от требований доверия?
25. В чем заключается иерархический принцип "класс – семейство – компонент – элемент"?
26. Какова цель требований по отказоустойчивости информационных систем?
27. Сколько классов функциональных требований?

Тема 4. Стандарты информационной безопасности распределенных систем. Стандарты информационной безопасности в РФ.

28. Дайте характеристику составляющих "информационной безопасности" применительно к вычислительным сетям.
29. Перечислите основные механизмы безопасности.
30. Какие механизмы безопасности используются для обеспечения конфиденциальности трафика?
31. Какие механизмы безопасности используются для обеспечения "неотказуемости" системы?
32. Что понимается под администрированием средств безопасности?
33. Какие виды избыточности могут использоваться в вычислительных сетях?
34. Сколько классов защищенности СВТ от НСД к информации устанавливает РД "СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации"?
35. Дайте характеристику уровням защиты СВТ от НСД к информации по РД "СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации"?
36. Классы защищенности АС от НСД по РД "АС. Защита от НСД к информации. Классификация АС и требования по защите информации".
37. Какие классы защищенных АС от НСД должны обеспечивать идентификацию, проверку подлинности и контроль доступа субъектов в систему?

Тема 5. Административный уровень обеспечения информационной безопасности.

38. Цели и задачи административного уровня обеспечения информационной безопасности.

39. Содержание административного уровня.
40. Дайте определение политики безопасности.
41. Направления разработки политики безопасности.
42. Перечислите составные элементы автоматизированных систем.
43. Субъекты информационных отношений и их роли при обеспечении информационной безопасности.

Тема 6. Классификация угроз "информационной безопасности". Вирусы как угроза информационной безопасности

44. Перечислите классы угроз информационной безопасности.
45. Назовите причины и источники случайных воздействий на информационные системы.
46. Дайте характеристику преднамеренным угрозам.
47. Перечислите каналы несанкционированного доступа.
48. В чем особенность "упреждающей" защиты в информационных системах.
49. Перечислите классификационные признаки компьютерных вирусов.
50. Охарактеризуйте файловый и загрузочный вирусы.
51. В чем особенности резидентных вирусов?
52. Сформулируйте признаки стелс-вирусов.
53. Перечислите деструктивные возможности компьютерных вирусов.
54. Поясните самошифрование и полиморфичность как свойства компьютерных вирусов.

Тема 7. Антивирусные программы, особенности их работы. Особенности обеспечения информационной безопасности в компьютерных сетях.

55. Поясните понятия "сканирование налету" и "сканирование по запросу".
56. Перечислите виды антивирусных программ.
57. Охарактеризуйте антивирусные сканеры.
58. Принципы функционирования блокировщиков и иммунизаторов.
59. Особенности CRC-сканеров.
60. В чем состоят особенности эвристических сканеров?
61. Какие факторы определяют качество антивирусной программы?
62. Особенности обеспечения информационной безопасности компьютерных сетей.
63. Дайте определение понятия "удаленная угроза".
64. Основные цели информационной безопасности компьютерных сетях.
65. В чем заключается специфика методов и средств защиты компьютерных сетей?
66. Поясните понятие "глобальная сетевая атака", приведите примеры.

Тема 8. Классификация удаленных угроз в вычислительных сетях, их характеристика. Механизмы обеспечения "информационной безопасности».

67. Перечислите классы удаленных угроз.
68. Как классифицируются удаленные угрозы "по характеру воздействия"?

69. Охарактеризуйте удаленные угрозы "по цели воздействия".
70. Как классифицируются удаленные угрозы "по расположению субъекта и объекта угрозы"?
71. Дайте определение маршрутизатора.
72. Что такое подсеть и сегмент сети? Чем они отличаются?
73. Может ли пассивная угроза привести к нарушению целостности информации?
74. Что понимается под идентификацией пользователя?
75. Что понимается под аутентификацией пользователей?
76. Применим ли механизм идентификации к процессам? Почему?
77. Перечислите возможные идентификаторы при реализации механизма идентификации.
78. Перечислите возможные идентификаторы при реализации механизма аутентификации.
79. Какой из механизмов (аутентификация или идентификация) более надежный? Почему?
80. В чем особенности динамической аутентификации?
81. Опишите механизм аутентификации пользователя.
82. Что такое "электронный ключ"?
83. Перечислите виды аутентификации по уровню информационной безопасности.
84. Какой из видов аутентификации (устойчивая аутентификация или постоянная аутентификация) более надежный?

5. Образовательные технологии

Образовательные технологии, используемые при реализации различных видов учебной работы по дисциплине, предусматривают широкое использование в учебном процессе как классических, так и активных и интерактивных форм проведения занятий:

– чтение лекций;
– практические занятия.

Изучение отдельных разделов дисциплины проводится в такой последовательности:

а) ознакомление с содержанием тем по рабочей программе;
б) изучение специальной литературы, конспектирование материала;
в) консультация с преподавателем;
г) самостоятельное изложение проблемы.

6.Учебно-методическое обеспечение самостоятельной работы студентов.

Самостоятельная работа студентов направлена на решение следующих задач: - расширение и закрепление знаний, полученных на лекционных, практических занятиях;

- выработка у студентов интереса к самостоятельному поиску и решению проблемных вопросов и задач;

- развитие навыков работы с учебной и дополнительной литературой и источниками;

- привлечение студентов к научно-исследовательской работе;

Самостоятельная работа проводится в следующей форме: написание докладов на семинарские занятия.

Виды и порядок выполнения самостоятельной работы:

1. Изучение рекомендованной литературы.
2. Поиск дополнительного материала.
3. Подготовка к зачету.

№	Вид самостоятельной работы	Вид контроля	Учебно-методическое обеспечение
1.	Изучение рекомендованной литературы	Контрольный опрос	См. разделы 7,8 данного документа
2.	Поиск дополнительного материала	Контрольный опрос	См. разделы 7,8 данного документа
3.	Подготовка к зачету	Контрольный опрос	См. разделы 7 данного документа

Текущий контроль: контрольный опрос, оценка на практическом занятии. Текущий контроль успеваемости осуществляется непрерывно. Прежде всего, это устный опрос по ходу лекции, выполняемый для оперативной активизации внимания студентов и оценки их уровня восприятия, а также на практических занятиях.

Итоговая аттестация проводится в форме зачета. Зачет проводится в устной форме. Студент должен показать знания по предмету отвечая на вопросы преподавателя и на дополнительные вопросы, если таковые будут заданы.

7. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код и наименование компетенция из ФГОС ВО	Планируемые результаты обучения	Процедура освоения
ОК-3 - владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией	**Знать:** сущность и содержание основных методов работы с информацией. **Уметь:** Работать с большим потоком информации в глобальных компьютерных сетях **Владеть:** навыками работы с информацией в глобальных компьютерных сетях.	контрольный опрос
ОК-4 способность работать с информацией в глобальных компьютерных сетях	**Знать:** систему правоотношений в сфере информационной безопасности. **Уметь:** обеспечивать соблюдение законодательства Российской Федерации в сфере информационной безопасности субъектами права **Владеть:** навыками анализа различных правовых явлений, юридических фактов, правовых норм и правовых отношений в сфере информационной безопасности.	контрольный опрос
ПК-6 способность юридически правильно квалифицировать факты и обстоятельства	**Знать**: понятие, виды и способы квалификации фактов и обстоятельств, этапы юридической квалификации, содержание источников информационной безопасности, с точки зрения разных авторов на проблемные вопросы **Уметь:** правильно давать юридическую оценку фактам и обстоятельствам, обоснованно применять нормы права при правовой квалификации обстоятельств.	контрольный опрос
ПК-15 Способность толковать нормативные правовые акты	**Знать:** понятие, виды и способы толкования правовых норм **Уметь:** анализировать содержание правовых норм, использовать различные приемы толкования для уяснения точного смысла нормы при квалификации фактов и обстоятельств **Владеть:**	контрольный опрос

ПК-16 - способность давать квалифицированные юридические заключения и консультации в конкретных видах юридической деятельности	**Знать:** Содержание нормативных правовых актов. **Уметь:** осуществлять правовую экспертизу нормативных правовых актов, принимать решения и совершать юридические действия в точном соответствии с законом. **Владеть:** навыками принятия необходимых мер защиты прав человека и гражданина.	контрольный опрос

7.2. Типовые задания

Перечень вопросов на зачет

1. Понятие "информационная безопасность".
2. Проблема информационной безопасности общества.
3. Составляющие информационной безопасности. Доступность, целостность, конфиденциальность.
4. Система формирования режима информационной безопасности. Уровни формирования режима информационной безопасности
5. Нормативно-правовые основы информационной безопасности в РФ. Правовые основы информационной безопасности общества.
6. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации.
7. Ответственность за нарушения в сфере информационной безопасности.
8. Стандарты информационной безопасности: "Общие критерии". Требования безопасности к информационным системам. Функциональные требования, требования доверия.
9. Стандарты информационной безопасности распределенных систем. Сервисы безопасности в вычислительных сетях.
10. Механизмы безопасности.
11. Администрирование средств безопасности.
12. Стандарты информационной безопасности в РФ.
13. Федеральная служба по техническому и экспортному контролю и ее роль в обеспечении информационной безопасности в РФ.
14. Документы по оценке защищенности автоматизированных систем в РФ.
15. Административный уровень обеспечения информационной безопасности. Разработка политики информационной безопасности.
16. Классификация угроз "информационной безопасности".
17. Каналы несанкционированного доступа к информации.
18. Вирусы как угроза информационной безопасности. Характерные черты компьютерных вирусов.
19. Классификация компьютерных вирусов по среде обитания, по особенностям алгоритма работы, по деструктивным возможностям.

20. Характеристика "вирусоподобных" программ.
21. Антивирусные программы, особенности их работы. Классификация антивирусных программ, факторы, определяющие их качество.
22. Особенности обеспечения информационной безопасности в компьютерных сетях.
23. Специфика средств защиты в компьютерных сетях.
24. Транспортный протокол TCP и модель TCP/IP. Основы IP-протокола.
25. Система доменных имен.
26. Классификация удаленных угроз в вычислительных сетях, их характеристика.
27. Механизмы обеспечения "информационной безопасности».
28. Определение понятий "идентификация" и "аутентификация". Механизм идентификации и аутентификации пользователей.

7.3. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Методические материалы, определяющие процедуру оценивания знаний, умений, навыков отражены в Положении о модульно-рейтинговой системе (МРС), обучения студентов Дагестанского государственного университета.

Общий результат выводится как интегральная оценка, складывающая из текущего контроля – 30 % и промежуточного контроля – 70 %.

Текущий контроль по дисциплине включает:

- посещение занятий – 5 баллов
- участие на практических занятиях - 15 баллов
- выполнение контрольных работ – 5 баллов

Написание и защита реферата – 5 баллов

Промежуточный контроль по дисциплине включает:

- письменная работа - 70 баллов

Критерии оценок следующие:

- 100 баллов - студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновывать выводы и разъяснять их в логической последовательности.
- 90 баллов - студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновывать выводы и разъяснять их в логической последовательности, но допускает отдельные неточности.
- 80 баллов - студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновывать выводы и разъяснять их в

логической последовательности, но допускает некоторые ошибки общего характера.
- 70 баллов - студент хорошо понимает пройденный материал, но не может теоретически обосновывать некоторые выводы.
- 60 баллов - студент отвечает в основном правильно, но чувствуется механическое заучивание материала.
- 50 баллов - в ответе студента имеются существенные недостатки, материал охвачен «половинчато», в рассуждениях допускаются ошибки.
- 40 баллов - ответ студента правилен частично, при разъяснении материала допускаются серьезные ошибки.
- 20 - 30 баллов - студент имеет общее представление о теме, но не умеет логически обосновать свои мысли.
- 10 баллов - студент имеет лишь частичное представление о теме.
- 0 баллов - нет ответа

Таблица перевода рейтингового балла по дисциплине в «зачтено» или «не зачтено»

Итоговая сумма баллов по дисциплине по 100-балльной шкале	Оценка по дисциплине
0-50	Не зачтено
51-100	Зачтено

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература

1. Филиппов, Б.И. Информационная безопасность. Основы надежности средств связи : учебник / Б.И. Филиппов, О.Г. Шерстнева. – Москва ; Берлин : Директ-Медиа, 2019. – 241 с. : ил., табл. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=499170 . – Библиогр.: с. 221-226. – ISBN 978-5-4475-9823-5. – DOI 10.23681/499170. – Текст : электронный.
2. Ищейнов, В.Я. Информационная безопасность и защита информации: теория и практика : учебное пособие : [16+] / В.Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=571485 – Библиогр. в кн. – ISBN 978-5-4499-0496-6. – DOI 10.23681/571485. – Текст : электронный.
3. Шилов, А.К. Управление информационной безопасностью : учебное пособие / А.К. Шилов ; Министерство науки и высшего образования РФ, Южный федеральный университет, Институт компьютерных технологий и информационной безопасности. – Ростов-на-Дону ; Таганрог : Южный

федеральный университет, 2018. – 121 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=500065 – Библиогр.: с. 81-82. – ISBN 978-5-9275-2742-7. – Текст : электронный.

2. Дополнительная литература

1. Моргунов, А.В. Информационная безопасность : учебно-методическое пособие : [16+] / А.В. Моргунов ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2019. – 83 с. : ил., табл. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=576726 . – Библиогр.: с. 64. – ISBN 978-5-7782-3918-0. – Текст : электронный.
2. Ищейнов, В.Я. Информационная безопасность и защита информации: теория и практика : учебное пособие : [16+] / В.Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=571485 – Библиогр. в кн. – ISBN 978-5-4499-0496-6. – DOI 10.23681/571485. – Текст : электронный.

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.

1. *www.jetinfo.ru*.
2. http://biblioclub.ru
3. https://fstec.ru/ Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России)
4. *www.iso.ch* – Web-сервер Международной организации по стандартизации.
5. eLIBRARY.RU [Электронный ресурс]: электронная библиотека / Науч. электрон. б-ка. — Москва, 1999 – . Режим доступа: http://elibrary.ru/defaultx.asp. – Яз. рус., англ.
6. Moodle [Электронный ресурс]: система виртуального обучением: [база данных] / Даг. гос. ун-т. – Махачкала, г. – Доступ из сети ДГУ или, после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: http://moodle.dgu.ru/
7. Электронный каталог НБ ДГУ [Электронный ресурс]: база данных содержит сведения о всех видах лит, поступающих в фонд НБ ДГУ/Дагестанский гос. ун-т. – Махачкала, 2010 – Режим доступа: http://elib.dgu.ru, через локальную сеть ДГУ

10. Методические указания для обучающихся по освоению дисциплины.

При самостоятельном освоении отдельных тем и вопросов, предусмотренных настоящей Рабочей программой обучающиеся должны следовать обычному для самостоятельного изучения материала алгоритму.

Во-первых, ознакомиться с соответствующими изучаемой теме разделами основной и дополнительной литературы, рекомендованными Разделом 8.

Во-вторых, по ключевым словам формулировки осваиваемой темы или вопроса произвести поиск и ознакомиться с соответствующими материалами интернет-ресурсов, рекомендованных Разделом 9.

В-третьих, если тема или вопрос, связаны с функциональными возможностями аппаратной части компьютера или конкретного средства программного обеспечения, в обязательном порядке следует закрепить прочитанное посредством практического использования этих функциональных возможностей.

Не следует забывать, что практически все средства программного обеспечения традиционно содержат в своем составе интерактивные справочные системы. Доступ к ним открывается, как правило, при нажатии на клавишу «F1» либо через пункт «Справка» или «?» меню основного окна программы. В открывшемся окне справочной системы, как правило, имеется возможность поиска нужного раздела справки по ключевым словам.

Настоятельно рекомендуется в процессе самостоятельной подготовки повторять все задания, которые выполнялись разово под руководством преподавателя в ходе практических занятий.

11.Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационно-справочных систем.

Программное обеспечение:

Microsoft Windows, Power Point - для создания презентаций, визуального сопровождения докладов по темам занятий, Microsoft Internet Explorer - для дополнительного поиска информации, подготовки к практическим занятиям, в целях поиска информации для самостоятельной работы, ABBYY FineReader - для распознавания и преобразования текста.

Информационно-справочная система:
1. Консультант плюс (договор № 40 от 09.01.2018г.)

12. Описание материально-технической базы, необходимой для осуществлении образовательного процесса по дисциплине.

Для проведения лекционных занятий по дисциплине «Информационная безопасность» используются:

парта семиместная – 12 шт., стулья ученические - 84 шт., доска классная - 1 шт., стол преподавателя - 3 шт., стул преподавателя - 6 шт., кафедра трибуна – 1 шт., стенды – 6 шт., проектор – 1 шт., экран для проектора – 1 шт., ноутбук – 1 шт.

Для проведения семинарского типа по дисциплине «Информационная безопасность» используются:

парта двухместная – 21 шт., стулья ученические - 42 шт., доска классная - 1 шт., стол преподавателя - 1 шт., стул преподавателя - 1 шт., кафедра трибуна – 1 шт., стенды – 14 шт.

Помещение для самостоятельной работы:

парта одноместная – 13 шт., стулья ученические – 13 шт., стол преподавателя - 3 шт., стул преподавателя - 3 шт., компьютеры – 16 шт., клавиатура – 16 шт., процессоры – 16 шт., компьютерная мышь -16 шт., принтер – 2 шт., стенды – 4 шт., шкаф – 1 шт., учебные пособия

Библиотека, читальный зал с выходом в сеть Интернет

парта двухместная – 63 шт., парта одноместная – 4 шт., стулья ученические - 92 шт., доска классная - 1 шт., стол преподавателя - 1 шт., стул преподавателя - 1 шт., стенды – 11 шт., проектор – 2 шт., экран для проектора – 2 шт., компьютеры – 22 шт., кафедра-трибуна – 1 шт