Федеральное государственное образовательное бюджетное учреждение
высшего образования
**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»**
**(Финансовый университет)**

**Департамент информационной безопасности**

**Борисов С.А., Пальчевский Е.В.**

# Информационная безопасность

**Рабочая программа дисциплины**
для студентов, обучающихся по направлению подготовки
02.03.01 Математика и компьютерные науки,
образовательная программа «Математика и компьютерные науки»
(Компьютерные технологии анализа больших данных)

**Москва 2021**

Федеральное государственное образовательное бюджетное учреждение
высшего образования
**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»**
**(Финансовый университет)**

**Департамент информационной безопасности**

УТВЕРЖДАЮ

Проректор по учебной
и методической работе

_____ Е.А. Каменева

«29» 06 2021 г.

**Борисов С.А., Пальчевский Е.В.**

# Информационная безопасность

**Рабочая программа дисциплины**
для студентов, обучающихся по направлению подготовки
02.03.01 Математика и компьютерные науки,
профиль Компьютерные технологии анализа больших данных

*Рекомендовано Ученым советом*
*Факультета информационных технологий и анализа больших данных*
*(протокол №09 от 18.05.2021 г.)*

*Одобрено Советом учебно-научного*
*Департамента информационной безопасности*
*(протокол № 10 от 29.04.2021 г.)*

**Москва 2021**

**Рецензент:** М.В. Коротеев, д.э.н., доцент департамента анализа данных и машинного обучения Факультета информационных технологий и анализа больших данных.

**Борисов С.А., Пальчевский Е.В. «Информационная безопасность»**.
Рабочая программа дисциплины для студентов, обучающихся по направлению подготовки 02.03.01 Математика и компьютерные науки ОП «Математика и компьютерные науки» (Компьютерные технологии анализа больших данных) — М.: Финансовый университет при Правительстве Российской Федерации, Департамент информационной безопасности Факультета информационных технологий и анализа больших данных, 2021. – 39 с.

Дисциплина «**Информационная безопасность**» является обязательной дисциплиной общефакультетского (предпрофильного) цикла направления подготовки 02.03.01 Математика и компьютерные науки, профиль Компьютерные технологии анализа больших данных.

Рабочая программа дисциплины содержит цели и задачи дисциплины, требования к результатам освоения дисциплины, содержание дисциплины, тематику практических занятий и технологии их проведения, формы самостоятельной работы студентов, систему оценивания, учебно-методическое и информационное обеспечение дисциплины.

УДК 003.26.09 (73) ББК 16.84я73

**С.А. Борисов, Е.В. Пальчевский**

**Рабочая программа дисциплины**
Рабочая программа дисциплины «Информационная безопасность», для студентов, обучающихся по направлениям подготовки:
02.03.01 Математика и компьютерные науки ОП «Математика и компьютерные науки»
(Компьютерные технологии анализа больших данных)

Компьютерный набор, верстка: Годлевский П.П.
Формат 60x90/16. Гарнитура *TimesNewRoman*.
Усл. п.л. 1,6. Изд. №– 2021. Тираж экз.
Заказ _____

Отпечатано в Финансовом университете

# СОДЕРЖАНИЕ

**1. Наименование дисциплины**

«Информационная безопасность».

**2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине**

Дисциплина «Информационная безопасность» обеспечивает формирование следующих компетенций: ОПК-5.

Таблица 1

| Код компетенции | Наименование компетенции | Индикаторы достижения компетенции | Результаты обучения (умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции |
|---|---|---|---|
| ОПК-5 | Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий, в том числе отечественного производителя, и с учетом основных требований информационной безопасности | 1.Владеет знаниями и технологиями, необходимыми для прикладного и системного программирования, включая современные языки программирования, а также основными принципами и понятиями, применяемыми при построении компьютерных сетей. | **1. Знать:**<br>1.1. Основные проблемы и направления развития аппаратных и программных средств защиты информации, в том числе и высокоуровневые современные языки программирования, необходимые для прикладного и системного программирования.<br>1.2. Основные принципы организации и алгоритмы функционирования систем безопасности в современных операционных системах и оболочках.<br>1.3. Возможности использования сетевых и криптографических технологий в различных областях информационной безопасности.<br>1.4. Законодательство Российской Федерации в области обеспечения безопасности и защиты персональных данных.<br>**2. Уметь:**<br>2.1. Адаптировать известные методы информационной безопасности и защиты информации для конкретных информационных систем.<br>2.2. Разрабатывать комплекс |

| | | | |
|---|---|---|---|
| | | | организационно-технических мероприятий по обеспечению безопасности данных в информационных системах. |
| | | 2.Умеет использовать технологии прикладного и системного программирования, включая среды высокоуровневого программирования, а также концепции построения компьютерных сетей в профессиональной деятельности. | **1. Знать:**<br>1.1. Основные составляющие технологий прикладного и системного программирования.<br>1.2. Концепции построения компьютерных сетей в профессиональной деятельности.<br>**2. Уметь:**<br>2.1. Использовать технологии прикладного и системного программирования, включая среды высокоуровневого программирования.<br>2.2. Проектировать компьютерные сети в профессиональной деятельности. |
| | | 3.Имеет практический опыт разработки программных продуктов и комплексов с использованием современных технологий программирования. | **1. Знать:**<br>1.1. Основные положения информационной безопасности информационных систем в рамках разработки программных продуктов и комплексов.<br>1.2. Программу информационной безопасности Российской Федерации.<br>1.3. Требования к информационной безопасности и защите информации в информационных системах.<br>**2. Уметь:**<br>2.1. Анализировать состав средств, обеспечивающих информационную безопасность и защиту информации в информационных системах, программных продуктах и комплексах.<br>2.2. Осуществлять выбор вида аппаратного и программного обеспечения для решения задач информационной безопасности информационных систем, программных продуктов и комплексов. |

## 3. Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» является обязательной дисциплиной общефакультетского (предпрофильного) цикла программы бакалавриата профиля «Компьютерные технологии анализа больших данных», направление подготовки 02.03.01 Математика и компьютерные науки.

Дисциплина «Информационная безопасность» базируется на знаниях, полученных в рамках изучения дисциплин «Математика», «Дискретная математика», «Анализ данных», «Алгоритмы и структуры данных в языке Python».

## 4. Объем дисциплины в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся

*Очная форма обучения*

Таблица 2

| **Вид учебной работы по дисциплине** | **Всего (в з/е и часах)** | **Семестр 6 (в часах)** |
|---|---|---|
| **Общая трудоемкость дисциплины** | **3/108** | **108** |
| ***Контактная работа - Аудиторные занятия*** | **50** | **50** |
| *Лекции* | 16 | 16 |
| *Семинары, практические занятия* | 34 | 34 |
| ***Самостоятельная работа*** | **58** | **58** |
| Вид текущего контроля | контрольная работа | контрольная работа |
| Вид промежуточной аттестации | зачет | зачет |

## 5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий

### 5.1 Содержание дисциплины

***Тема 1. Основные понятия и задачи информационной безопасности. Информационная безопасность в системе национальной безопасности РФ***

Понятийный аппарат и основы терминологии информационной и национальной безопасности. Виды национальной безопасности и их краткая

характеристика. Системные связи информационной безопасности с другими видами национальной безопасности. Информационная война против РФ.

***Тема 2. Угрозы и уязвимости информационной безопасности. Управление рисками***

Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация. Угрозы конфиденциальности, целостности и доступности информации. Системная классификация угроз.

Антропогенные, техногенные, организационно-правовые и комбинированные информационные уязвимости.

Общая характеристика анализа и управления рисками. Программные средства, используемые для анализа рисков

***Тема 3. Меры и средства обеспечения информационной безопасности. Государственная политика в области информационной безопасности***

Организационно-правовые, программно-аппаратные, криптографические и стеганографические средства обеспечения информационной безопасности. Пассивные и активные средства противодействия техническим разведкам. Защита информации от утечки по техническим каналам.

Национальные интересы личности, общества и государства в информационной сфере. Государственные органы РФ обеспечения информационной безопасности. Приоритетные направления и проблемы обеспечения информационной безопасности в условиях информационного противоборства. Основные законы в области обеспечения информационной безопасности.

***Тема 4. Обработка и передача информации в вычислительных и управляющих системах и сетях связи. Вопросы информационной безопасности и защиты информации для вычислительных и управляющих систем и сетей. Общие вопросы организации системы защиты информации на предприятии***

Человек и информация; сообщения, сигналы; обобщенная структурная схема систем электросвязи. Компьютерная информация; системное, прикладное и специальное программное обеспечение; понятие «открытой» системы; модель

взаимодействия элементов «открытых» систем, информационно-вычислительная система. Виды защищаемой информации: семантическая и признаковая. Исторический аспект развития проблемы защиты информации. Развитие идей и концепций защиты информации.

Технические, правовые и организационные методы и средства защиты информации. Уязвимые места информационно-вычислительных и управляющих систем на предприятии: кабельная система, система электроснабжения, система архивирования и дублирования информации. Защита от стихийных бедствий.

### 5.2 Учебно-тематический план

Таблица 3

| № п/п | Наименование разделов дисциплины | Трудоемкость в часах | | | | | |
|---|---|---|---|---|---|---|---|
| | | Всего часов* | Аудиторная работа | | | Самостоятельная работа | Форма текущего контроля успеваемости |
| | | | Общая* | Лекции | Семинары, практические занятия* | | |
| 1 | Основные понятия и задачи информационной безопасности. Информационная безопасность в системе национальной безопасности РФ | 26 | 8 | 2 | 6 | 18 | Доклады, презентации, обсуждение в группе |
| 2 | Угрозы и уязвимости информационной безопасности. Управление рисками | 26 | 16 | 4 | 12 | 10 | Доклады, презентации, обсуждение в группе, опрос, решение ситуационной задачи |
| 3 | Меры и средства обеспечения информационной безопасности. Государственная политика в области информационной безопасности | 26 | 16 | 8 | 8 | 10 | Доклады, презентации, обсуждение в группе, опрос, решение ситуационной задачи |
| 4 | Обработка и передача информации в вычислительных и управляющих системах и сетях связи. Вопросы информационной | 30 | 10 | 2 | 8 | 20 | Доклады, презентации, групповые и индивидуальные |

| № п/п | Наименование разделов дисциплины | Трудоемкость в часах | | | | | |
|---|---|---|---|---|---|---|---|
| | | Всего часов* | Аудиторная работа | | | Самостоятельная работа | Форма текущего контроля успеваемости |
| | | | Общая* | Лекции | Семинары, практические занятия* | | |
| | безопасности и защиты информации для вычислительных и управляющих систем и сетей. Общие вопросы организации системы защиты информации на предприятии | | | | | | практические задания, аудиторная письменная контрольная работа |
| | В целом по дисциплине | 108 | 50 | 16 | 34 | 58 | Согласно учебному плану: контрольная работа |
| | Итого в % | 100% | 48% | 32% | 68% | 52% | |

## 5.3 Содержание семинаров, практических занятий

Таблица 4

| Наименование тем (разделов) дисциплины | Перечень вопросов для обсуждения на семинарских, практических занятиях, рекомендуемые источники из разделов 8,9 (указывается раздел и порядковый номер источника) | Формы проведения занятий |
|---|---|---|
| Основные понятия и задачи информационной безопасности. Информационная безопасность в системе национальной безопасности РФ | Понятийный аппарат и основы терминологии информационной и национальной безопасности. Виды национальной безопасности и их краткая характеристика. Системные связи информационной безопасности с другими видами национальной безопасности. Информационная война против РФ.<br><br>Источники: 8 – 1, 12;<br>9 – 2, 3, 4, 5, 9 | Подготовка докладов с презентациями.<br><br>Учебное практическое задание: проанализировать Доктрину ИБ РФ и построить схему органов государственной власти и самоуправления, отвечающих за информационную безопасность и определить их функциональные обязанности; определить положения государственной политики в области обеспечения ИБ, выделить первоочередные |

| Наименование тем (разделов) дисциплины | Перечень вопросов для обсуждения на семинарских, практических занятиях, рекомендуемые источники из разделов 8,9 (указывается раздел и порядковый номер источника) | Формы проведения занятий |
|---|---|---|
| | | мероприятия по обеспечению ИБ, дать им оценку. |
| Угрозы и уязвимости информационной безопасности. Управление рисками | Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация. Угрозы конфиденциальности, целостности и доступности информации. Системная классификация угроз.<br>Антропогенные, техногенные, организационно-правовые и комбинированные информационные уязвимости.<br>Общая характеристика анализа и управления рисками. Программные средства, используемые для анализа рисков<br><br>Источники: 8- 1, 4, 7, 8, 9, 10, 11, 12;<br>9 – 2, 3, 4, 5, 6, 7, 8, 9 | Подготовка докладов с презентациями.<br><br>Учебное практическое задание:<br>анализ возможных уязвимостей ИС, используя БДУ ФСТЭК России, а также иные источники данных об уязвимостях в качестве исходных данных.<br><br>Учебное практическое задание: Исходя из целей защиты информации и носителей информации необходимо определить список угроз ИБ, характерных для конкретного предприятия. Проанализировать риски, определить степень их допустимости. Составить модели нарушителей информационной безопасности, актуальных для данного предприятия. |
| Меры и средства обеспечения информационной безопасности. Государственная политика в области информационной безопасности | Организационно-правовые, программно-аппаратные, криптографические и стеганографические средства обеспечения информационной безопасности. Пассивные и активные средства противодействия техническим разведкам. Защита информации от утечки по техническим каналам.<br>Национальные интересы личности, общества и государства в информационной сфере. Государственные органы РФ обеспечения информационной безопасности. Приоритетные направления и проблемы обеспечения информационной безопасности в условиях информационного противоборства. Основные законы в области обеспечения информационной безопасности | Подготовка докладов с презентациями.<br><br>Учебное практическое задание: Разработка практических рекомендаций по обеспечению безопасности информационных систем. Функциональные компоненты и архитектура. Шифрование. Контроль целостности.<br><br>Учебное практическое задание: |

| Наименование тем (разделов) дисциплины | Перечень вопросов для обсуждения на семинарских, практических занятиях, рекомендуемые источники из разделов 8,9 (указывается раздел и порядковый номер источника) | Формы проведения занятий |
|---|---|---|
| | Источники: 8- 1, 2, 3, 4, 9, 10, 11, 12;<br>9 – 2, 3, 4, 5, 6, 7, 8, 9 | Обзор российского законодательства в области информационной безопасности (уголовный кодекс РФ, ФЗ, работа в Консультанте)<br>Другие законы и нормативные акты. Обзор зарубежного законодательства в области информационной безопасности. |
| Обработка и передача информации в вычислительных и управляющих системах и сетях связи. Вопросы информационной безопасности и защиты информации для вычислительных и управляющих систем и сетей. Общие вопросы организации системы защиты информации на предприятии | Человек и информация; сообщения, сигналы; обобщенная структурная схема систем электросвязи. Компьютерная информация; системное, прикладное и специальное программное обеспечение; понятие «открытой» системы; модель взаимодействия элементов «открытых» систем, информационно-вычислительная система. Виды защищаемой информации: семантическая и признаковая. Исторический аспект развития проблемы защиты информации. Развитие идей и концепций защиты информации.<br>Технические, правовые и организационные методы и средства защиты информации. Уязвимые места информационно-вычислительных и управляющих систем на предприятии: кабельная система, система электроснабжения, система архивирования и дублирования информации. Защита от стихийных бедствий.<br><br>Источники: 8- 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12;<br>9 – 1, 2, 3, 4, 5, 6, 7, 8, 9 | Подготовка докладов с презентациями.<br><br>Учебное практическое задание:<br>проанализировать защищенность системного, прикладного и специального программного обеспечения; информационно-вычислительной системы предприятия.<br><br>Учебное практическое задание:<br>проанализировать структуру среднего предприятия, рассмотреть виды информации и носители, используемые в его подразделениях. Сформулировать цели защиты информации на данном предприятии. Составить программу информационной безопасности.<br><br>Учебное практическое задание:<br>Управление персоналом, физическая защита, |

| Наименование тем (разделов) дисциплины | Перечень вопросов для обсуждения на семинарских, практических занятиях, рекомендуемые источники из разделов 8,9 (указывается раздел и порядковый номер источника) | Формы проведения занятий |
|---|---|---|
| | | планирование восстановительных работ. |

## 6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

### 6.1 Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы

Таблица 5

| Наименование тем (разделов) дисциплины | Перечень вопросов, отводимых на самостоятельное освоение | Формы внеаудиторной самостоятельной работы |
|---|---|---|
| Основные понятия и задачи информационной безопасности. Информационная безопасность в системе национальной безопасности РФ | Виды национальной безопасности и их краткая характеристика. Системные связи информационной безопасности с другими видами национальной безопасности. | - работа с учебной, научной и справочной литературой;<br>- конспект;<br>- подготовка докладов по теме;<br>- подготовка презентаций по теме;<br>- выполнение учебного задания |
| Угрозы и уязвимости информационной безопасности. Управление рисками | Системная классификация угроз информационной безопасности. Организационно-правовые и комбинированные информационные уязвимости. Программные средства, используемые для анализа рисков | - работа с учебной, научной и справочной литературой;<br>- конспект;<br>- подготовка докладов по теме;<br>- подготовка презентаций по теме;<br>- выполнение учебного задания |
| Меры и средства обеспечения информационной безопасности. Государственная политика в области информационной безопасности | Программно-аппаратные, криптографические. Пассивные и активные средства противодействия техническим разведкам. Защита информации от утечки по техническим каналам. Основные законы РФ и стандарты в области обеспечения информационной безопасности | - работа с учебной, научной и справочной литературой;<br>- конспект;<br>- подготовка докладов по теме;<br>- подготовка презентаций по теме;<br>- выполнение учебного задания |
| Риски информационной безопасности и проблема построения комплексной | Оценка рисков и организация управления процессом защиты информации. | - работа с учебной, научной и справочной литературой;<br>- конспект; |

| Наименование тем (разделов) дисциплины | Перечень вопросов, отводимых на самостоятельное освоение | Формы внеаудиторной самостоятельной работы |
|---|---|---|
| системы защиты информации | | - подготовка докладов по теме;<br>- подготовка презентаций по теме;<br>- выполнение учебного задания |
| Обработка и передача информации в вычислительных и управляющих системах и сетях связи. Вопросы информационной безопасности и защиты информации для вычислительных и управляющих систем и сетей. Общие вопросы организации системы защиты информации на предприятии | Основные виды защищаемой информации.<br>Уязвимые места информационно-вычислительных и управляющих систем на предприятии: кабельная система, система электроснабжения, система архивирования и дублирования информации.<br>Защита от стихийных бедствий. | - работа с учебной, научной и справочной литературой;<br>- конспект;<br>- подготовка докладов по теме;<br>- подготовка презентаций по теме;<br>- выполнение учебного задания |

### 6.2 Перечень вопросов, заданий, тем для подготовки к текущему контролю

Форма текущего контроля – контрольная работа.

### Примерный перечень вопросов к контрольной работе, примеры заданий контрольных работ

1. Какие вам известны подходы к классификации угроз безопасности информации? Сравните их между собой с точки зрения наибольшего соответствия практическим потребностям создания систем защиты информации.

2. Каковы основные принципы защиты информации от несанкционированного доступа? В чем заключается суть каждого из них?

3. Что можно сказать о взаимодействии уровней безопасности субъектов и объектов доступа для различных видов доступа, с которыми оперирует модель Белла – Ла Падула?

4. Назовите основные способы аутентификации. Какой из этих способов является, по-вашему, наиболее эффективным?

5. Раскройте содержание разграничения доступа к информации с помощью монитора обращений.

6. Что изучают криптография, криптоанализ и криптология? Дайте определения этим наукам.

7. Раскройте основное содержание алгоритма электронной цифровой подписи.

8. Назовите основные виды технических каналов.

9. Назовите известные вам методы и средства контроля акустической информации.

10. Охарактеризуйте основные способы предотвращения утечки информации по техническим каналам.

11. Опишите систему органов государственного управления Российской Федерации, осуществляющих управление и координацию деятельности в области защиты информации и обеспечения информационной безопасности.

**Примерный перечень вопросов к аудиторной письменной работе**

1. Охарактеризуйте основные принципы системной классификации угроз безопасности информации.

2. Сравните различные известные вам модели защиты от несанкционированного доступа к информации.

3. Дайте определения идентификации и аутентификации пользователей. В чем разница между этими понятиями?

4. Раскройте содержание разграничения доступа к информации с помощью монитора обращений.

5. Раскройте содержание модели разграничения доступа Лэмпсона – Грэхема – Деннинга.

6. Какие методы криптографического закрытия информации вы знаете? В чем разница между шифрованием и кодированием?

7. Охарактеризуйте основные фазы, в которых может существовать компьютерный вирус.

8. Дайте определение понятию «технический канал утечки информации».

9. Охарактеризуйте методы контроля информации техническими средствами в каналах телефонной связи.

10. Приведите известные вам методы защиты от утечки информации по акустическому каналу. Попробуйте сравнить их, используя критерий «эффективность/стоимость».

11. Изложите кратко основное содержание деятельности ФСТЭК России в области обеспечения информационной безопасности.

**Примерный перечень докладов и презентаций по проблемным темам дисциплины**

1. Государственная система защиты информации в России.
2. Стратегия национальной безопасности Российской Федерации.
3. Современная защита информационной безопасности в России: проблемы и направления её развития.
4. Государственная система защиты информации в России.
5. Содержание правового режима информации.
6. Понятие правового режима информации.
7. Соотношение государственной и служебной тайн.
8. Правовое регулирование международного информационного обмена.
9. Преступления в информационной сфере.
10. Соотношение служебной и коммерческой тайн.
11. Правовое регулирование использования аналогов собственноручной подписи.
12. Информационная безопасность общества.
13. Информационная безопасность личности.
14. Информационная безопасность государства.
15. Правовой режим коммерческой тайны.
16. Правовой режим персональных данных.
17. Административно-правовая ответственность в информационной сфере.

18. Уголовно-правовая ответственность в информационной сфере.

19. Гражданско-правовая ответственность в информационной сфере.

20. Правовая защита информации.

21. Право граждан на доступ к информации.

22. Право юридических лиц на получение информации.

23. Информационная открытость органов государственной власти.

24. Информационное обеспечение деятельности органов государственной власти.

25. Правовой режим информации, составляющей государственную тайну.

26. Информационное обеспечение деятельности правоохранительных органов.

27. Защита коммерческой тайны фирмы.

28. География киберпреступности: преступление и наказание.

29. Особенности нормативно-правовой защиты кибернетической информации в нашей стране.

30. Информационное противоборство в бизнесе: кто же реально управляет предприятием?

31. Защита информационной среды бизнеса от киберпреступлений.

32. Что же защищает информационная безопасность в компании, или какие тайны страшнее.

33. Безопасность как социальное явление: сущность и содержание.

34. Можно ли говорить о том, что в РФ созданы безопасные условия для бизнеса?

35. Облачные вычисления: условия применения, проблемы внедрения и сопровождения.

36. Обосновать критерии построения безопасного информационного общества.

37. Профессиональная и служебная тайна в РФ.

38. Меры государственного контроля в области обеспечения безопасности кибернетической информации.

39. Что же защищает информационная безопасность в компании, или какие тайны страшнее.

40. Импортозамещение и информационная безопасность бизнеса.

41. Особенности нормативно-правовой защиты кибернетической информации в нашей стране.

42. Информационная безопасность в социальных сетях.

43. В чем отличия обеспечения информационной безопасности в Российской Федерации от других стран.

44. Источники угроз безопасности персональных данных.

45. Понятия информации и информационных ресурсов в законодательстве.

46. Место информационной безопасности в стратегии национальной безопасности Российской Федерации.

**Примерный перечень тематики учебных практических заданий (лабораторных работ)**

1. Информационная война как высшая форма угрозы информационной безопасности.

2. Антропогенные информационные уязвимости.

3. Техногенные информационные уязвимости.

4. Организационно-правовые и комбинированные информационные уязвимости.

5. Уязвимые места информационно-вычислительных и управляющих систем на предприятии.

6. Оценка рисков и организация управления процессом защиты информации.

7. Защита информации от утечки по техническим каналам.

8. Обеспечение информационной безопасности средствами антивирусной защиты.

9. Обеспечение информационной безопасности при использовании ресурсов сети Интернет.

10. Обеспечение информационной безопасности при использовании средств криптографической защиты информации.

11. Обеспечение информационной безопасности информационных технологических процессов.

12. Угрозы конфиденциальности, целостности и доступности информации.

13. Обработка персональных данных в организации.

14. Организация и функционирование службы информационной безопасности организации.

15. Организация реализации планов внедрения системы обеспечения информационной безопасности.

16. Организация обнаружения и реагирования на инциденты информационной безопасности.

17. Организация обеспечения непрерывности бизнеса и его восстановления после прерываний

18. Мониторинг информационной безопасности и контроль защитных мер.

19. Проведение аудита информационной безопасности.

20. Подходы к оценке рисков нарушения информационной безопасности.

21. Процедуры оценки рисков нарушения информационной безопасности.

22. Оценка рисков нарушения информационной безопасности

23. Основные задачи и функции службы информационной безопасности организаций

24. Расчет ресурсов информационной безопасности организации.

25. Основы определения затрат на информационную безопасность.

26. Определение размера целесообразных затрат на обеспечение безопасности информации.

27. Модель определения зон и средств защиты предприятия от угроз.

28. Модель распределения работы службы безопасности предприятия.

29. Прикладной информационный анализ.

30. Потребительский индекс.

31. Добавленная экономическая стоимость.

32. Исходная экономическая стоимость.

33. Управление портфелем активов.

34. Оценка действительных возможностей.

35. Метод жизненного цикла искусственных систем.

36. Функционально-стоимостной анализ.

37. Совокупная стоимость владения.

38. Экономическая эффективность обеспечения информационной безопасности организации.

В течение семестра студент может набрать максимальное количество баллов равное 40. На промежуточную аттестацию (зачет) отводится 60 баллов. Распределение баллов по видам работ, формирующих текущий контроль успеваемости по дисциплине, отражает качество подготовки обучающихся к занятиям семинарского типа и выполнение различных видов самостоятельной работы. Критерии балльной оценки различных форм текущего контроля успеваемости содержатся в соответствующих методических рекомендациях кафедры «Информационная безопасность».

**7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине**

Перечень компетенций, формируемых в процессе освоения дисциплины содержится в Разделе 2. *«Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине».*

**Типовые контрольные задания или иные материалы, необходимые для индикаторов достижения компетенций, умений и знаний**

Таблица 6

| **Код компетенции** | **Наименование компетенции** | **Типовые задания** |
|---|---|---|
| **ОПК-5** | Способен решать стандартные задачи профессиональной деятельности на основе информационной и | **1. Владеет знаниями и технологиями, необходимыми для прикладного и системного программирования, включая современные языки программирования, а** |

| | | |
|---|---|---|
| | библиографической культуры с применением информационно-коммуникационных технологий, в том числе отечественного производителя, и с учетом основных требований информационной безопасности | **также основными принципами и понятиями, применяемыми при построении компьютерных сетей.**<br><br>**Задание 1.**<br>Классы пространства имен System.Security.Cryptography.Xml могут использоваться для шифрования элементов в XML-документе. Шифрование XML-данных позволяет хранить и передавать важные XML-данные, не беспокоясь о том, что они могут быть прочитаны.<br>При использовании симметричного алгоритма шифрования, такого как AES, также известного как алгоритм Rijndael, необходимо использовать один и тот же ключ как для шифрования, так и для расшифровки XML-данных. Предполагается, что зашифрованный XML-документ будет расшифровываться с помощью того же ключа, а между шифрующей и расшифровывающей сторонами существует соглашение по поводу используемых алгоритма и ключа. В этом примере в зашифрованный XML-документ ключ AES не включается (в зашифрованном или незашифрованном виде). Таким образом, необходимо зашифровать и расшифровать XML-элементы с помощью симметричного ключа.<br><br>**2. Умеет использовать технологии прикладного и системного программирования, включая среды высокоуровневого программирования, а также концепции построения компьютерных сетей в профессиональной деятельности.**<br><br>**Задание 2**<br><br>Необходимо реализовать шифрование XML-элемента с использованием двух ключей.<br>Изначально создается пара ключей, состоящая из открытого и закрытого ключа RSA, которая сохраняется в безопасный контейнер ключа. Далее создается отдельный ключ сеанса с использованием алгоритма AES (Rijndael) для шифрования XML-документа с последующим использованием открытого ключа RSA для шифрования ключа сеанса AES. Наконец зашифрованный |

| | | |
|---|---|---|
| | | ключ сеанса AES и зашифрованные XML-данные сохраняются в XML-документе в новом элементе EncryptedData.<br>Для расшифровки XML-элемента из контейнера ключа извлекается закрытый ключ RSA, который затем используется для шифрования ключа сеанса. Ключ сеанса далее используется для расшифровки документа.<br><br>**Задание 3**<br>Установить и настроить NGINX на базе операционной системы Linux, а также создать самоподписанный сертификат для локального веб-ресурса.<br><br>**Задание 4**<br>Разграничить права доступа пользователей в MySQL и проверить правильность работы разграничения в указанной базе данных.<br><br>**3. Имеет практический опыт разработки программных продуктов и комплексов с использованием современных технологий программирования.**<br><br>**Задание 5**<br><br>Построение модели трехсегментной ЛВС с применением языков программирования C++, C# или Python на базе маршрутизаторов и дальнейшим назначением IP-адресов сетевым интерфейсам маршрутизаторов и локальных компьютеров. Настройка статической маршрутизации Анализ работоспособности сети в режиме симуляции по протоколу ICMP. |

**Примерный перечень вопросов к зачету**

1. Были ли в вашей практике случаи попыток несанкционированного получения информации, обрабатываемой в АС? Охарактеризуйте проявившийся в каждом конкретном случае канал несанкционированного доступа и оцените возможную уязвимость информации.

2. Какие вам известны подходы к классификации угроз безопасности информации? Сравните их между собой с точки зрения наибольшего соответствия практическим потребностям создания систем защиты информации.

3. Охарактеризуйте основные принципы системной классификации угроз безопасности информации.

4. В чем, с вашей точки зрения, состоит опасность разработки и применения информационного оружия? Какие необходимо было бы применить меры международного характера в целях предотвращения информационных войн?

5. Каковы основные принципы защиты информации от несанкционированного доступа? В чем заключается суть каждого из них?

6. Представьте следующую ситуацию: министры внутренних дел и экономики имеют одинаковую (наивысшую) форму допуска и пытаются с помощью автоматизированной системы получить строго конфиденциальную информацию по вопросу расследования экономических преступлений. Каковы, на ваш взгляд, должны быть возможности их доступа к этой информации? Рассмотрите все возможные ситуации и последствия, к которым приведут принимаемые решения по доступу с точки зрения обеспечения безопасности информации.

7. Сравните различные известные вам модели защиты от несанкционированного доступа к информации.

8. Что можно сказать о взаимодействии уровней безопасности субъектов и объектов доступа для различных видов доступа, с которыми оперирует модель Белла – Ла Падула?

9. Дайте определения идентификации и аутентификации пользователей. В чем разница между этими понятиями?

10. Назовите основные способы аутентификации. Какой из этих способов является, по-вашему, наиболее эффективным?

11. Приведите примеры известных вам систем аутентификации, построенных по принципу «пользователь имеет». Что вы можете сказать о преимуществах и недостатках методов аутентификации пользователей пластиковых карт, широко используемых в банковской сфере?

12. Каковы основные характеристики устройств аутентификации? Сравните известные вам устройства по каждой из этих характеристик.

13. Какие основные методы контроля доступа используются в современных автоматизированных системах? Охарактеризуйте эти методы и рассмотрите их возможности для реализации автоматизированной системы ведения текущих счетов клиентов банка.

14. Охарактеризуйте процесс развития проблемы защиты информации в современных системах ее обработки.

15. Раскройте содержание разграничения доступа к информации с помощью монитора обращений.

16. Охарактеризуйте проблему определения предметной области информационной безопасности и дайте определения основным понятиям, используемым в этой сфере.

17. Раскройте содержание исторических этапов развития подходов к защите информации и обеспечению информационной безопасности.

18. Охарактеризуйте «вредительские» программы как один из видов угроз информационной безопасности.

19. Раскройте содержание модели разграничения доступа Лэмпсона – Грэхема – Деннинга.

20. Раскройте содержание принципов обоснованности доступа и персональной ответственности как основных принципов защиты от несанкционированного доступа.

21. В чем состоит суть принципов достаточной глубины контроля и разграничения потоков информации как основных принципов защиты информации от несанкционированного доступа?

22. Раскройте содержание принципов чистоты повторно используемых ресурсов и целостности средств защиты как основных принципов защиты информации от несанкционированного доступа.

23. Раскройте основные особенности известных вам методов аутентификации с использованием индивидуальных физиологических характеристик пользователей.

24. Рассмотрите основные методы повышения стойкости парольных систем аутентификации пользователей автоматизированных систем.

25. Что изучают криптография, криптоанализ и криптология? Дайте определения этим наукам.

26. Какие методы криптографического закрытия информации вы знаете? В чем разница между шифрованием и кодированием?

27. Объясните, что представляет собой стеганография?

28. Расскажите об особенностях симметричных и несимметричных шифров. Попробуйте привести примеры этих способов шифрования.

29. Объясните, почему основными требованиями, предъявляемыми к криптосистемам, являются наличие очень большого числа возможных ключей и равная вероятность их генерации.

30. От каких основных свойств криптографических алгоритмов зависит, на ваш взгляд, стойкость криптосистемы?

31. В чем принципиальное различие оценки стойкости криптосистемы с использованием теории информации и теории вычислительной сложности?

32. Какие основные способы шифрования вы знаете? Каковы их преимущества и недостатки?

33. Опишите наиболее известный алгоритм шифрования DES. Какие из основных методов шифрования использованы в этом алгоритме?

34. Каковы основные особенности криптосистем с общедоступным ключом?

35. Раскройте основное содержание алгоритма электронной цифровой подписи.

36. Какие методы распределения ключей в криптографических системах с большим числом абонентов вы знаете? Охарактеризуйте основные особенности децентрализованных и централизованных систем.

37. Опишите последовательность установления связи и передачи сообщений в централизованных системах распределения ключей шифрования с центром трансляции ключей и с центром распределения ключей.

38. В каких случаях применяются криптографические методы защиты информации непосредственно в ЭВМ?

39. Дайте определение компьютерного вируса как саморепродуцирующейся программы. Приведите примеры известных вам случаев заражения компьютеров вирусами.

40. Попробуйте изобразить структуру компьютерного вируса в виде программы, написанной на псевдоязыке.

41. Охарактеризуйте основные фазы, в которых может существовать компьютерный вирус.

42. Охарактеризуйте известные вам основные классы антивирусных программ. В чем смысл комплексного применения нескольких программ?

43. Каковы, на ваш взгляд, должны быть основные правила работы с компьютером, предупреждающие возможное заражение его вирусами?

44. Охарактеризуйте перспективные методы защиты компьютеров от программ-вирусов.

45. Рассмотрите возможности вирусного подавления как одной из форм радиоэлектронной борьбы.

46. Каковы основные механизмы внедрения компьютерных вирусов в поражаемую систему?

47. Раскройте содержание комплексной стратегии защиты, ориентированной на противодействие возможному вирусному подавлению.

48. Дайте определение понятию «технический канал утечки информации». Назовите основные виды технических каналов.

49. Какой, по вашему мнению, технический канал утечки информации можно отнести к наиболее часто используемым техническими разведками для получения конфиденциальной информации? Раскройте особенности этого канала.

50. Дайте классификацию источников утечки информации по техническим каналам.

51. Что такое основные и вспомогательные технические средства автоматизированной системы? Приведите примеры и рассмотрите возможности их использования в качестве технических каналов утечки информации.

52. Назовите известные вам методы и средства контроля акустической информации.

53. Охарактеризуйте методы контроля информации техническими средствами в каналах телефонной связи.

54. Назовите методы контроля информации, обрабатываемой средствами вычислительной техники.

55. Охарактеризуйте основные способы предотвращения утечки информации по техническим каналам.

56. Приведите известные вам методы защиты от утечки информации по акустическому каналу. Попробуйте сравнить их, используя критерий «эффективность/стоимость».

57. Охарактеризуйте существующие на сегодняшний день способы защиты информации в каналах связи.

58. Назовите методы и средства защиты информации от утечки по побочному электромагнитному каналу.

59. С чем, по вашему мнению, связана необходимость организационно-правового обеспечения защиты информации? в чем заключается специфика этого обеспечения применительно к информации, обрабатываемой в автоматизированных системах?

60. Охарактеризуйте задачи, решаемые организационно-правовым обеспечением защиты информации в АС. Выделите особенности, связанные с «электронной» формой представления информации в АС.

61. Сформулируйте основные направления развития организационно-правового обеспечения защиты информации в зарубежных странах. Назовите известные вам законодательные акты зарубежных стран в области регулирования процессов информатизации и обеспечения безопасности информации.

62. Что вы знаете из истории развития организационно-правового обеспечения зашиты информации в СССР и Российской Федерации? Охарактеризуйте современное состояние отечественной законодательной базы в области информатизации и защиты информации.

63. Сформулируйте основные положения Закона Российской Федерации «Об информации, информационных технологиях и защите информации». Какие еще вы знаете российские законодательные акты в этой области?

64. Сформулируйте основные подходы к разработке организационно-правового обеспечения защиты информации. Раскройте содержание структуры этого обеспечения.

65. Сформулируйте основные требования, предъявляемые к системе стандартизации в области защиты информации. Назовите известные вам системы стандартов в этой области, принятые в России и за рубежом.

66. Опишите систему органов государственного управления Российской Федерации, осуществляющих управление и координацию деятельности в области защиты информации и обеспечения информационной безопасности.

67. Изложите кратко основное содержание деятельности ФСТЭК России в области обеспечения информационной безопасности.

68. Почему, на ваш взгляд, действительно эффективная защита информации может быть обеспечена только при комплексном системном подходе к решению этой проблемы? В чем заключается комплексность? Каким требованиям должна удовлетворять концепция комплексной защиты?

69. Сформулируйте основные концептуальные положения теории защиты информации.

70. Раскройте содержание функции защиты информации. Какие из функций образуют полное множество функций защиты?

71. Сформулируйте определение задачи защиты информации и попытайтесь назвать десять классов задач, образующих репрезентативное множество задач защиты.

72. Приведите наиболее распространенную на сегодняшний день классификацию средств защиты информации. Каковы, на ваш взгляд, преимущества и недостатки программных, аппаратных и организационных средств защиты информации?

73. Дайте определение системы защиты информации и сформулируйте основные концептуальные требования, предъявляемые к ней.

74. Раскройте содержание концепции управления системой защиты информации. Каковы ее особенности по сравнению с общей концепцией управления системами организационно-технологического типа?

**Примеры практико-ориентированных (ситуационных) заданий**

**Задача 1.** Компании нужно организовать удаленный доступ для одного своего сервера в целях технического обслуживания. Политика МСЭ запрещает любой внешний доступ во внутреннюю сеть компании. Было решено установить модем для доступа к серверу по телефонной линии. В качестве контроля было решено в ручном режиме включать модем перед осуществлением работ и выключать его сразу после их окончания. Так как всё чаще и чаще организации начинают администрировать системы удаленно, компания попросила аудитора оценить риски существующего решения и предложить лучшую стратегию для аналогичных задач в будущем.

*Вопрос 1: что является наиболее важным при тестировании существующего решения?*

1. Проверка телефонной линии с точки зрения доверия к ней.

2. Определение максимальной полосы пропускания телефонной линии и её загрузки во время обслуживания.

3. Доступность телефонной линии для предоставления услуги в любое время.

4. Проверка возможности реализации модемом обратных звонков.

*Вопрос 2: какой наибольший риск в существующей реализации?*

1. Модем не включат или не выключат, когда это будет нужно.

2. Соглашение о конфиденциальности не подписано.

3. При обмене данными не используется шифрование.

4. Политика МСЭ нарушена.

*Вопрос 3: какие из следующих рекомендаций наилучшим образом позволят снизить риски удаленного доступа?*

1. Анализ логов модема, когда он был включен или выключен.

2. Шифрование трафика, идущего по телефонной линии.

3. Миграция с модема в сторону VPN.

4. Актуализация политики МСЭ и внедрение IDS системы.

**Задача 2**. Иванов И.И. устраивается на работу в ООО «Альфа». В данной организации существует режим коммерческой тайны.

Какие сведения не могут относиться к коммерческой тайне и не подлежат засекречиванию?

Составьте примерный договор об оформлении допуска сотрудников к коммерческой тайне

**Задача 3**. Деятельностью компании ООО «Звезда» является торговля товарами по каталогам в соответствии с соглашением с БПР, которая осуществляется следующим образом: покупатели выбирают товары по каталогам, находящимся в офисе предприятия, менеджер принимает заказы и оформляет необходимые документы; заказ поступает в БПР, где формируются все заказы, затем выбранные товары высылаются в г. Тамбов, где принимаются сотрудниками предприятия, покупатели оплачивают и получают заказанные товары.

Селезнева С.А. работала в ООО «Звезда» в должности менеджера, в обязанности которой входило принятие и обработка заказов от покупателей.

Общество, полагая, что Селезнева С.А. в период своей работы в должности менеджера в ООО «Звезда», имея доступ к компьютеру, подключенному по сети «Интернет» к центру заказов N 120, принадлежащий обществу, скопировала персональные данные 164 клиентов и использовала сведения, составляющих коммерческую тайну истца, в результате чего общество понесло убытки в виде потери контрагентов.

Как ООО «Звезда» может защитить свои права и законные интересы?

**Задача 4**. Уволенный работник разгласил информацию, составляющую коммерческую тайну и ставшую ему известной в связи с исполнением трудовых обязанностей у бывшего работодателя.

Вправе ли организация взыскать с уволенного работника убытки, причиненные разглашением информации?

**Задача 5**. Организация, являющаяся лицом, участвующим в деле, которое рассматривается арбитражным судом, заявила ходатайство о рассмотрении дела в закрытом судебном заседании. Ходатайство было заявлено из соображений сохранения сведений, составляющих коммерческую тайну. Судом отказано в удовлетворении ходатайства. Можно ли обжаловать в апелляционную инстанцию определение арбитражного суда об отказе в удовлетворении ходатайства о рассмотрении дела в закрытом судебном заседании?

**Задача 6**. Петрова работала на секретном предприятии с допуском к государственной тайне. В 2014 году она уволилась. В 2019 году Петрова захотела поехать отдыхать в Турцию. Однако в выдаче загранпаспорта ей было отказано т.к. сведения, к которым Петрова была допущена в 2014 году, сохраняют секретность.

Оцените ситуацию. Через какое время Петрова сможет выехать за границу?

**Задача 7**. Вы – начальник информационной службы в Компании. У вас возникли подозрения, что сотрудник вашей Компании позволил себе неправомерный доступ к охраняемой законом компьютерной информации, что повлекло уничтожение и блокирование информации.

1. Какая статья уголовного кодекса была нарушена?

2. Какое наказание должен понести нарушитель?

**Задача 8.** В одной из фирм, занимающихся разработкой прикладных программ, группа программистов, используя свое служебное положение, подобрала код к банковским счетам некоторых клиентов.

В течение некоторого времени они переводили деньги на счета подставных лиц. Чтобы скрыть следы своего преступления, программисты запустили вирус, который разрушил базу данных банка.

Кроме того, им удалось прослушать переговоры между банковскими служащими. По решению правления банка, историю с взломом счетов и распространением вируса, решили замолчать, чтобы не портить репутацию банка.

Программисты стали шантажировать председателя правления, требуя дополнительных денежных переводов. В противном случае, они обещали распространить подробную информацию в глобальной сети.

В ходе проводившейся налоговой проверки были установлены факты правонарушений со стороны руководства банка, за что оно было привлечено к ответственности. Вину программистов доказали частично.

Найти и определить тип информационных преступлений. Предложить меры по предотвращению подобных преступлений.

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

**Рекомендуемая литература**

**Нормативные акты**

1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне».

3. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных».

4. СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».

5. СТО БР ИББС-1.2 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0».

6. Рекомендации в области стандартизации Банка России РС БР ИББС-2.0 «Обеспечение информационной безопасности организаций БС РФ. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0».

7. СТО БР ИББС-2.2-2009 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности».

8. РС БР ИББС-2.7-2015 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Ресурсное обеспечение информационной безопасности.

**Основная литература**

9. Хорев, П.Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - Москва: Форум: НИЦ ИНФРА-М, 2019. - 352 с. – ЭБС Znanium.com. - URL: http://znanium.com/catalog/product/1025261 (дата обращения: 11.11.2019). – Текст: электронный.

10. Гришина, Н. В. Информационная безопасность предприятия: учебное пособие / Н. В. Гришина. — Москва: ФОРУМ, 2017. – 239 с. – ЭБС Znanium.com. – URL: http://znanium.com/catalog/product/612572 (дата обращения: 11.11.2019). - Текст: электронный.

11. Баранова, Е.К. Информационная безопасность и защита информации: учебное пособие / Е.К.Баранова, А.В. Бабаш. — Москва: РИОР: ИНФРА-М, 2019. — 322 с. — ЭБС Znanium.com. - URL: http://znanium.com/catalog/product/1009606 (дата обращения 11.11.2019). - Текст: электронный.

**Дополнительная литература**

12. Жук, А.П. Защита информации: учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — Москва: РИОР: ИНФРА-М, 2019. — 400 с. — ЭБС Znanium.com. - URL: http://znanium.com/catalog/product/1018901 (дата обращения: 11.11.2019). - Текст: электронный.

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

1. Сайт Центрального банка Российской Федерации: www.cbr.ru;
2. Сайт Федеральной службы по техническому и экспортному контролю: www.fstec.ru;

3. Электронная библиотека Финансового университета (ЭБ) http://elib.fa.ru/ (http://library.fa.ru/files/elibfa.pdf)

4. Электронно-библиотечная система BOOK.RU http://www.book.ru

5. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» http://biblioclub.ru/

6. Электронно-библиотечная система Znanium http://www.znanium.com

7. «Деловая онлайн библиотека» издательства «Альпина Паблишер» http://lib.alpinadigital.ru/en/library

8. Электронно-библиотечная система издательства «Лань» https://e.lanbook.com/

9. Электронно-библиотечная система издательства «ЮРАЙТ» https://www.biblio-online.ru/

10. Научная электронная библиотека eLibrary.ru http://elibrary.ru

11. Справочная правовая система КонсультантПлюс». [Электронный ресурс]. Режим доступа: http://www.consultant.ru/

## 10. Методические указания для обучающихся по освоению дисциплины

Рекомендации по освоению дисциплины приведены в «Методических рекомендациях для студентов бакалавриата по освоению дисциплин образовательных программ высшего образования», утвержденных распоряжением Финуниверситета от 14 мая 2014 г. № 256.

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

### 11.1 Комплект лицензионного программного обеспечения:

1. Windows, Linux, Microsoft Office, Chrome

2. Программное обеспечение антивирусной защиты компьютера

**11.2 Современные профессиональные базы данных и информационные справочные системы:**

1. Информационно-правовая система «Гарант».

2. Информационно-правовая система «Консультант Плюс».

3. Электронная энциклопедия: http://ru.wikipedia.org/wiki/Wiki.

4. Система комплексного раскрытия информации «СКРИН» - http://www.skrin.ru/11.3.

**11.3 Сертифицированные программные и аппаратные средства защиты информации –** не предусмотрены

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

Занятия по дисциплине проводятся в аудиториях, оборудованных мультимедийными комплексами, компьютерами с выходом в Интернет.