

Федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный университет имени Г.Р. Державина»
Институт математики, физики и информационных технологий
Кафедра математического моделирования и информационных технологий

УТВЕРЖДАЮ:
Директор института



Н. Л. Королева
«05» июля 2021 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине Б1.В.ДВ.04.1 Теоретические основы информационной безопасности

Направление подготовки/специальность: 10.05.05 - Безопасность информационных технологий в правоохранительной сфере

Профиль/направленность/специализация: Технологии защиты информации в правоохранительной сфере

Уровень высшего образования: специалитет

Квалификация: Специалист по защите информации

год набора: 2021

Автор программы:

Кандидат педагогических наук, доцент Михайлова Елена Михайловна

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.05 - Безопасность информационных технологий в правоохранительной сфере (уровень специалитета) (приказ Министерства образования и науки РФ от «26» ноября 2020 г. № 1461).

Рабочая программа принята на заседании Кафедры математического моделирования и информационных технологий «18» мая 2021 г. Протокол № 9

Рассмотрена и одобрена на заседании Ученого совета Института математики, физики и информационных технологий, Протокол от «05» июля 2021 г. № 5.

СОДЕРЖАНИЕ

1. Цели и задачи дисциплины.....	4
2. Место дисциплины в структуре ОП Специалиста.....	5
3. Объем и содержание дисциплины.....	5
4. Контроль знаний обучающихся и типовые оценочные средства.....	19
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	32
6. Учебно-методическое и информационное обеспечение дисциплины.....	34
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	34

1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ПК-1 Способен разрабатывать требования по защите, формировать политику безопасности компьютерных систем и сетей

1.2 Типы задач профессиональной деятельности, к которым готовятся обучающиеся в рамках освоения дисциплины:

- организационно-управленческий

1.3 Дисциплина ориентирована на подготовку обучающихся к профессиональной деятельности в сферах: 06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере), 12 Обеспечение безопасности (в сфере защиты информации), Сфера правоохранительной деятельности

1.4 В результате освоения дисциплины у обучающихся должны быть сформированы:

Обобщенные трудовые функции / трудовые функции / трудовые или профессиональные действия (при наличии профстандарта)	Код и наименование компетенции ФГОС ВО, необходимой для формирования трудового или профессионального действия	Индикаторы достижения компетенций
	ПК-1 Способен разрабатывать требования по защите, формировать политику безопасности компьютерных систем и сетей	Разрабатывает требования по защите, формирует политику безопасности компьютерных систем и компьютерных сетей

1.5 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ПК-1 Способен разрабатывать требования по защите, формировать политику безопасности компьютерных систем и сетей

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения				
		Очная (семестр)				
		2	3	5	6	9
1	Автоматизация деятельности предприятий		+			
2	Защита компьютерных систем от вредоносных программ		+			
3	Компьютерные сети			+	+	
4	Ознакомительная практика				+	
5	Организационная защита информации					+

6	Основы программирования в корпоративных информационных системах		+			
7	Современные технологии обеспечения информационной безопасности	+				
8	Теоретические основы защиты информации на английском языке	+				

2. Место дисциплины в структуре ОП специалитета:

Дисциплина «Теоретические основы информационной безопасности» относится к части, формируемой участниками образовательных отношений, учебного плана ОП по направлению подготовки 10.05.05 - Безопасность информационных технологий в правоохранительной сфере.

Дисциплина «Теоретические основы информационной безопасности» изучается в 2 семестре.

3. Объем и содержание дисциплины

3.1. Объем дисциплины: 2 з.е.

Очная: 2 з.е.

Вид учебной работы	Очная (всего часов)
Общая трудоёмкость дисциплины	72
Контактная работа	48
Лекции (Лекции)	16
Лабораторные (Лаб. раб.)	32
Самостоятельная работа (СР)	24
Зачет	-

3.2. Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.			Формы текущего контроля
		Лек ции	Лаб · раб.	СР	
		О	О	О	
2 семестр					
1	Основные понятия теории информационной безопасности.	2	4	3	Тестирование
2	Информация как объект защиты.	2	4	3	Тестирование

3	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности.	2	4	3	Опрос
4	Угрозы информационной безопасности.	2	4	3	Тестирование
5	Построение систем защиты от угрозы нарушения конфиденциальности .	2	4	3	Тестирование
6	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа.	2	3	3	Тестирование
7	Политика и модели безопасности.	2	3	2	Тестирование
8	Обзор международных стандартов информационной безопасности.	1	3	2	Выполнение практических заданий
9	Информационные войны и информационное противоборство.	1	3	2	Выполнение практических заданий

Тема 1. Основные понятия теории информационной безопасности. (ПК-1)

Лекция.

Предметная область теории информационной безопасности. Систематизация понятий в области защиты информации. Основные термины и определения правовых понятий в области информационных отношений и защиты информации. Понятия предметной области «Защита информации». Основные принципы построения систем защиты. Концепция комплексной защиты информации. Задачи защиты информации. Средства реализации комплексной защиты информации.

Лабораторные работы.

1. Информация это:
 - a) сведения, поступающие от СМИ;
 - b) только документированные сведения о лицах, предметах, фактах, событиях;
 - c) сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;
 - d) только сведения, содержащиеся в электронных базах данных.
2. Информация
 - a) не исчезает при потреблении;

- b) становится доступной, если она содержится на материальном носителе;
 - c) подвергается только "моральному износу";
 - d) характеризуется всеми перечисленными свойствами.
3. Информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать, называется:
- a) достоверной;
 - b) конфиденциальной;
 - c) документированной;
 - d) коммерческой тайной.
4. Информационно-телекоммуникационная сеть это:
- a) технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;
 - b) технологическая система, предназначенная для передачи по сети интернет, доступ к которой осуществляется с использованием средств вычислительной техники;
 - c) технологическая система, предназначенная для передачи информации по локально сети, доступ к которой осуществляется с использованием средств вычислительной техники.
5. Доступ к информации это:
- a) возможность получения информации;
 - b) возможность получения информации, и ее использовании;
 - c) возможность получения информации, и ее распространения.
6. Предоставление информации это действия, направленные:
- a) на получение информации определенным кругом лиц;
 - b) на получение информации руководителем и передачу информации определенному кругу лиц;
 - c) на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.
7. Информационная безопасность это:
- a) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре;
 - b) защищенность программных продуктов предприятия от случайных или преднамеренных воздействий естественного или случайного характера;
 - c) защищенность информации, циркулирующей в сети от случайных или преднамеренных воздействий естественного или случайного характера.
8. Безопасность информации это защищенность информации:
- a) от разглашения, искажения, утраты;
 - b) от разглашения, искажения, утраты или снижения степени доступности информации, а также незаконного ее тиражирования;
 - c) от передачи третьим лицам, искажения и не законного использования.
9. Угроза – это:
- a) потенциальная возможность определенным образом нарушить информационную безопасность;
 - b) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных;

с) процесс определения отвечает на текущее состояние разработки требованиям данного этапа.

10. Эффективное обеспечение защиты информации возможно:

- а) только на основе комплексного использования всех известных методов и подходов к решению данной проблемы;
- д) только при использовании сертифицированных средств защиты информации;
- е) только при использовании технических средств защиты информации;
- ф) Все ответы правильные.

Задания для самостоятельной работы.

Покажите связь между уровнем развития общества и технологиями защиты информации.

В каких направлениях идет развитие теории информационной безопасности в настоящее время?

Каков вклад российских ученых в теорию информационной безопасности?

С чем связан возросший интерес к проблемам защиты информации?

Каковы отличия формального и неформального подходов к проблемам защиты информации?

В чем, на Ваш взгляд, заключаются основные трудности

обеспечения информационной безопасности в настоящее время?

Что такое информационная система? Телекоммуникационная система? Автоматизированная система?

Каковы правовые понятия в области защиты информации?

Что такое защита информации? Информационная безопасность?

Охарактеризуйте понятия, связанные с организацией защиты информации.

Каковы основные принципы построения систем защиты информации?

Что такое комплексный подход к обеспечению информационной безопасности?

Каковы основные задачи защиты информации?

Докажите, что приведенное множество функций защиты является полным.

Какова взаимосвязь различных средств защиты информации? Есть ли среди них приоритетные?

Каковы основные средства реализации комплексной системы защиты информации?

Что такое морально-этические средства защиты информации?

Докажите необходимость сочетания различных средств защиты информации. 20. Приведите примеры формальных и неформальных средств защиты?

Что такое центры информационной безопасности и какова их роль в развитии теории и практики защиты информации?

Тема 2. Информация как объект защиты. (ПК-1)

Лекция.

Понятие об информации как объекте защиты. Уровни представления информации. Основные свойства защищаемой информации. Виды и формы представления информации. Информационные ресурсы. Структура и шкала ценности информации. Классификация информационных ресурсов. Правовой режим информационных ресурсов.

Лабораторные работы.

1. Документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, депозитариях, музейных хранилищах и т. п.):

- а) информационные ресурсы;
- б) информационные продукты;
- с) информационные ресурсы.

2. Информационные ресурсы являются одним из видов общественных, экономических ресурсов:

- а) факторов ведения дел;
- б) факторов производства;

с) факторов деятельности.

3. Уровень развития сферы информационных услуг во многом определяет степень приближенности к такому обществу:

- a) информационному;
- b) открытому;
- c) закрытому.

4. Документооборот – это:

- a) движение документов в организации с момента их создания или получения до завершения исполнения или отправки; +
- b) вид государственной, муниципальной, научной, коммерческой и некоммерческой деятельности;
- c) это система стандартов по информации, библиотечному и издательскому делу.

5. Аутентификация – это:

- a) механизм разграничения доступа к данным и функциям системы;
- b) способность подтвердить личность пользователя; +
- c) поиск и исследование математических методов преобразования информации.

6. В информационных системах документированная информация представлена в виде:

- a) файлов, папок, массивов, баз данных, программ;
- b) баз данных и программного обеспечения;
- c) файлов и баз данных.

7. Информационные ресурсы могут быть:

- a) открытые, закрытые;
- b) открытые и ограниченного доступа;
- c) ограниченного доступа.

8. Режим защиты информации устанавливается:

- a) в отношении сведений, отнесенных к государственной тайне;
- b) в отношении конфиденциальной информации;
- c) в отношении сведений, отнесенных к государственной тайне и персональных данных.

9. Что подлежит обязательной сертификации:

- a) автоматизированные системы органов государственной власти, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих систем;
- b) автоматизированные системы органов муниципальной власти, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих систем;
- c) автоматизированные системы, которые обрабатывают сведения, составляющие государственную тайну.

Задания для самостоятельной работы.

1. Что такое информация и каковы уровни ее представления?
2. Перечислите основные носители информации, особенности их использования и защиты.
3. Какими свойствами определяется ценность информации?
4. Какие критерии оценки ценности информации Вы можете предложить?
5. Приведите примеры различной зависимости ценности информации от времени.

6. Что понимается под информационными ресурсами?
7. Что не разрешается относить к информации ограниченного доступа?
8. Что понимается под конфиденциальной информацией?
9. Какие существуют виды тайны?
10. Какое назначение имеет перечень конфиденциальных сведений предприятия?

Тема 3. Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности. (ПК-1)

Лекция.

Информационная безопасность и ее место в системе национальной безопасности Российской Федерации. Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность.

Лабораторные работы.

1. Каковы функции руководителей предприятий при организации защиты информации?
2. Каковы основные функции ФСТЭК?
3. Каковы основные функции ФСБ?
4. Каковы основные функции межведомственной комиссии?
5. Каковы основные функции Совета безопасности РФ?
6. Кто ответственный за использование несертифицированных средств защиты информации в автоматизированных системах?

Задания для самостоятельной работы.

1. Каково место информационной безопасности в системе национальной безопасности Российской Федерации?
2. Сформулируйте основные положения Доктрины информационной безопасности РФ.
3. Каковы основные цели защиты информации?
4. Каковы основные задачи в области информационной безопасности?
5. Какова структура государственной системы защиты информации?
6. Кто несет ответственность за нарушение режима защиты информации?
7. Покажите роль различных министерств и ведомств в вопросах защиты информации.

Тема 4. Угрозы информационной безопасности. (ПК-1)

Лекция.

Анализ уязвимостей системы. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз. Неформальная модель нарушителя. Оценка уязвимости системы.

Лабораторные работы.

1. При проектировании системы защиты необходимо:
 - a) определение перечня угроз и построение модели нарушителя;
 - b) определение программно-аппаратных средств защиты информации;
 - c) определение сертифицированных средств защиты и построение модели нарушителя.
2. Анализ уязвимостей обязательная процедура.....
 - a) при анализе средств защиты информации;
 - b) при аттестации объекта информатизации;
 - c) при определении модели нарушителя.
3. Естественные угрозы безопасности информации вызваны:
 - a) деятельностью человека;
 - b) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;

- с) воздействиями объективных физических процессов или стихийных природных явлений, независимых от человека;
- д) корыстными устремлениями злоумышленников;
- е) ошибками при действиях персонала.

4. Искусственные угрозы безопасности информации вызваны:

- а) деятельностью человека;
- б) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
- с) воздействиями объективных физических процессов или стихийных природных явлений, независимых от человека;
- д) корыстными устремлениями злоумышленников;
- е) ошибками при действиях персонала.

5. К основным непреднамеренным искусственным угрозам АСОИ относится:

- а) физическое разрушение системы путем взрыва, поджога и т.п.;
- б) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
- с) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
- д) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
- е) неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.

6. К посторонним лицам нарушителям информационной безопасности относится:

- а) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
- б) персонал, обслуживающий технические средства;
- с) технический персонал, обслуживающий здание;
- д) пользователи;
- е) сотрудники службы безопасности.
- ф) представители конкурирующих организаций.
- г) лица, нарушившие пропускной режим;

7. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

- а) сотрудники;
- б) хакеры;
- с) атакующие;
- д) контрагенты (лица, работающие по договору).

8. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

- а) владельцы данных;
- б) пользователи;
- с) администраторы;
- д) руководство.

Задания для самостоятельной работы.

1. На примере нескольких различных угроз покажите, что их осуществление приведет к изменению одного из основных свойств защищаемой информации (конфиденциальности, целостности, доступности).

2. Приведите примеры систем, для которых наибольшую угрозу безопасности представляет нарушение конфиденциальности информации.

3. Для каких систем (приведите примеры) наибольшую опасность представляет нарушение целостности информации?
4. В каких системах на первом месте стоит обеспечение доступности информации?
5. В чем различие понятий «нарушение конфиденциальности информации», «несанкционированный доступ к информации», «утечка информации»?
6. Определите перечень основных угроз для АС, состоящей из автономно работающего компьютера без выхода в сеть, расположенной в одной из лабораторий университета.
7. Постройте неформальную модель нарушителя для учебной компьютерной лаборатории.
8. Выведите формулу для расчета прочности трехуровневой защитной оболочки.
9. Охарактеризуйте защитные оболочки и перечень преград, применяемые в учебной компьютерной лаборатории

Тема 5. Построение систем защиты от угрозы нарушения конфиденциальности . (ПК-1)

Лекция.

Определение и основные способы несанкционированного доступа. Методы защиты от НСД. Организационные методы защиты от НСД. Инженерно-технические методы защиты от НСД. Построение систем защиты от угрозы утечки по техническим каналам. Идентификация и аутентификация. Основные направления и цели использования криптографических методов. Защита от угрозы нарушения конфиденциальности на уровне содержания информации.

Лабораторные работы.

1. Основные источники угроз информационной безопасности:
 - a) Хищение жестких дисков, подключение к сети, инсайдерство;
 - b) Перехват данных, хищение данных, изменение архитектуры системы;+
 - c) Хищение данных, подкуп системных администраторов, нарушение регламента работы.
2. Определите виды информационной безопасности:
 - a) Персональная, корпоративная, государственная;
 - b) Клиентская, серверная, сетевая;
 - c) Локальная, глобальная, смешанная.
3. Отметьте основную массу угроз информационной безопасности:
 - a) Троянские программы ;
 - b) Шпионские программы;
 - c) Черви.
4. Вид идентификации и аутентификации, который получил наибольшее распространение:
 - a) системы PKI;
 - b) постоянные пароли;
 - c) одноразовые пароли.
5. Определите, под какие системы распространение вирусов происходит наиболее динамично:
 - a) Windows;
 - b) Mac OS;
 - c) Android.
6. Цели информационной безопасности – своевременное обнаружение, предупреждение:
 - a) несанкционированного доступа, воздействия в сети;
 - b) воздействия в сети;
 - c) чрезвычайных ситуаций.

7. Определите основные объекты информационной безопасности:
 - a) Компьютерные сети, базы данных;
 - b) Информационные системы, психологическое состояние пользователей;
 - c) Бизнес-ориентированные, коммерческие системы.
8. Методы защиты от НСД:
 - a) организационные, правовые, технологические;
 - b) морально-этические, финансовые;
 - c) инженерно-технические, правовые.
9. В соответствии с ГОСТ Р 50922–96 рассматриваются три вида утечки информации основными причинами утечки информации являются:
 - a) ошибки в проектировании системы и систем защиты, несоблюдение персоналом норм, требований, правил эксплуатации;
 - b) ведение противостоящей стороной технической и агентурной разведок;
 - c) применение несертифицированных средств защиты, ошибки персонала.
10. В соответствии с ГОСТ Р 50922–96 рассматриваются три вида утечки информации:
 - a) разглашение;
 - b) несанкционированный доступ к информации;
 - c) получение защищаемой информации разведками;
 - d) Хищение, модификация, разглашение.
11. Эффективная защита от НСД возможна при сочетании
 - a) организационных, правовых методов;
 - b) сертифицированных средств защиты, организационных методов.
 - c) технических, нормативно-правовых методов;
12. Для перекрытия каналов несанкционированного доступа к информации большое значение имеет:
 - a) построение систем идентификации и аутентификации;
 - b) построение систем идентификации;
 - c) применение технических, нормативно-правовых методов.
13. Криптографические методы защиты информации от несанкционированного доступа являются единственным надежным средством защиты при передаче информации по:
 - a) каналам связи;
 - b) по сети интернет;
 - c) по корпоративной сети.

Задания для самостоятельной работы.

1. В чем отличие терминов «НСД» и «Нарушение конфиденциальности информации»?
2. Что понимается под утечкой информации?
3. Каким образом классифицируются каналы утечки информации?
4. Каким образом следует выбирать меры защиты конфиденциальности информации?
5. Дайте определение идентификации и аутентификации пользователя. В чем разница между этими понятиями?
6. Перечислите основные способы аутентификации. Какой, на Ваш взгляд, является наиболее эффективным?
7. Какие основные методы контроля доступа используются в известных вам информационных системах? В чем их достоинства и недостатки?

8. Почему аутентификация с использованием пароля считается в настоящее время ненадежной?
9. Каковы методы аутентификации с использованием предметов заданного типа? Назовите те, которые получили распространение в последнее время.
10. Дайте определение шифра и сформулируйте основные требования к нему.
11. Поясните, что понимается под совершенным шифром.
12. Почему большинство современных шифрограмм могут быть однозначно дешифрованы?
13. Каким образом государство регулирует использование средств криптозащиты?

Тема 6. Построение систем защиты от угрозы нарушения целостности информации и отказа доступа. (ПК-1)

Лекция.

Защита целостности информации при хранении. Защита целостности информации при обработке. Защита целостности информации при транспортировке. Защита от угрозы нарушения целостности информации на уровне содержания. Построение систем защиты от угрозы отказа доступа к информации. Защита семантического анализа и актуальности информации. Применение общенаучных методов, законы физики, математический аппарат, методы моделирования и прогнозирования в сфере защиты информации.

Лабораторные работы.

1. Как называется умышленно искаженная информация?
 - a) Дезинформация
 - b) Информативный поток
 - c) Достоверная информация
 - d) Перестает быть информацией
2. Как называется информация, к которой ограничен доступ?
 - a) Недоступная
 - b) Противозаконная
 - c) Открытая
 - d) Конфиденциальная
3. Какими путями может быть получена информация?
 - a) Проведением, покупкой и противоправным добыванием информации научных исследований
 - b) Захватом и взломом ПК информации научных исследований
 - c) Добыванием информации из внешних источников и скремблированием информации научных исследований
 - d) Захватом и взломом защитной системы для информации научных исследований
4. Как называются компьютерные системы, в которых обеспечивается безопасность информации?
 - a) Защищенные КС
 - b) Небезопасные КС
 - c) Самодостаточные КС
 - d) Саморегулирующиеся КС
5. Основной документ, на основе которого проводится политика информационной безопасности?
 - a) Политическая информационная безопасность
 - b) Регламент информационной безопасности
 - c) Программа информационной безопасности
 - d) Протекторат
6. В зависимости от формы представления информация может быть разделена на?
 - a) Мысль, слово и речь

- b) Речевую, документированную и телекоммуникационную
 - c) Цифровая, звуковая и тайная
 - d) Цифровая, звуковая
7. К каким процессам относят процессы сбора, обработки, накопления, хранения, поиска и распространения информации
- a) Информационным процессам
 - b) Мыслительным процессам
 - c) Машинным процессам
 - d) Микропроцессам
8. Что называют защитой информации?
- a) Называют деятельность по предотвращению непреднамеренных воздействий на защищаемую информацию
 - b) Называют деятельность по предотвращению утечки защищаемой информации
 - c) Называют деятельность по предотвращению несанкционированных воздействий на защищаемую информацию
 - d) Все ответы верны
9. Под непреднамеренным воздействием на защищаемую информацию понимают?
- a) Возможности ее преобразования, при котором содержание информации изменяется на ложную информацию;
 - b) Процесс ее преобразования, при котором содержание информации изменяется на ложную;
 - c) Воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств и воздействие природных явлений;
 - d) Не ограничения доступа в отдельные отрасли экономики или на конкретные производства.
10. Шифрование информации это:
- a) Процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов
 - b) Процесс преобразования, при котором информация удаляется
 - c) Процесс ее преобразования, при котором содержание информации изменяется на ложную
 - d) Процесс преобразования информации в машинный код

Задания для самостоятельной работы.

1. Каковы способы контроля целостности потока сообщений?
2. Какие существуют способы контроля целостности сообщений при взаимном доверии сторон?
3. Как контролировать целостность сообщений при высоком уровне помех в каналах связи?
4. Как организован обмен документами, заверенными цифровой подписью?
5. В чем отличие и сходство обычной и цифровой подписей?
6. Какими принципами нужно руководствоваться для сохранения целостности данных при их обработке?
7. Почему проблемы контроля целостности данных относятся к проблемам информационной безопасности?
8. Что означает контроль целостности данных на уровне содержания? Приведите примеры.
9. Как обеспечить целостность данных при их хранении?
10. Что такое надежность и чем отличается надежность аппаратуры от надежности программного обеспечения?
11. Следует ли различать защиту от случайных угроз и от действий злоумышленника при обеспечении беспрепятственного доступа к информации? Обоснуйте свой ответ.
12. Как защитить программное обеспечение от изучения логики его работы?
13. Предложите меры по обеспечению более надежной работы ЛВС университета.

14. Как изменяется надежность аппаратуры с течением времени?
15. Каковы способы повышения надежности аппаратуры и линий связи?

Тема 7. Политика и модели безопасности. (ПК-1)

Лекция.

Политика безопасности. Субъектно-объектные модели разграничения доступа. Аксиомы политики безопасности. Политика и модели дискреционного доступа. Парольные системы разграничения доступа. Политика и модели мандатного доступа. Теоретико-информационные модели. Политика и модели тематического разграничения доступа. Ролевая модель безопасности.

Лабораторные работы.

- 1) При полномочной политике безопасности совокупность меток с одинаковыми значениями образует:
 - a) Область равной критичности;
 - b) Область равного доступа;
 - c) Уровень безопасности;
 - d) Уровень доступности.
- 2) Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования это:
 - a) уязвимость информации;
 - b) надежность информации;
 - c) защищенность информации;
 - d) безопасность информации.
- 3) Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы это:
 - a) авторизация;
 - b) аудит;
 - c) идентификация;
 - d) аутентификация.
- 4) С помощью закрытого ключа информация:
 - a) копируется;
 - b) транслируется;
 - c) расшифровывается;
 - d) зашифровывается.
- 5) Совокупность свойств, обуславливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением, называется:
 - a) актуальностью информации;
 - b) доступностью;
 - c) качеством информации;
 - d) целостностью.
- 6) Недостатком модели конечных состояний политики безопасности является:
 - a) изменение линии связи;
 - b) статичность;
 - c) сложность реализации;
 - d) низкая степень надежности.
- 7) Метод управления доступом, при котором каждому объекту системы присваивается метка критичности, определяющая ценность информации, называется:
 - a) идентифицируемым;
 - b) мандатным;
 - c) избирательным;
 - d) привилегированным.

8) Организационные требования к системе защиты:

- a) управленческие и идентификационные;
- b) административные и аппаратные;
- c) административные и процедурные;
- d) аппаратные и физические.

9) Основу политики безопасности составляет:

- a) программное обеспечение;
- b) управление рисками;
- c) способ управления доступом;
- d) выбор канала связи.

10) Наукой, изучающей математические методы защиты информации путем ее преобразования, является:

- a) криптография;
- b) стенография;
- c) криптоанализ;
- d) криптология.

11) Согласно «Оранжевой книге» минимальную защиту имеет группа критериев:

- a) C;
- b) A;
- c) B;
- d) D.

12) С точки зрения ГТК основной задачей средств безопасности является обеспечение:

- a) сохранности информации;
- b) защиты от НСД;
- c) простоты реализации;
- d) надёжности функционирования.

13) Согласно «Оранжевой книге» дискреционную защиту имеет группа критериев:

- a) D;
- b) A;
- c) B;
- d) C.

14) При качественном подходе риск измеряется в терминах:

- a) денежных потерь;
- b) заданных с помощью шкалы ранжирования;
- c) оценок экспертов;
- d) объёма информации.

15) Согласно «Европейским критериям» формальное описание функций безопасности требуется на уровне:

- a) E5;
- b) E7;
- c) E4;
- d) E6.

Задания для самостоятельной работы.

1. Подготовка к практическим занятиям, повторение изучения лекционного материала;
2. Подготовка к лекциям, повторение учебного материала предыдущих лекций;
3. Изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях;

Лекция.

Роль стандартов информационной безопасности. Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC. Европейские критерии безопасности информационных технологий (ITSEC). Федеральные критерии безопасности информационных технологий США. Единые критерии безопасности информационных технологий. Группа международных стандартов 270000.

Лабораторные работы.

Цель работы: ознакомление с основными международными стандартами, регламентирующими обеспечение защиты конфиденциальной информации.

При выполнении задания следует проанализировать содержание следующих основных международных стандартов безопасности:

1. Международный стандарт управления информационной безопасностью ISO 17799.
2. Общие критерии безопасности информационных технологий ГОСТ ИСО\МЭК 15408.
3. Критерии оценки надежности компьютерных систем («Оранжевая книга»).
4. Канадские критерии и Общие критерии.
5. Стандарт COBIT («Контрольные объекты для информационных и смежных технологий»).

Необходимо сопоставить эти стандарты с российской нормативной базой в области информационной безопасности и оценить их применимость в России.

Задания для самостоятельной работы.

1. Подготовка к практическим занятиям, повторение изучения лекционного материала.
2. Подготовка к лекциям, повторение учебного материала предыдущих лекций.
3. Изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях.

Тема 9. Информационные войны и информационное противоборство. (ПК-1)

Лекция.

Определение и основные виды информационных войн. Требования разделены на три группы: стратегия, подотчетность, гарантии. Информационно-техническая война. Информационно-психологическая война.

Лабораторные работы.

Практическое задание.

Цель работы:

1. Закрепить знания нормативно – законодательной базе Российской Федерации по вопросам информационной войны.
2. Закрепить понятия: информационные операции, психологические операции, оперативная маскировка, радиоэлектронная борьба.

Задания:

Вариант №1.

1. Каковы социальные и личностные предпосылки возникновения информационных операций и войн?
2. Каковы особенности стратегического планирования в информационных войнах?
3. Опишите базовые стратегии информационных войн.
4. Опишите стратегии, использованные оппозицией для свержения правительства в процессе «цветных» революций.
5. Гуманитарные аспекты информационного оружия и проиллюстрируйте их собственными найденными примерами из вашей жизни или из жизни современного общества.

Вариант №2.

1. Истинные цели и причины использования информационного оружия.
2. Средства и способы ведения информационно-психологической войны.
3. Виды угроз безопасности личности, общества и государства в условиях информационно-психологической войны.

4. Источники угроз безопасности личности, общества и государства в условиях информационно-психологической войны.

5. Опишите особенности быстрого реагирования на внезапно выявленные акции (мероприятия) информационно-психологической агрессии (войны).

Задания для самостоятельной работы.

1. Подготовка к практическим занятиям, повторение изучения лекционного материала;
2. Подготовка к лекциям, повторение учебного материала предыдущих лекций;
3. Изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях;

4. Контроль знаний обучающихся и типовые оценочные средства

4.1. Распределение баллов:

2 семестр

- посещаемость – 5 баллов
- текущий контроль – 81 балл
- контрольные срезы – 2 среза по 7 баллов каждый
- премиальные баллы – 14 баллов

Распределение баллов по заданиям:

№ темы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Мак. кол-во баллов	Методика проведения занятия и оценки
1.	Основные понятия теории информационной безопасности.	Тестирование	7	Тест состоит из вопросов с выбором ответа. 7 баллов - студент правильно отвечает более чем на 90% вопросов. 4-6 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 2-3 балла - студент правильно отвечает на 30-50% вопросов. 1 балл - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
2.	Информация как объект защиты.	Тестирование(контрольный срез)	7	Тест состоит из вопросов с выбором ответа. 7 баллов - студент правильно отвечает более чем на 90% вопросов. 4-6 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 2-3 балла - студент правильно отвечает на 30-50% вопросов. 1 балл - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.

3.	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности.	Опрос	7	<p>Опрос предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.</p> <p>Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения поставленной учебной задачи; - своевременность и эффективность использования наглядных пособий и технических средств при ответе; - использование дополнительного материала; - рациональность использования времени, отведенного на задание. <p>7 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>5 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>2 балла – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.</p>
4.	Угрозы информационной безопасности.	Тестирование	7	<p>Тест состоит из вопросов с выбором ответа.</p> <p>7 баллов - студент правильно отвечает более чем на 90% вопросов.</p> <p>4-6 баллов – студент правильно отвечает на 50-80% вопросов в тесте.</p> <p>2-3 балла - студент правильно отвечает на 30-50% вопросов.</p> <p>1 балл - студент правильно отвечает на 25-30% вопросов в тесте.</p> <p>Менее 25% правильных ответов баллов не дает.</p>
5.	Построение систем защиты от угрозы нарушения конфиденциальности .	Тестирование	7	<p>Тест состоит из вопросов с выбором ответа.</p> <p>7 баллов - студент правильно отвечает более чем на 90% вопросов.</p> <p>4-6 баллов – студент правильно отвечает на 50-80% вопросов в тесте.</p> <p>2-3 балла - студент правильно отвечает на 30-50% вопросов.</p> <p>1 балл - студент правильно отвечает на 25-30% вопросов в тесте.</p> <p>Менее 25% правильных ответов баллов не дает.</p>
6.	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа.	Тестирование	17	<p>Тест состоит из вопросов с выбором ответа.</p> <p>17 баллов - студент правильно отвечает более чем на 90% вопросов.</p> <p>6 баллов – студент правильно отвечает на 50-80% вопросов в тесте.</p> <p>2-3 балла - студент правильно отвечает на 30-50% вопросов.</p> <p>1 балл - студент правильно отвечает на 25-30% вопросов в тесте.</p> <p>Менее 25% правильных ответов баллов не дает.</p>

7.	Политика и модели безопасности.	Тестирование(контрольный срез)	7	Тест состоит из вопросов с выбором ответа. 7 баллов - студент правильно отвечает более чем на 90% вопросов. 4-6 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 2-3 балла - студент правильно отвечает на 30-50% вопросов. 1 балл - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
8.	Обзор международных стандартов информационной безопасности.	Выполнение практических заданий	18	Лабораторные работы выполняются по тематике практических занятий. 18 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию 10 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы 3 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы
9.	Информационные войны и информационное противоборство.	Выполнение практических заданий	18	Лабораторные работы выполняются по тематике практических занятий. 18 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию 10 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы 3 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы
10.	Посещаемость		5	5 баллов – стопроцентное посещение занятий студентом 4 баллов – посещаемость студента составляет не менее 80 % занятий 3 баллов – посещаемость студента составляет не менее 50 % занятий 2 балла – посещаемость студента составляет не менее 25 % занятий
11.	Премиальные баллы		14	Дополнительные премиальные баллы могут быть начислены: - за проект, выполненный по заказу работодателя и реализованный на практике – 20 баллов; - постоянная активность во время практических занятий – 10 баллов; - полностью подготовленная к публикации статья по тематике в рамках дисциплины – 10 баллов; - участие с докладом во всероссийской олимпиаде по тематике изучаемой дисциплины – 20 баллов; - участие в выставке по тематике изучаемой дисциплины – 20 баллов; - публикация статьи по тематике изучаемой дисциплины в сборнике студенческих работ / материалах всероссийской конференции / журнале из перечня ВАК – 10 / 15 / 20

12.	Индивидуальные задания, с помощью которых можно набрать дополнительные баллы	20	Решение кейса (10 баллов) Прохождение тестирования (30 вопросов) по всему курсу дисциплины (10 баллов)
13.	Итого за семестр	100	

Итоговая оценка по зачету выставляется в 100-балльной шкале и в традиционной четырехбалльной шкале. Перевод 100-балльной рейтинговой оценки по дисциплине в традиционную четырехбалльную осуществляется следующим образом:

100-балльная система	Традиционная система
50 - 100 баллов	Зачтено
0 - 49 баллов	Не зачтено

4.2 Типовые оценочные средства текущего контроля

Выполнение практических заданий

Тема 8. Обзор международных стандартов информационной безопасности.

Цель работы: ознакомление с основными международными стандартами, регламентирующими обеспечение защиты конфиденциальной информации.

При выполнении задания следует проанализировать содержание следующих основных международных стандартов безопасности:

1. Международный стандарт управления информационной безопасностью ISO 17799.
2. Общие критерии безопасности информационных технологий ГОСТ ИСО\МЭК 15408.
3. Критерии оценки надежности компьютерных систем («Оранжевая книга»).
4. Канадские критерии и Общие критерии.
5. Стандарт COBIT («Контрольные объекты для информационных и смежных технологий»).

Необходимо сопоставить эти стандарты с российской нормативной базой в области информационной безопасности и оценить их применимость в России.

Тема 9. Информационные войны и информационное противоборство.

Практическое задание.

Цель работы:

1. Закрепить знания нормативно – законодательной базе Российской Федерации по вопросам информационной войны.
2. Закрепить понятия: информационные операции, психологические операции, оперативная маскировка, радиоэлектронная борьба.

Задания:

Вариант №1.

1. Каковы социальные и личностные предпосылки возникновения информационных операций и войн?
2. Каковы особенности стратегического планирования в информационных войнах?
3. Опишите базовые стратегии информационных войн.
4. Опишите стратегии, использованные оппозицией для свержения правительства в процессе «цветных» революций.
5. Гуманитарные аспекты информационного оружия и проиллюстрируйте их собственными найденными примерами из вашей жизни или из жизни современного общества.

Вариант №2.

1. Истинные цели и причины использования информационного оружия.
2. Средства и способы ведения информационно-психологической войны.

3. Виды угроз безопасности личности, общества и государства в условиях информационно-психологической войны.
4. Источники угроз безопасности личности, общества и государства в условиях информационно-психологической войны.
5. Опишите особенности быстрого реагирования на внезапно выявленные акции (мероприятия) информационно-психологической агрессии (войны).

Опрос

Тема 3. Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности.

1. Каковы функции руководителей предприятий при организации защиты информации?
2. Каковы основные функции ФСТЭК?
3. Каковы основные функции ФСБ?
4. Каковы основные функции межведомственной комиссии?
5. Каковы основные функции Совета безопасности РФ?
6. Кто ответственный за использование несертифицированных средств защиты информации в автоматизированных системах?

Тестирование

Тема 1. Основные понятия теории информационной безопасности.

1. Информация это:
 - a) сведения, поступающие от СМИ;
 - b) только документированные сведения о лицах, предметах, фактах, событиях;
 - c) сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;
 - d) только сведения, содержащиеся в электронных базах данных.
2. Информация
 - a) не исчезает при потреблении;
 - b) становится доступной, если она содержится на материальном носителе;
 - c) подвергается только "моральному износу";
 - d) характеризуется всеми перечисленными свойствами.
3. Информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать, называется:
 - a) достоверной;
 - b) конфиденциальной;
 - c) документированной;
 - d) коммерческой тайной.
4. Информационно-телекоммуникационная сеть это:
 - a) технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;
 - b) технологическая система, предназначенная для передачи по сети интернет, доступ к которой осуществляется с использованием средств вычислительной техники;
 - c) технологическая система, предназначенная для передачи информации по локально сети, доступ к которой осуществляется с использованием средств вычислительной техники.

5. Доступ к информации это:
 - a) возможность получения информации;
 - b) возможность получения информации, и ее использования;
 - c) возможность получения информации, и ее распространения.

6. Предоставление информации это действия, направленные:
 - a) на получение информации определенным кругом лиц;
 - b) на получение информации руководителем и передачу информации определенному кругу лиц;
 - c) на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

7. Информационная безопасность это:
 - a) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре;
 - b) защищенность программных продуктов предприятия от случайных или преднамеренных воздействий естественного или случайного характера;
 - c) защищенность информации, циркулирующей в сети от случайных или преднамеренных воздействий естественного или случайного характера.

8. Безопасность информации это защищенность информации:
 - a) от разглашения, искажения, утраты;
 - b) от разглашения, искажения, утраты или снижения степени доступности информации, а также незаконного ее тиражирования;
 - c) от передачи третьим лицам, искажения и не законного использования.

9. Угроза – это:
 - a) потенциальная возможность определенным образом нарушить информационную безопасность;
 - b) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных;
 - c) процесс определения отвечает на текущее состояние разработки требованиям данного этапа.

10. Эффективное обеспечение защиты информации возможно:
 - a) только на основе комплексного использования всех известных методов и подходов к решению данной проблемы;
 - b) только при использовании сертифицированных средств защиты информации;
 - c) только при использовании технических средств защиты информации;
 - d) Все ответы правильные.

Тема 2. Информация как объект защиты.

1. Документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, депозитариях, музейных хранилищах и т. п.):
 - a) информационные ресурсы;
 - b) информационные продукты;
 - c) информационные ракурсы.

2. Информационные ресурсы являются одним из видов общественных, экономических ресурсов:
 - a) факторов ведения дел;

- b) факторов производства;
- c) факторов деятельности.

3. Уровень развития сферы информационных услуг во многом определяет степень приближенности к такому обществу:

- a) информационному;
- b) открытому;
- c) закрытому.

4. Документооборот – это:

- a) движение документов в организации с момента их создания или получения до завершения исполнения или отправки; +
- b) вид государственной, муниципальной, научной, коммерческой и некоммерческой деятельности;
- c) это система стандартов по информации, библиотечному и издательскому делу.

5. Аутентификация – это:

- a) механизм разграничения доступа к данным и функциям системы;
- b) способность подтвердить личность пользователя; +
- c) поиск и исследование математических методов преобразования информации.

6. В информационных системах документированная информация представлена в виде:

- a) файлов, папок, массивов, баз данных, программ;
- b) баз данных и программного обеспечения;
- c) файлов и баз данных.

7. Информационные ресурсы могут быть:

- a) открытые, закрытые;
- b) открытые и ограниченного доступа;
- c) ограниченного доступа.

8. Режим защиты информации устанавливается:

- a) в отношении сведений, отнесенных к государственной тайне;
- b) в отношении конфиденциальной информации;
- c) в отношении сведений, отнесенных к государственной тайне и персональных данных.

9. Что подлежит обязательной сертификации:

- a) автоматизированные системы органов государственной власти, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих систем;
- b) автоматизированные системы органов муниципальной власти, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих систем;
- c) автоматизированные системы, которые обрабатывают сведения, составляющие государственную тайну.

Тема 4. Угрозы информационной безопасности.

1. При проектировании системы защиты необходимо:

- a) определение перечня угроз и построение модели нарушителя;
- b) определение программно-аппаратных средств защиты информации;

- c) определение сертифицированных средств защиты и построение модели нарушителя.
2. Анализ уязвимостей обязательная процедура.....
 - a) при анализе средств защиты информации;
 - b) при аттестации объекта информатизации;
 - c) при определении модели нарушителя.
 3. Естественные угрозы безопасности информации вызваны:
 - a) деятельностью человека;
 - b) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
 - c) воздействиями объективных физических процессов или стихийных природных явлений, независимых от человека;
 - d) корыстными устремлениями злоумышленников;
 - e) ошибками при действиях персонала.
 4. Искусственные угрозы безопасности информации вызваны:
 - a) деятельностью человека;
 - b) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
 - c) воздействиями объективных физических процессов или стихийных природных явлений, независимых от человека;
 - d) корыстными устремлениями злоумышленников;
 - e) ошибками при действиях персонала.
 5. К основным непреднамеренным искусственным угрозам АСОИ относится:
 - a) физическое разрушение системы путем взрыва, поджога и т.п.;
 - b) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
 - c) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
 - d) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
 - e) неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.
 6. К посторонним лицам нарушителям информационной безопасности относится:
 - a) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
 - b) персонал, обслуживающий технические средства;
 - c) технический персонал, обслуживающий здание;
 - d) пользователи;
 - e) сотрудники службы безопасности.
 - f) представители конкурирующих организаций.
 - g) лица, нарушившие пропускной режим;
 7. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
 - a) сотрудники;
 - b) хакеры;
 - c) атакующие;
 - d) контрагенты (лица, работающие по договору).

8. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

- a) владельцы данных;
- b) пользователи;
- c) администраторы;
- d) руководство.

Тема 5. Построение систем защиты от угрозы нарушения конфиденциальности .

1. Основные источники угроз информационной безопасности:

- a) Хищение жестких дисков, подключение к сети, инсайдерство;
- b) Перехват данных, хищение данных, изменение архитектуры системы;+
- c) Хищение данных, подкуп системных администраторов, нарушение регламента работы.

2. Определите виды информационной безопасности:

- a) Персональная, корпоративная, государственная;
- b) Клиентская, серверная, сетевая;
- c) Локальная, глобальная, смешанная.

3. Отметьте основную массу угроз информационной безопасности:

- a) Троянские программы ;
- b) Шпионские программы;
- c) Черви.

4. Вид идентификации и аутентификации, который получил наибольшее распространение:

- a) системы PKI;
- b) постоянные пароли;
- c) одноразовые пароли.

5. Определите, под какие системы распространение вирусов происходит наиболее динамично:

- a) Windows;
- b) Mac OS;
- c) Android.

6. Цели информационной безопасности – своевременное обнаружение, предупреждение:

- a) несанкционированного доступа, воздействия в сети;
- b) воздействия в сети;
- c) чрезвычайных ситуаций.

7. Определите основные объекты информационной безопасности:

- a) Компьютерные сети, базы данных;
- b) Информационные системы, психологическое состояние пользователей;
- c) Бизнес-ориентированные, коммерческие системы.

8. Методы защиты от НСД:

- a) организационные, правовые, технологические;
- b) морально-этические, финансовые;
- c) инженерно-технические, правовые.

9. В соответствии с ГОСТ Р 50922–96 рассматриваются три вида утечки информации основными причинами утечки информации являются:
- ошибки в проектировании системы и систем защиты, несоблюдение персоналом норм, требований, правил эксплуатации;
 - ведение противостоящей стороной технической и агентурной разведок;
 - применение несертифицированных средств защиты, ошибки персонала.
10. В соответствии с ГОСТ Р 50922–96 рассматриваются три вида утечки информации:
- разглашение;
 - несанкционированный доступ к информации;
 - получение защищаемой информации разведками;
 - хищение, модификация, разглашение.
11. Эффективная защита от НСД возможна при сочетании
- организационных, правовых методов;
 - сертифицированных средств защиты, организационных методов.
 - технических, нормативно-правовых методов;
12. Для перекрытия каналов несанкционированного доступа к информации большое значение имеет:
- построение систем идентификации и аутентификации;
 - построение систем идентификации;
 - применение технических, нормативно-правовых методов.
13. Криптографические методы защиты информации от несанкционированного доступа являются единственным надежным средством защиты при передаче информации по:
- каналам связи;
 - по сети интернет;
 - по корпоративной сети.

Тема 6. Построение систем защиты от угрозы нарушения целостности информации и отказа доступа.

- Как называется умышленно искаженная информация?
 - Дезинформация
 - Информативный поток
 - Достоверная информация
 - Перестает быть информацией
- Как называется информация, к которой ограничен доступ?
 - Недоступная
 - Противозаконная
 - Открытая
 - Конфиденциальная
- Какими путями может быть получена информация?
 - Проведением, покупкой и противоправным добыванием информации научных исследований
 - Захватом и взломом ПК информации научных исследований
 - Добытием информации из внешних источников и скремблированием информации научных исследований
 - Захватом и взломом защитной системы для информации научных исследований

4. Как называются компьютерные системы, в которых обеспечивается безопасность информации?
 - a) Защищенные КС
 - b) Небезопасные КС
 - c) Самодостаточные КС
 - d) Саморегулирующиеся КС

5. Основной документ, на основе которого проводится политика информационной безопасности?
 - a) Политическая информационная безопасность
 - b) Регламент информационной безопасности
 - c) Программа информационной безопасности
 - d) Протекторат
6. В зависимости от формы представления информация может быть разделена на?
 - a) Мысль, слово и речь
 - b) Речевую, документированную и телекоммуникационную
 - c) Цифровая, звуковая и тайная
 - d) Цифровая, звуковая
7. К каким процессам относят процессы сбора, обработки, накопления, хранения, поиска и распространения информации
 - a) Информационным процессам
 - b) Мыслительным процессам
 - c) Машинным процессам
 - d) Микропроцессам

8. Что называют защитой информации?
 - a) Называют деятельность по предотвращению непреднамеренных воздействий на защищаемую информацию
 - b) Называют деятельность по предотвращению утечки защищаемой информации
 - c) Называют деятельность по предотвращению несанкционированных воздействий на защищаемую информацию
 - d) Все ответы верны

9. **Под непреднамеренным воздействием на защищаемую информацию понимают?**
 - a) Возможности ее преобразования, при котором содержание информации изменяется на ложную информацию;
 - b) Процесс ее преобразования, при котором содержание информации изменяется на ложную;
 - c) Воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств и воздействие природных явлений;
 - d) Не ограничения доступа в отдельные отрасли экономики или на конкретные производства.

10. Шифрование информации это:
 - a) Процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов
 - b) Процесс преобразования, при котором информация удаляется
 - c) Процесс ее преобразования, при котором содержание информации изменяется на ложную
 - d) Процесс преобразования информации в машинный код

Тема 7. Политика и модели безопасности.

1) При полномочной политике безопасности совокупность меток с одинаковыми значениями образует:

- a) Область равной критичности;
 - b) Область равного доступа;
 - c) Уровень безопасности;
 - d) Уровень доступности.
- 2) Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования это:
- a) уязвимость информации;
 - b) надежность информации;
 - c) защищенность информации;
 - d) безопасность информации.
- 3) Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы это:
- a) авторизация;
 - b) аудит;
 - c) идентификация;
 - d) аутентификация.
- 4) С помощью закрытого ключа информация:
- a) копируется;
 - b) транслируется;
 - c) расшифровывается;
 - d) зашифровывается.
- 5) Совокупность свойств, обуславливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением, называется:
- a) актуальностью информации;
 - b) доступностью;
 - c) качеством информации;
 - d) целостностью.
- 6) Недостатком модели конечных состояний политики безопасности является:
- a) изменение линии связи;
 - b) статичность;
 - c) сложность реализации;
 - d) низкая степень надежности.
- 7) Метод управления доступом, при котором каждому объекту системы присваивается метка критичности, определяющая ценность информации, называется:
- a) идентифицируемым;
 - b) мандатным;
 - c) избирательным;
 - d) привилегированным.
- 8) Организационные требования к системе защиты:
- a) управленческие и идентификационные;
 - b) административные и аппаратные;
 - c) административные и процедурные;
 - d) аппаратные и физические.
- 9) Основу политики безопасности составляет:
- a) программное обеспечение;
 - b) управление рисками;
 - c) способ управления доступом;
 - d) выбор канала связи.

10) Наукой, изучающей математические методы защиты информации путем ее преобразования, является:

- a) криптография;
- b) стенография;
- c) криптоанализ;
- d) криптология.

11) Согласно «Оранжевой книге» минимальную защиту имеет группа критериев:

- a) C;
- b) A;
- c) B;
- d) D.

12) С точки зрения ГТК основной задачей средств безопасности является обеспечение:

- a) сохранности информации;
- b) защиты от НСД;
- c) простоты реализации;
- d) надёжности функционирования.

13) Согласно «Оранжевой книге» дискреционную защиту имеет группа критериев:

- a) D;
- b) A;
- c) B;
- d) C.

14) При качественном подходе риск измеряется в терминах:

- a) денежных потерь;
- b) заданных с помощью шкалы ранжирования;
- c) оценок экспертов;
- d) объёма информации.

15) Согласно «Европейским критериям» формальное описание функций безопасности требуется на уровне:

- a) E5;
- b) E7;
- c) E4;
- d) E6.

4.3 Промежуточная аттестация по дисциплине проводится в форме зачета

Типовые вопросы зачета (ПК-1)

1. Теория защиты информации. Основные направления
2. Виды угроз. Основные нарушения.
3. Общая модель воздействия на информацию.
4. Общая модель процесса нарушения физической целостности информации.
5. Методы определения требований к защите информации.
6. Допущения в моделях оценки уязвимости информации.
7. Классификация требований к средствам защиты информации.
8. Способы и средства защиты информации.
9. Способы «абсолютной системы защиты».

Типовые задания для зачета (ПК-1)

1. Содержание интересов личности, общества и государства в информационной сфере.
2. Источники и содержание угроз в информационной сфере.

3. Классы информационных ресурсов.
4. Общая схема обеспечения информационной безопасности
5. Ретроспективный анализ развития подходов к защите информации.
6. Сущность и содержание эмпирического, концептуально-эмпирического теоретико-концептуального подходов к защите информации

4.4. Шкала оценивания промежуточной аттестации

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
«зачтено» (50 - 100 баллов)	ПК-1	Демонстрирует достаточный уровень знаний в области основ информационной безопасности.¶Анализирует существующие методики определений требования к защите информации.¶Демонстрирует знание принципов обеспечения защиты информации и источников угроз ИБ.¶Способен продемонстрировать современные подходы к технологиям и методам обеспечения ИБ.¶
«не зачтено» (0 - 49 баллов)	ПК-1	Не имеет знаний в области основ информационной безопасности.¶Не анализирует существующие методики определений требования к защите информации.¶Не способен продемонстрировать знания принципов обеспечения защиты информации и источников угроз ИБ.¶

5. Методические указания для обучающихся по освоению дисциплины (модуля)

5.1 Методические указания по организации самостоятельной работы обучающихся:

Приступая к изучению дисциплины, в первую очередь обучающимся необходимо ознакомиться содержанием рабочей программы дисциплины (РПД), которая определяет содержание, объем, а также порядок изучения и преподавания учебной дисциплины, ее раздела, части.

Для самостоятельной работы важное значение имеют разделы «Объем и содержание дисциплины», «Учебно-методическое и информационное обеспечение дисциплины» и «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы».

В разделе «Объем и содержание дисциплины» указываются все разделы и темы изучаемой дисциплины, а также виды занятий и планируемый объем в академических часах.

В разделе «Учебно-методическое и информационное обеспечение дисциплины» указана рекомендуемая основная и дополнительная литература.

В разделе «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы» содержится перечень профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины.

5.2 Рекомендации обучающимся по работе с теоретическими материалами по дисциплине

При изучении и проработке теоретического материала необходимо:

- просмотреть еще раз презентацию лекции в системе MOODLe, повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной дополнительной литературы;
- при самостоятельном изучении теоретической темы сделать конспект, используя рекомендованные в РПД источники, профессиональные базы данных и информационные справочные системы;
- ответить на вопросы для самостоятельной работы, по теме представленные в пункте 3.2 РПД.
- при подготовке к текущему контролю использовать материалы фонда оценочных средств (ФОС).

5.3 Рекомендации по работе с научной и учебной литературой

Работа с основной и дополнительной литературой является главной формой самостоятельной работы и необходима при подготовке к устному опросу на семинарских занятиях, к дебатам, тестированию, экзамену. Она включает проработку лекционного материала и рекомендованных источников и литературы по тематике лекций.

Конспект лекции должен содержать реферативную запись основных вопросов лекции, в том числе с опорой на размещенные в системе MOODLe презентации, основных источников и литературы по темам, выводы по каждому вопросу. Конспект может быть выполнен в рамках распечатки выдачи презентаций лекций или в отдельной тетради по предмету. Он должен быть аккуратным, хорошо читаемым, не содержать не относящуюся к теме информацию или рисунки.

Конспекты научной литературы при самостоятельной подготовке к занятиям должны содержать ответы на каждый поставленный в теме вопрос, иметь ссылку на источник информации с обязательным указанием автора, названия и года издания используемой научной литературы. Конспект может быть опорным (содержать лишь основные ключевые позиции), но при этом позволяющим дать полный ответ по вопросу, может быть подробным. Объем конспекта определяется самим студентом.

В процессе работы с основной и дополнительной литературой студент может:

- делать записи по ходу чтения в виде простого или развернутого плана (создавать перечень основных вопросов, рассмотренных в источнике);
- составлять тезисы (цитирование наиболее важных мест статьи или монографии, короткое изложение основных мыслей автора);
- готовить аннотации (краткое обобщение основных вопросов работы);
- создавать конспекты (развернутые тезисы).

5.4. Рекомендации по подготовке к отдельным заданиям текущего контроля

Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.

Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:

- правильность ответа по содержанию;
- полнота и глубина ответа;
- сознательность ответа;
- логика изложения материала;
- рациональность использованных приемов и способов решения поставленной учебной задачи;
- своевременность и эффективность использования наглядных пособий и технических средств при ответе;
- использование дополнительного материала;
- рациональность использования времени, отведенного на задание.

Устный опрос может сопровождаться презентацией, которая подготавливается по одному из вопросов практического занятия. При выступлении с презентацией необходимо обращать внимание на такие моменты как:

- содержание презентации: актуальность темы, полнота ее раскрытия, смысловое содержание, соответствие заявленной темы содержанию, соответствие методическим требованиям (цели, ссылки на ресурсы, соответствие содержания и литературы), практическая направленность, соответствие содержания заявленной форме, адекватность использования технических средств учебным задачам, последовательность и логичность презентуемого материала;
- оформление презентации: объем (оптимальное количество), дизайн (читаемость, наличие и соответствие графики и анимации, звуковое оформление, структурирование информации, соответствие заявленным требованиям), оригинальность оформления, эстетика, использование возможности программной среды, соответствие стандартам оформления;
- личностные качества: ораторские способности, соблюдение регламента, эмоциональность, умение ответить на вопросы, систематизированные, глубокие и полные знания по всем разделам программы;

- содержание выступления: логичность изложения материала, раскрытие темы, доступность изложения, эффективность применения средств ИКТ, способы и условия достижения результативности и эффективности для выполнения задач своей профессиональной или учебной деятельности, доказательность принимаемых решений, умение аргументировать свои заключения, выводы.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература:

1. Передков В.М., Митрошкин А.Г. Информационная безопасность и защита информации. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)
2. Лопатин Д.В., Калинина Ю.В. Безопасные информационные технологии : электрон. учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)
3. Тамб гос. ун-т им. Г.Р. Державина, Ин-т математики, физики и информатики Техническая защита информации : учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)

6.2 Дополнительная литература:

1. Загинайлов Ю. Н. Основы информационной безопасности: курс визуальных лекций : учебное пособие. - Москва|Берлин: Директ-Медиа, 2015. - 105 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=362895>
2. Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие. - Москва|Берлин: Директ-Медиа, 2015. - 253 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=276557>
3. Аверченков В. И., Рытов М. Ю., Кувыклин А. В., Рудановский М. В. Аудит информационной безопасности органов исполнительной власти : учебное пособие. - 4-е изд., стер.. - Москва: Флинта, 2016. - 100 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=93259>
4. Комплексное обеспечение информационной безопасности автоматизированных систем : лабораторный практикум. - Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2016. - 242 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=458012>
5. Петренко В. И. Теоретические основы защиты информации : учебное пособие. - Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2015. - 222 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=458204>

6.3 Иные источники:

1. Курс «Стандарты информационной безопасности» - <https://www.intuit.ru/studies/courses/30/30/info>
2. Курс «Основы информационной безопасности» - <https://www.intuit.ru/studies/courses/10/10/info>

7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы

Для проведения занятий по дисциплине необходимо следующее материально-техническое обеспечение: учебные аудитории для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы.

Учебные аудитории и помещения для самостоятельной работы укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы укомплектованы компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета.

Для проведения занятий лекционного типа используются наборы демонстрационного оборудования, обеспечивающие тематические иллюстрации (проектор, ноутбук, экран/ интерактивная доска).

Лицензионное и свободно распространяемое программное обеспечение:

Microsoft Windows 10

Google Chrome

Microsoft Office Профессиональный плюс 2007

Профессиональные базы данных и информационные справочные системы:

1. Электронный каталог Фундаментальной библиотеки ТГУ. – URL: <http://biblio.tsutmb.ru/elektronnyij-katalog>
2. Университетская библиотека онлайн: электронно-библиотечная система. – URL: <https://biblioclub.ru>
3. Консультант студента. Гуманитарные науки: электронно-библиотечная система. – URL: <https://www.studentlibrary.ru>
4. Научная электронная библиотека eLIBRARY.ru. – URL: <https://elibrary.ru>
5. Научная электронная библиотека Российской академии естествознания. – URL: <https://www.monographies.ru>
6. Российская государственная библиотека. – URL: <https://www.rsl.ru>
7. Российская национальная библиотека. – URL: <http://nlr.ru>
8. Президентская библиотека имени Б.Н. Ельцина. – URL: <https://www.prilib.ru>
9. Электронная библиотека РФФИ. – URL: <https://www.rfbr.ru/rffi/ru/library>

Электронная информационно-образовательная среда

https://auth.tsutmb.ru/authorize?response_type=code&client_id=moodle&state=xyz

Взаимодействие преподавателя и студента в процессе обучения осуществляется посредством мультимедийных, гипертекстовых, сетевых, телекоммуникационных технологий, используемых в электронной информационно-образовательной среде университета.