

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 защиты информации

Направление подготовки/специальность: 10.03.01 - Информационная безопасность

Профиль/направленность/специализация: Безопасность компьютерных систем

Уровень высшего образования: бакалавриат

Квалификация: Бакалавр

год набора: 2021

**Автор программы:**

Минаев Дмитрий Сергеевич

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.03.01 - Информационная безопасность (уровень бакалавриата) (приказ Министерства образования и науки РФ от «17» ноября 2020 г. № 1427).

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 бакалавра.....	5
3. Объем и содержание дисциплины.....	5
4. Контроль знаний обучающихся и типовые оценочные средства.....	14
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	23
6. Учебно-методическое и информационное обеспечение дисциплины.....	25
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	26

## 1. Цели и задачи дисциплины

### 1.1 Цель дисциплины – формирование компетенций:

ПК-3 Способен администрировать средства защиты информации прикладного и системного программного обеспечения

### 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 сфере: 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)

### 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-3 Способен администрировать средства защиты информации прикладного и системного программного обеспечения	На основе современных технологий обеспечений информационной безопасности администрирует средства защиты информации прикладного и системного программного обеспечения для обеспечения безопасности программ и данных

### 1.5 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ПК-3 Способен администрировать средства защиты информации прикладного и системного программного обеспечения

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения			
		Очная (семестр)			
		2	6	7	8
1	Защита программ и данных			+	
2	Избранные вопросы информационной безопасности		+	+	
3	Преддипломная практика				+
4	Современные технологии обеспечения информационной безопасности	+			
5	Теоретические основы защиты информации на английском языке	+			

## 2. Место дисциплины в структуре ОП бакалавриата:

Дисциплина «Теоретические основы защиты информации» относится к части, формируемой участниками образовательных отношений, учебного плана ОП по направлению подготовки 10.03.01 - Информационная безопасность.

Дисциплина «Теоретические основы защиты информации» 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)
<b>Общая трудоёмкость дисциплины</b>	<b>72</b>
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	6	4	Тестирование
3	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности.	2	4	3	Собеседование
4	Угрозы информационной безопасности.	3	5	4	Тестирование
5	Политика и модели безопасности.	2	4	3	Тестирование

6	Информационные войны и информационное противоборство.	3	5	4	Выполнение практических заданий
7	Обзор международных стандартов информационной безопасности.	2	4	3	Выполнение практических заданий

## **Тема 1. Основные понятия теории информационной безопасности. (ПК-3)**

### **Лекция.**

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

### **Лабораторные работы.**

#### **1. Информация:**

- а) информация, полученная из СМИ;
- б) только документированные сведения о лицах, предметах, фактах, событиях;
- в) сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;
- г) только информация, содержащаяся в электронных базах данных.

#### **2. Информация**

- а) не исчезает при употреблении;
- б) становится доступной, если она содержится на материальном носителе;
- в) подлежит только «моральному износу»;
- г) характеризуется всеми перечисленными свойствами.

3. Информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать, называется:

- а) надежный;
- б) конфиденциальный;
- в) документированные;
- г) коммерческая тайна.

#### **4. Информационно-телекоммуникационная сеть – это:**

- а) технологическая система, предназначенная для передачи информации по линиям связи, доступ к которой осуществляется с использованием вычислительной техники;
- б) технологическая система, предназначенная для передачи по сети Интернет, доступ к которой осуществляется с использованием компьютерных технологий;
- в) технологическая система, предназначенная для передачи информации по локальной сети, доступ к которой осуществляется с помощью компьютерной техники.

#### **5. Доступ к информации:**

- а) возможность получения информации;
- б) возможность получения информации и ее использования;
- в) возможность получения информации и ее распространения.

#### **6. Предоставление информации – это действие, направленное на:**

- а) получать информацию от определенного круга лиц;
- б) получать информацию руководителем и передавать информацию определенному кругу лиц;
- в) получать информацию от определенного круга лиц или передавать информацию определенному кругу лиц.

7. Информационная безопасность – это:

- а) защита информации и обеспечивающей инфраструктуры от случайных или преднамеренных воздействий природного или случайного характера, которые могут причинить неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и обеспечивающей инфраструктуры;
- б) защищенность программных продуктов компании от случайных или преднамеренных воздействий естественного или случайного характера;
- в) защищенность информации, циркулирующей в сети, от случайных или преднамеренных воздействий естественного или случайного характера.

8. Информационная безопасность – это защита информации:

- а) от разглашения, искажения, утраты;
- б) от разглашения, искажения, утраты или снижения степени доступности информации, а равно ее незаконного тиражирования;
- в) от передачи третьим лицам, искажения и незаконного использования.

9. Угроза – это:

- а) возможность нарушения информационной безопасности определенным образом;
- б) система программно-языковых организационно-технических средств, предназначенных для накопления и коллективного использования данных;
- в) процесс определения соответствует текущему состоянию разработки требованиям данного этапа.

10. Эффективная защита информации возможна:

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

### **Задания для самостоятельной работы.**

Показать связь между уровнем развития общества и технологиями защиты информации.

В каких направлениях в настоящее время развивается теория информационной безопасности?

Каков вклад российских ученых в теорию информационной безопасности?

С чем связан повышенный интерес к проблемам информационной безопасности?

В чем отличия формального и неформального подходов к проблемам информационной безопасности?

В чем, на ваш взгляд, основные трудности

обеспечения информационной безопасности в настоящее время?

Что такое информационная система? Телекоммуникационная система? Автоматизированная система?

Какие существуют правовые концепции в области защиты информации?

Что такое защита информации? Информационная безопасность?

Дайте характеристику понятиям, связанным с организацией защиты информации.

Каковы основные принципы построения систем защиты информации?

Что такое комплексный подход к информационной безопасности?

Каковы основные задачи защиты информации?

Докажите, что приведенный выше набор функций защиты является полным.

Какова взаимосвязь между различными средствами защиты информации? Есть ли среди них приоритетные?

Каковы основные средства реализации комплексной системы защиты информации?

Каковы морально-этические средства защиты информации?

Доказать 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 информационной безопасности?

## **Тема 2. Информация как объект защиты. (ПК-3)**

### **Лекция.**

Понятие информации как объекта защиты. Уровни представления информации. Основные свойства защищаемой информации. Виды и формы подачи 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 (библиотеки, архивы, фонды, банки данных, депозитарии, музейные фондохранилища и др.):
  - а) информационные ресурсы;
  - б) информационные продукты;
  - в) информационные перспективы.
2. Информационные ресурсы являются одним из видов социально-экономических ресурсов:
  - а) деловые факторы;
  - б) факторы производства;
  - в) факторы активности.
3. Уровень развития сферы информационных услуг во многом определяет степень близости к такому обществу:
  - а) информация;
  - б) открытый;
  - в) закрытый.
4. Документооборот – это:
  - а) движение документов в организации с момента их создания или поступления до завершения исполнения или отправки; +
  - б) вид государственной, муниципальной, научной, коммерческой и некоммерческой деятельности;
  - в) это система стандартов для информации, библиотеки и издательского дела.
5. Аутентификация это:
  - а) механизм разграничения доступа к данным и функциям системы;
  - б) возможность проверки личности пользователя; +
  - в) поиск и исследование математических методов преобразования информации.
6. В информационных системах документированная информация представляется в виде:
  - а) файлы, папки, массивы, базы данных, программы;
  - б) базы данных и программное обеспечение;
  - в) файлы и базы данных.
7. Информационные ресурсы могут быть:
  - а) открытый, закрытый;
  - б) открытый и ограниченный доступ;
  - в) ограниченный доступ.
8. Устанавливается режим защиты информации:
  - а) в отношении сведений, отнесенных к государственной тайне;
  - б) в отношении конфиденциальной информации;
  - в) в отношении сведений, составляющих государственную тайну, и персональных данных.
9. Что подлежит обязательной сертификации:
  - а) автоматизированные системы органов государственной власти, обрабатывающие документированную информацию с ограниченным доступом, а также средства защиты этих систем;
  - б) автоматизированные системы органов местного самоуправления, обрабатывающие документированную информацию с ограниченным доступом, а также средства защиты этих систем;



в) автоматизированные системы, обрабатывающие сведения, составляющие государственную тайну.

#### **Задания для самостоятельной работы.**

1. Что такое информация и каковы уровни ее представления?
2. Перечислите основные носители, особенности их использования и защиты.
3. Какие свойства определяют 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 допускается относить к информации с ограниченным доступом?
8. Какие есть секреты?

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

#### **Лекция.**

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

#### **Лабораторные работы.**

1. Каковы функции руководителей предприятий в 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 Российской Федерации?
6. Кто несет ответственность 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. Сформулировать основные положения Доктрины информационной безопасности Российской Федерации.
3. Каковы основные задачи защиты информации?
4. Какова структура государственной системы защиты информации?
5. Кто несет ответственность за нарушение режима защиты данных?
6. Показать роль различных министерств и ведомств в защите информации.

### **Тема 4. Угрозы информационной безопасности. (ПК-3)**

#### **Лекция.**

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

#### **Лабораторные работы.**

1. При проектировании системы защиты необходимо:
  - а) определение перечня угроз и построение модели нарушителя;
  - б) определение программно-аппаратных средств защиты информации;
  - в) выявление сертифицированных средств защиты и построение модели нарушителя.
2. Анализ уязвимостей является обязательной процедурой...
  - а) при анализе средств защиты информации;
  - б) при сертификации объекта информатизации;
  - в) при определении модели нарушителя.
3. Природные угрозы информационной безопасности вызываются:

- а) деятельность человека;
- б) ошибки при проектировании АСОИ, ее элементов или разработке программного обеспечения;
- в) последствия объективных физических процессов или явлений природы, не зависящих от человека;
- г) корыстные устремления злоумышленников;
- д) ошибки в действиях персонала.

4. Искусственные угрозы информационной безопасности, вызванные:

- а) деятельность человека;
- б) ошибки при проектировании АСОИ, ее элементов или разработке программного обеспечения;
- в) последствия объективных физических процессов или явлений природы, не зависящих от человека;
- г) корыстные устремления злоумышленников;
- д) ошибки в действиях персонала.

5. К основным непреднамеренным искусственным угрозам АСОИ относятся:

- а) физическое разрушение системы взрывом, поджогом и т.п.;
- б) перехват боковых электромагнитных, акустических и других средств излучения и линий связи;
- в) изменение режимов работы устройств или программ, забастовка, саботаж персонала, установка мощных активных помех и т. п.;
- г) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
- д) непреднамеренные действия, приводящие к частичному или полному отказу системы или уничтожению аппаратных, программных, информационных ресурсов системы.

6. К посторонним, нарушающим информационную безопасность, относятся:

- а) представителей организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
- б) обслуживающий персонал технического оборудования;
- в) технический персонал, обслуживающий здание;
- г) пользователи;
- д) сотрудники службы безопасности.
- е) представители конкурирующих организаций.
- ж) лица, нарушившие пропускной режим;

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

- а) сотрудники;
- б) хакеры;
- в) злоумышленники;
- г) подрядчики (лица, работающие по договору).

8. Кто в конечном итоге несет ответственность за обеспечение секретности и защиты данных?

- а) владельцы данных;
- б) пользователи;
- в) администраторы;
- г) руководство.

### **Задания для самостоятельной работы.**

1. На примере нескольких различных угроз показать, что их реализация приведет к изменению одного из основных свойств защищаемой информации (конфиденциальность, целостность, доступность).
2. Приведите примеры систем, для которых наибольшую угрозу безопасности представляет нарушение конфиденциальности информации.
3. Для каких систем (приведите примеры) наиболее опасно нарушение целостности информации?
4. В каких системах доступность информации стоит на первом месте?

5. Чем отличаются понятия «нарушение конфиденциальности информации», «несанкционированный доступ к информации», «утечка информации»?
6. Определить перечень основных угроз для АС, состоящей из автономного компьютера без доступа к сети, расположенного в одной из лабораторий вуза.

### **Тема 5. Политика и модели безопасности. (ПК-3)**

#### **Лекция.**

Политика безопасности. Субъектно-объектные модели разграничения доступа. Аксиомы политики безопасности. Политики и модели дискреционного доступа. Системы контроля доступа по паролю. Политика и модели обязательного доступа. Информационно-теоретические модели. Политики и модели тематического разграничения доступа. Ролевая модель безопасности.

#### **Лабораторные работы.**

- 1) При авторизованной политике безопасности формируется набор меток с одинаковыми значениями:
  - а) область равной критичности;
  - б) зона равного доступа;
  - в) уровень безопасности;
  - г) Уровень доступности.
- 2) Степень защищенности информации от негативного воздействия на нее в части нарушения ее физической и логической целостности или несанкционированного использования составляет:
  - а) уязвимость информации;
  - б) достоверность информации;
  - в) информационная безопасность;
  - г) информационная безопасность.
- 3) Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы:
  - а) авторизация;
  - б) аудит;
  - в) идентификация;
  - г) аутентификация.
- 4) Используя информацию о секретном ключе:
  - а) скопировано;
  - б) трансляция;
  - в) обозначает;
  - г) в зашифрованном виде.
- 5) Совокупность свойств, определяющих пригодность информации для удовлетворения определенных потребностей в соответствии с ее назначением, называется:
  - а) актуальность информации;
  - б) доступность;
  - в) качество информации;
  - г) целостность.
- 6) Недостатком модели конечного состояния политики безопасности является:
  - а) изменение линии связи;
  - б) статический;
  - в) сложность реализации;
  - г) низкая степень надежности.
- 7) Способ контроля доступа, при котором каждому объекту системы присваивается метка критичности, определяющая ценность информации, называется:
  - а) идентифицируемый;
  - б) обязательный;

- в) избирательный;
  - г) привилегированный.
- 8) Организационные требования к системе защиты:
- а) управление и идентификация;
  - б) административно-аппаратные;
  - с) административно-процессуальные;
  - г) аппаратные и физические.
- 9) Основой политики безопасности является:
- а) программное обеспечение;
  - б) управление рисками;
  - с) метод управления доступом;
  - г) выбор канала связи.
- 10) Наукой, изучающей математические методы защиты информации путем ее преобразования, является:
- а) криптография;
  - б) стенография;
  - в) криптоанализ;
  - г) криптология.
- 11) Согласно Оранжевой книге минимальную защиту имеет группа критериев:
- а) С;
  - б) А;
  - в) Б;
  - г) Д.
- 12) С точки зрения ГТК основной задачей средств безопасности является обеспечение:
- а) сохранность информации;
  - б) защита от НСД;
  - в) простота реализации;
  - г) надежность работы.
- 13) Согласно Оранжевой книге группа критериев имеет дискреционную защиту:
- а) Д;
  - б) А;
  - в) Б;
- Округ Колумбия.
- 14) При качественном подходе риск измеряется с точки зрения:
- а) денежные потери;
  - б) установить с помощью рейтинговой шкалы;
  - с) экспертные оценки;
  - г) количество информации.
- 15) Согласно «Европейским критериям» требуется формальное описание функций безопасности на уровне:
- а) E5;
  - б) E7;
  - в) E4;
  - г) 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 для самостоятельного изучения, выданным преподавателем на занятиях;

## **Тема 6. Информационные войны и информационное противоборство. (ПК-3)**

### **Лекция.**

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

### **Лабораторные работы.**

Практическая задача.

Цель работы:

1. Закрепить знания нормативно-правовой базы Российской Федерации по вопросам информационного противоборства.
2. Закрепить понятия: информационные операции, психологические операции, оперативная маскировка, радиоэлектронная борьба.

Задачи:

Вариант №1.

1. Каковы социальные и личностные предпосылки возникновения информационных операций и войн?
2. Каковы особенности стратегического планирования в информационных войнах?
3. Охарактеризуйте основные стратегии информационных войн.
4. Охарактеризуйте стратегии, используемые оппозицией для свержения власти в процессе «цветных» революций.
5. Гуманитарные аспекты информационного оружия и проиллюстрируйте их реальными примерами из своей жизни или из жизни современного общества.

Вариант №2.

1. Истинные цели и причины применения информационного оружия.
2. Средства и методы информационно-психологической борьбы.
3. Виды угроз безопасности личности, общества и государства в условиях информационно-психологического противоборства.
4. Источники угроз безопасности личности, общества и государства в условиях информационно-психологического противоборства.
5. Охарактеризуйте особенности оперативного реагирования на внезапно выявленные действия (события) 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 для самостоятельного изучения, выданным преподавателем на занятиях;

## **Тема 7. Обзор международных стандартов информационной безопасности. (ПК-3)**

### **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 в США. Единые критерии безопасности информационных технологий. Группа международных стандартов 270000.

### **Лабораторные работы.**

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

При выполнении задания необходимо проанализировать содержание следующих основных международных норм безопасности:

1. Международный стандарт менеджмента информационной безопасности ISO 17799.

1. Общие критерии безопасности информационных технологий ГОСТ ИСО/МЭК 15408.
  2. Критерии оценки надежности компьютерных систем («Оранжевая книга»).
  3. Канадские критерии и общие критерии.
  4. Стандарт COBIT («Объекты управления информационными и смежными технологиями»).
- Необходимо сравнить эти стандарты с российской нормативно-правовой 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 для самостоятельного изучения, выданным преподавателем на занятиях.

#### **4. Контроль знаний обучающихся и типовые оценочные средства**

##### **4.1. Распределение баллов:**

##### **2 семестр**

- посещаемость – 15 баллов
- текущий контроль – 65 баллов
- контрольные срезы – 2 среза по 10 баллов каждый
- премиальные баллы – 20 баллов

##### **Распределение баллов по заданиям:**

№ темы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Макс. кол-во баллов	Методика проведения занятия и оценки
1.	Основные понятия теории информационной безопасности.	Тестирование	10	Тест состоит из вопросов с выбором ответа. 10 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	15	Тест состоит из вопросов с выбором ответа. 15 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.	<b>Собеседование(контрольный срез)</b>	10	<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"> <li>- правильность ответа по содержанию;</li> <li>- полнота и глубина ответа;</li> <li>- сознательность ответа;</li> <li>- логика изложения материала;</li> <li>- рациональность использованных приемов и способов решения поставленной учебной задачи;</li> <li>- своевременность и эффективность использования наглядных пособий и технических средств при ответе;</li> <li>- использование дополнительного материала;</li> <li>- рациональность использования времени, отведенного на задание.</li> </ul> <p>10 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	15	<p>Тест состоит из вопросов с выбором ответа.</p> <p>15 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.	Политика и модели безопасности.	<b>Тестирование(контрольный срез)</b>	10	<p>Тест состоит из вопросов с выбором ответа.</p> <p>10 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.	Информационные войны и информационное противоборство.	Выполнение практических заданий	15	Лабораторные работы выполняются по тематике практических занятий. 15 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию 5 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы 2 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
7.	Обзор международных стандартов информационной безопасности.	Выполнение практических заданий	10	Лабораторные работы выполняются по тематике практических занятий. 10 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию 5 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы 2 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
8.	Посещаемость		15	15 баллов – стопроцентное посещение занятий студентом 7 баллов – посещаемость студента составляет не менее 80 % занятий 5 баллов – посещаемость студента составляет не менее 50 % занятий 3 балла – посещаемость студента составляет не менее 25 % занятий
9.	Премиальные баллы		20	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
10.	Индивидуальные задания, с помощью которых можно набрать дополнительные баллы		40	Решение кейса (10 баллов) Прохождение тестирования (30 вопросов) по всему курсу дисциплины (40 баллов)
11.	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 6. Информационные войны и информационное противоборство.

Практическая задача.

Цель работы:

1. Закрепить знания нормативно-правовой базы Российской Федерации по вопросам информационного противоборства.
2. Закрепить понятия: информационные операции, психологические операции, оперативная маскировка, радиоэлектронная борьба.

Задачи:

Вариант №1.

1. Каковы социальные и личностные предпосылки возникновения информационных операций и войн?
2. Каковы особенности стратегического планирования в информационных войнах?
3. Охарактеризуйте основные стратегии информационных войн.
4. Охарактеризуйте стратегии, используемые оппозицией для свержения власти в процессе «цветных» революций.
5. Гуманитарные аспекты информационного оружия и проиллюстрируйте их реальными примерами из своей жизни или из жизни современного общества.

Вариант №2.

1. Истинные цели и причины применения информационного оружия.
2. Средства и методы информационно-психологической борьбы.
3. Виды угроз безопасности личности, общества и государства в условиях информационно-психологического противоборства.
4. Источники угроз безопасности личности, общества и государства в условиях информационно-психологического противоборства.
5. Охарактеризуйте особенности оперативного реагирования на внезапно выявленные действия (события) информационно-психологической агрессии (войны).

#### Тема 7. Обзор международных стандартов информационной безопасности.

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

При выполнении задания необходимо проанализировать содержание следующих основных международных норм безопасности:

1. Международный стандарт менеджмента информационной безопасности ISO 17799.
1. Общие критерии безопасности информационных технологий ГОСТ ИСО/МЭК 15408.
2. Критерии оценки надежности компьютерных систем («Оранжевая книга»).
3. Канадские критерии и общие критерии.
4. Стандарт COBIT («Объекты управления информационными и смежными технологиями»).

Необходимо сравнить эти стандарты с российской нормативно-правовой базой в области информационной безопасности и оценить их применимость в России.

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

1. Каковы функции руководителей предприятий в 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 Российской Федерации?
6. Кто несет ответственность за использование несертифицированных средств защиты информации в автоматизированных системах?

### Тестирование

#### Тема 1. Основные понятия теории информационной безопасности.

1. Информация:
  - а) информация, полученная из СМИ;
  - б) только документированные сведения о лицах, предметах, фактах, событиях;
  - в) сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;
  - г) только информация, содержащаяся в электронных базах данных.
2. Информация
  - а) не исчезает при употреблении;
  - б) становится доступной, если она содержится на материальном носителе;
  - в) подлежит только «моральному износу»;
  - г) характеризуется всеми перечисленными свойствами.
3. Информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать, называется:
  - а) надежный;
  - б) конфиденциальный;
  - в) документированные;
  - г) коммерческая тайна.
4. Информационно-телекоммуникационная сеть – это:
  - а) технологическая система, предназначенная для передачи информации по линиям связи, доступ к которой осуществляется с использованием вычислительной техники;
  - б) технологическая система, предназначенная для передачи по сети Интернет, доступ к которой осуществляется с использованием компьютерных технологий;
  - в) технологическая система, предназначенная для передачи информации по локальной сети, доступ к которой осуществляется с помощью компьютерной техники.
5. Доступ к информации:
  - а) возможность получения информации;
  - б) возможность получения информации и ее использования;
  - в) возможность получения информации и ее распространения.
6. Предоставление информации – это действие, направленное на:
  - а) получать информацию от определенного круга лиц;
  - б) получать информацию руководителем и передавать информацию определенному кругу лиц;
  - в) получать информацию от определенного круга лиц или передавать информацию определенному кругу лиц.
7. Информационная безопасность – это:

а) защита информации и обеспечивающей инфраструктуры от случайных или преднамеренных воздействий природного или случайного характера, которые могут причинить неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и обеспечивающей инфраструктуры;

б) защищенность программных продуктов компании от случайных или преднамеренных воздействий естественного или случайного характера;

в) защищенность информации, циркулирующей в сети, от случайных или преднамеренных воздействий естественного или случайного характера.

8. Информационная безопасность – это защита информации:

а) от разглашения, искажения, утраты;

б) от разглашения, искажения, утраты или снижения степени доступности информации, а равно ее незаконного тиражирования;

в) от передачи третьим лицам, искажения и незаконного использования.

9. Угроза – это:

а) возможность нарушения информационной безопасности определенным образом;

б) система программно-языковых организационно-технических средств, предназначенных для накопления и коллективного использования данных;

в) процесс определения соответствует текущему состоянию разработки требованиям данного этапа.

10. Эффективная защита информации возможна:

а) только на основе комплексного использования всех известных методов и подходов к решению данной проблемы;

г) только при использовании сертифицированных средств защиты информации;

д) только при использовании технических средств защиты информации;

е) Все ответы правильные.

## Тема 2. Информация как объект защиты.

1. Документы и массивы документов в информационных системах (библиотеки, архивы, фонды, банки данных, депозитарии, музейные фондохранилища и др.):

а) информационные ресурсы;

б) информационные продукты;

в) информационные перспективы.

2. Информационные ресурсы являются одним из видов социально-экономических ресурсов:

а) деловые факторы;

б) факторы производства;

в) факторы активности.

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

а) информация;

б) открытый;

в) закрытый.

4. Документооборот – это:

а) движение документов в организации с момента их создания или поступления до завершения исполнения или отправки; +

б) вид государственной, муниципальной, научной, коммерческой и некоммерческой деятельности;

в) это система стандартов для информации, библиотеки и издательского дела.

5. Аутентификация это:

а) механизм разграничения доступа к данным и функциям системы;

б) возможность проверки личности пользователя; +

в) поиск и исследование математических методов преобразования информации.

6. В информационных системах документированная информация представляется в виде:

а) файлы, папки, массивы, базы данных, программы;

б) базы данных и программное обеспечение;

в) файлы и базы данных.

7. Информационные ресурсы могут быть:

а) открытый, закрытый;

б) открытый и ограниченный доступ;

в) ограниченный доступ.

8. Устанавливается режим защиты информации:

а) в отношении сведений, отнесенных к государственной тайне;

б) в отношении конфиденциальной информации;

в) в отношении сведений, составляющих государственную тайну, и персональных данных.

9. Что подлежит обязательной сертификации:

а) автоматизированные системы органов государственной власти, обрабатывающие

документированную информацию с ограниченным доступом, а также средства защиты этих систем;

б) автоматизированные системы органов местного самоуправления, обрабатывающие

документированную информацию с ограниченным доступом, а также средства защиты этих систем;

в) автоматизированные системы, обрабатывающие сведения, составляющие государственную тайну.

#### Тема 4. Угрозы информационной безопасности.

1. При проектировании системы защиты необходимо:

а) определение перечня угроз и построение модели нарушителя;

б) определение программно-аппаратных средств защиты информации;

в) выявление сертифицированных средств защиты и построение модели нарушителя.

2. Анализ уязвимостей является обязательной процедурой... .

. а) при анализе средств защиты информации;

б) при сертификации объекта информатизации;

в) при определении модели нарушителя.

3. Природные угрозы информационной безопасности вызываются:

а) деятельность человека;

б) ошибки при проектировании АСОИ, ее элементов или разработке программного обеспечения;

в) последствия объективных физических процессов или явлений природы, не зависящих от человека;

г) корыстные устремления злоумышленников;

д) ошибки в действиях персонала.

4. Искусственные угрозы информационной безопасности, вызванные:

а) деятельность человека;

б) ошибки при проектировании АСОИ, ее элементов или разработке программного обеспечения;

в) последствия объективных физических процессов или явлений природы, не зависящих от человека;

г) корыстные устремления злоумышленников;

д) ошибки в действиях персонала.

5. К основным непреднамеренным искусственным угрозам АСОИ относятся:

а) физическое разрушение системы взрывом, поджогом и т.п.;

б) перехват боковых электромагнитных, акустических и других средств излучения и линий связи;

в) изменение режимов работы устройств или программ, забастовка, саботаж персонала, установка мощных активных помех и т. п.;

г) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

д) непреднамеренные действия, приводящие к частичному или полному отказу системы или уничтожению аппаратных, программных, информационных ресурсов системы.

6. К посторонним, нарушающим информационную безопасность, относятся:

- а) представителей организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
- б) обслуживающий персонал технического оборудования;
- в) технический персонал, обслуживающий здание;
- г) пользователи;
- д) сотрудники службы безопасности.
- е) представители конкурирующих организаций.
- ж) лица, нарушившие пропускной режим;

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

- а) сотрудники;
- б) хакеры;
- в) злоумышленники;
- г) подрядчики (лица, работающие по договору).

8. Кто в конечном итоге несет ответственность за обеспечение секретности и защиты данных?

- а) владельцы данных;
- б) пользователи;
- в) администраторы;
- г) руководство.

#### Тема 5. Политика и модели безопасности.

1) При авторизованной политике безопасности формируется набор меток с одинаковыми значениями:

- а) область равной критичности;
- б) зона равного доступа;
- в) уровень безопасности;
- г) Уровень доступности.

2) Степень защищенности информации от негативного воздействия на нее в части нарушения ее физической и логической целостности или несанкционированного использования составляет:

- а) уязвимость информации;
- б) достоверность информации;
- в) информационная безопасность;
- г) информационная безопасность.

3) Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы:

- а) авторизация;
- б) аудит;
- в) идентификация;
- г) аутентификация.

4) Используя информацию о секретном ключе:

- а) скопировано;
- б) трансляция;
- в) обозначает;
- г) в зашифрованном виде.

5) Совокупность свойств, определяющих пригодность информации для удовлетворения определенных потребностей в соответствии с ее назначением, называется:

- а) актуальность информации;
- б) доступность;

- в) качество информации;
  - г) целостность.
- 6) Недостатком модели конечного состояния политики безопасности является:
- а) изменение линии связи;
  - б) статический;
  - в) сложность реализации;
  - г) низкая степень надежности.
- 7) Способ контроля доступа, при котором каждому объекту системы присваивается метка критичности, определяющая ценность информации, называется:
- а) идентифицируемый;
  - б) обязательный;
  - в) избирательный;
  - г) привилегированный.
- 8) Организационные требования к системе защиты:
- а) управление и идентификация;
  - б) административно-аппаратные;
  - с) административно-процессуальные;
  - г) аппаратные и физические.
- 9) Основой политики безопасности является:
- а) программное обеспечение;
  - б) управление рисками;
  - с) метод управления доступом;
  - г) выбор канала связи.
- 10) Наукой, изучающей математические методы защиты информации путем ее преобразования, является:
- а) криптография;
  - б) стенография;
  - в) криптоанализ;
  - г) криптология.
- 11) Согласно Оранжевой книге минимальную защиту имеет группа критериев:
- а) С;
  - б) А;
  - в) Б;
  - г) Д.
- 12) С точки зрения ГТК основной задачей средств безопасности является обеспечение:
- а) сохранность информации;
  - б) защита от НСД;
  - в) простота реализации;
  - г) надежность работы.
- 13) Согласно Оранжевой книге группа критериев имеет дискреционную защиту:
- а) Д;
  - б) А;
  - в) Б;
- Округ Колумбия.
- 14) При качественном подходе риск измеряется с точки зрения:
- а) денежные потери;
  - б) установить с помощью рейтинговой шкалы;
  - с) экспертные оценки;
  - г) количество информации.

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

- а) Е5;
- б) Е7;
- в) Е4;
- г) Е6.

#### 4.3 Промежуточная аттестация по дисциплине проводится в форме зачета

##### Типовые вопросы зачета (ПК-3)

1. Теория информационной безопасности. Основные направления
2. Классификация требований к защите информации.
3. Общая модель воздействия на информацию.
4. Общая модель процесса нарушения физической целостности информации.
5. Методика определения требований к защите информации.
6. Допущения в моделях оценки информационной уязвимости.
7. Виды угроз. Основные нарушения.

##### Типовые задания для зачета (ПК-3)

1. Содержание интересов личности, общества и государства в информационной сфере.
2. Сущность и содержание эмпирических, концептуально-эмпирических теоретико-концептуальных подходов к обеспечению информационной безопасности.
3. Классы информационных ресурсов.
4. Общая схема обеспечения информационной безопасности
5. Ретроспективный анализ развития подходов к информационной безопасности.
6. Источники и содержание угроз в информационной сфере.

#### 4.4. Шкала оценивания промежуточной аттестации

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
«зачтено» (50 - 100 баллов)	ПК-3	Демонстрирует высокий уровень теоретических знаний методологического базиса решения задач защиты информации. Анализирует существующие методики определений требования к защите информации. Превосходно владеет знанием принципов обеспечения защиты информации. Способен продемонстрировать современные подходы к администрированию средств защиты информации прикладного и системного программного обеспечения.
«не зачтено» (0 - 49 баллов)	ПК-3	Не способен продемонстрировать знания методологического базиса решения задач защиты информации. Не анализирует существующие методики определений требования к защите информации. Не владеет знанием принципов обеспечения защиты информации. Не способен продемонстрировать современные подходы к администрированию средств защиты информации прикладного и системного программного обеспечения.

### 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. 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>
4. 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>

### **6.2 Дополнительная литература:**

1. 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>

2. 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>
3. Журнал «BIS Journal - Информационная безопасность банков» - <https://journal.ib-bank.ru/pub/169>

## 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

Yandex браузер

Kaspersky Endpoint Security 10 для Windows "Лаборатория Касперского" 26.07.2018

Профессиональные базы данных и информационные справочные системы:

1. Электронная библиотека РФФИ. – URL: <https://www.rfbr.ru/rffi/ru/library>
2. Российская государственная библиотека. – URL: <https://www.rsl.ru>
3. Электронный каталог Фундаментальной библиотеки ТГУ. – URL: <http://biblio.tsutmb.ru/elektronnyij-katalog>
4. Российская национальная библиотека. – URL: <http://nlr.ru>
5. Научная электронная библиотека eLIBRARY.ru. – URL: <https://elibrary.ru>
6. Научная электронная библиотека Российской академии естествознания. – URL: <https://www.monographies.ru>

### Электронная информационно-образовательная среда

[https://auth.tsutmb.ru/authorize?response\\_type=code&client\\_id=moodle&state=xyz](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.