

**МИНОБРНАУКИ РОССИИ**

**Федеральное государственное автономное образовательное  
учреждение высшего образования "Пермский  
государственный национальный исследовательский  
университет"**

**Колледж профессионального образования**

Авторы-составители: **Журавлева Анастасия Валерьевна  
Серебрякова Наталия Александровна**

Рабочая программа дисциплины  
**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**  
Код УМК 89466

Утверждено  
Протокол №10  
от «23» мая 2023 г.

Пермь, 2023

## **1. Наименование дисциплины**

Информационная безопасность

## **2. Место дисциплины в структуре образовательной программы**

Дисциплина входит в Блок « ПРОФ » образовательной программы по направлениям подготовки (специальностям):

Направление подготовки: **09.02.07** Информационные системы и программирование  
направленность не предусмотрена

### **3. Планируемые результаты обучения по дисциплине**

В результате освоения дисциплины **Информационная безопасность** у обучающегося должны быть сформированы следующие компетенции:

**09.02.07** Информационные системы и программирование (направленность : не предусмотрена)

**ОК.1** Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам

**ОК.2** Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности

**ОК.4** Эффективно взаимодействовать и работать в коллективе и команде

**ПК.4.4** Обеспечивать защиту программного обеспечения компьютерных систем программными средствами

#### 4. Объем и содержание дисциплины

<b>Направление подготовки</b>	09.02.07 Информационные системы и программирование (направленность: не предусмотрена) на базе среднего общего
<b>форма обучения</b>	очная
<b>№№ триместров, выделенных для изучения дисциплины</b>	8
<b>Объем дисциплины (з.е.)</b>	4.2
<b>Объем дисциплины (ак.час.)</b>	150
<b>Контактная работа с преподавателем (ак.час.), в том числе:</b>	104
<b>Проведение лекционных занятий</b>	48
<b>Проведение практических занятий, семинаров</b>	56
<b>Самостоятельная работа (ак.час.)</b>	46
<b>Формы текущего контроля</b>	Входное тестирование (1) Защищаемое контрольное мероприятие (1) Итоговое контрольное мероприятие (1) Письменное контрольное мероприятие (1)
<b>Формы промежуточной аттестации</b>	Экзамен (8 триместр)

## **5. Аннотированное описание содержания разделов и тем дисциплины**

### **Безопасность и управление доступом в информационных системах**

#### **Основные понятия и определения, эволюция подходов к обеспечению информационной безопасности**

Общие проблемы безопасности. Роль и место информационной безопасности.

Основные предметные направления защиты информации

Информационные, программно-математические, физические и организационные угрозы системы

- Понятие угрозы защиты информации, источники угроз.

- Угрозы информации в ЭВМ.

- Классификация угроз и их характеристики.

- Функции и задачи защиты информации.

- Угроза безопасности информации в компьютерных системах.

#### **Функции и задачи защиты информации. Методы и системы защиты информации**

Защита от несанкционированного доступа, модели, и основные принципы защиты информации.

Функции и задачи защиты информации. Методы и системы защиты информации.

Основные свойства защищаемой информации.

Методы и средства защиты информации от традиционных шпионажи и диверсий.

Методы и средства защиты информации от электромагнитных излучений и наводок

#### **Криптографические методы защиты информации**

Криптографические методы защиты информации.

Асимметричные шифры

Симметричные шифры

Блочные шифры

Поточные шифры

Шифры Цезаря, Вижинера, Полибия и т.д.

#### **Алгоритмы шифрования**

Зашифровывание и расшифровывание

Криптостойкость шифра

Алгоритмы шифрования

Симметричное шифрование

Асимметричное шифрование (с открытым ключом)

Хеш-функции

ЭЦП

#### **Организация безопасности в автоматизированных информационных системах АИС**

Понятие клиента прав доступа, групп, паролей, политики безопасности в современных АИС

Элементы и объекты защиты информации в АИС. Угрозы безопасности информации. Методы

подтверждения подлинности пользователей и разграничение доступа к компьютерным ресурсам. Цели защиты информации в АИС.

Информационные, программно-математические, физические и организационные угрозы.

Обеспечение и поддержка целостности и согласованности данных в АИС. Основные цели политики безопасности современных АИС. Методы и приемы обеспечения безопасности информации в АИС.

Политика безопасности АИС.

Принципы организации разноуровневого доступа в АИС. Способы защиты. Разграничение и управление доступом к элементам защищаемой информации.

## **Задачи по защите информации в АИС. Объекты защиты. Планирование и реализация систем защиты**

Системный и комплексный подход к анализу и обеспечению информационной безопасности АИС, БД и БНД в процессах их создания и эксплуатации (администрирования). Представление, анализ и обоснование моделей, методов и механизмы обеспечения информационной безопасности АИС, БД и БНД; практические навыки работы с нормативно-методическими документами (стандартами) в сфере информационной безопасности автоматизированных информационных систем.

### **Методы и средства защиты информации в АИС**

При организации автоматизированных информационных систем (АИС) должны строго соблюдаться требования по защите конфиденциальных данных, которые призваны предотвратить их утечку или искажение. Защита информации в автоматизированной системе должна предотвратить воздействие угроз различного происхождения, включая техногенные аварии, воздействие вредоносного ПО или хакеров, похищение данных инсайдерами с целью продажи или шпионажа. Снизить уровень таких рисков позволяет реализация комплекса мер защиты аппаратного и программного уровня.

### **Защита программного обеспечения**

Проблема вирусного заражения программ

Классификация вирусов. Вред наносимый информации компьютерными вирусами

Структура современных антивирусных программ и перспективные методы антивирусной защиты.

Методы борьбы с компьютерными вирусами

### **Защита от несанкционированного использования программ**

Система мер, направленных на противодействие нелегальному использованию программного обеспечения

### **Защита от копирования ПО**

Система мер, направленных на противодействие несанкционированному копированию информации, как правило, представленной в электронном виде

### **Сертификация ПО**

Проведение независимой, в том числе метрологической, экспертизы используемого программного обеспечения на предмет установления его соответствия требованиям соответствующей нормативной документации.

### **Защита от утечки информации по техническим причинам**

Безопасность компьютерных сетей

Элементы сети. Возможности угрозы целостности информации сети.

Защита информации в компьютерных сетях.

Политика безопасности работы в Интернете.

Требования к защищенности КС от несанкционированного изменения структур.

Система разграничения доступа к информации в КС.

Меры технологической безопасности информации в вычислительных сетях.

Программные и технические средства защиты информации в сети.

Сетевые экраны/

### **Цели и способы обеспечения защиты каналов утечки информации**

В зависимости от происхождения информации (речевая, печатная, цифровая) ее утечка может

происходить по следующим каналам: физическое хищение документов или цифровых носителей; копирование и считывание конфиденциальной информации; применение «троянских» и фишинговых вирусных программ; хищение паролей персонала компании или организации; подключение к линиям связи незаконными способами; выведение существующих механизмов защиты из строя.

Меры защиты от утечки информации: аутентификация и управление доступом, фильтрация контента, шифрование, аудит инфобезопасности.

### **Виды технических каналов утечки информации**

Методы и пути утечки информации из информационной системы; паразитная цепочка носителей информации, один или несколько из которых являются правонарушителем или его специальной аппаратурой. Играют основную роль в защите информации, как фактор информационной безопасности. Классификация технических каналов утечки информации проводится по физической принадлежности: акустические; электромагнитные; материально-вещественные; визуально-оптические (использование видеонаблюдения и фотографии).

### **Организационно-правовое обеспечение информационной безопасности**

Правовые основы защиты информации

Правовые и законодательные меры по защите информации

Административные и организационные мероприятия информационной безопасности

Построение политики безопасности организации.

### **Международное и российское законодательство в сфере защиты информации**

Понятие информационной безопасности и защищенной системы. Необходимость защиты информационных систем и телекоммуникаций. Технические предпосылки кризиса информационной безопасности. Информационная безопасность в условиях функционирования в России глобальных сетей. Основные задачи обеспечения защиты информации. Основные методы и средства защиты информационных систем.

### **Правовое регулирование информационной безопасности. Правонарушения в области ИТ.**

Общее представление о структуре защищенной информационной системы. Особенности современных информационных систем, факторы влияющие на безопасность информационной системы. Понятие информационного сервиса безопасности. Виды сервисов безопасности.

Идентификация и аутентификация. Парольные схемы аутентификации. Симметричные схемы аутентификации субъекта. Несимметричные схемы аутентификации (с открытым ключом).

Аутентификация с третьей доверенной стороной (схема Kerberos). Токены, смарт-карты, их применение. Использование биометрических данных при аутентификации пользователей. Сервисы управления доступом. Механизмы доступа данных в операционных системах, системах управления базами данных.

Ролевая модель управления доступом.

### **Назначение обеспечения информационной безопасности. Виды тайны**

Государственная тайна. Персональные данные/GDPR. Коммерческая тайна. Автоматизированные системы управления технологическими процессами (АСУ ТП). Государственные и муниципальные ИС. Информация для служебного пользования. Открытые информационные ресурсы.

К видам информационной безопасности относят: сетевую безопасность, безопасность веб-приложений, безопасность данных, безопасность конечных точек, безопасность мобильных устройств, облачная безопасность, безопасность Интернета вещей (IoT Security), целевые кибератаки АРТ-группировок (Advanced Persistent Threat)

### **Нормативное, организационное и правовое регулирование информационной безопасности в**

### **организациях. Политика безопасности**

Основные положения теории информационной безопасности информационных систем. Формальные модели безопасности их значение для построения защищенных информационных систем. Понятие доступа к данным и монитора безопасности. Функции монитора безопасности. Понятие политики безопасности информационных систем. Разработка и реализация политики безопасности. Управление доступом к данным. Основные типы политики безопасности управления доступом к данным: дискреционная и мандатная политика безопасности. Анализ способов нарушений безопасности. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.

## **6. Методические указания для обучающихся по освоению дисциплины**

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторские занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы. Обучающемуся важно помнить, что контактная работа с преподавателем эффективно помогает ему овладеть программным материалом благодаря расстановке необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации.

Самостоятельная работа преследует следующие цели:

- закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;
- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;
- совершенствование навыков поиска научных публикаций и образовательных ресурсов, размещенных в сети Интернет;
- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем во время проведения мероприятий текущего контроля и учитываются при промежуточной аттестации.

Обучающимся с ОВЗ и инвалидов предоставляется возможность выбора форм проведения мероприятий текущего контроля, альтернативных формам, предусмотренным рабочей программой дисциплины. Предусматривается возможность увеличения в пределах 1 академического часа времени, отводимого на выполнение контрольных мероприятий.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации.

При проведении текущего контроля применяются оценочные средства, обеспечивающие передачу информации, от обучающегося к преподавателю, с учетом психофизиологических особенностей здоровья обучающихся.

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

При самостоятельной работе обучающимся следует использовать:

- конспекты лекций;
- литературу из перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля);
- текст лекций на электронных носителях;
- ресурсы информационно-телекоммуникационной сети "Интернет", необходимые для освоения дисциплины;
- лицензионное и свободно распространяемое программное обеспечение из перечня информационных технологий, используемых при осуществлении образовательного процесса по дисциплине;
- методические указания для обучающихся по освоению дисциплины.

## 8. Перечень основной и дополнительной учебной литературы

### Основная:

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2021. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. <https://urait.ru/bcode/470351>
2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // ЭБС Юрайт [сайт]. <https://urait.ru/bcode/449548>

### Дополнительная:

1. Информационные технологии в 2 т. Том 1 : учебник для среднего профессионального образования / В. В. Трофимов, О. П. Ильина, В. И. КИЯЕВ, Е. В. Трофимова ; под редакцией В. В. Трофимова. — Москва : Издательство Юрайт, 2021. — 238 с. — (Профессиональное образование). — ISBN 978-5-534-03964-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. <https://urait.ru/bcode/469957>
2. Информационные технологии в 2 т. Том 2 : учебник для среднего профессионального образования / В. В. Трофимов, О. П. Ильина, В. И. КИЯЕВ, Е. В. Трофимова ; под редакцией В. В. Трофимова. — Москва : Издательство Юрайт, 2021. — 390 с. — (Профессиональное образование). — ISBN 978-5-534-03966-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. <https://urait.ru/bcode/469958>
3. Рыбальченко, М. В. Архитектура информационных систем : учебное пособие для среднего профессионального образования / М. В. Рыбальченко. — Москва : Издательство Юрайт, 2020. — 91 с. — (Профессиональное образование). — ISBN 978-5-534-01252-1. — Текст : электронный // ЭБС Юрайт [сайт]. <https://urait.ru/bcode/452922>



безопасности : учебник и практикум для среднего профессионального образов

<https://urait.ru/bcode/469958> Информационные технологии в 2 т. Том 2 : учебник для среднего профессионального образования

<https://urait.ru/bcode/470351> Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образов

<https://urait.ru/bcode/452922> Архитектура информационных систем : учебное пособие для среднего профессионального образования

<https://urait.ru/bcode/469958> Информационные технологии в 2 т. Том 2 : учебник для среднего профессионального образования

<https://urait.ru/bcode/470351> Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образов

<https://urait.ru/bcode/469958> Информационные технологии в 2 т. Том 2 : учебник для среднего профессионального образования

<https://urait.ru/bcode/470351> Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образов

<https://urait.ru/bcode/469958> Информационные технологии в 2 т. Том 2 : учебник для среднего профессионального образования

<https://urait.ru/bcode/470351> Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образов

<https://urait.ru/bcode/449548> Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессиона

<https://urait.ru/bcode/470351> Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образов

## **10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине**

Образовательный процесс по дисциплине **Информационная безопасность** предполагает использование следующего программного обеспечения и информационных справочных систем:  
Лекционная аудитория: проектор, экран, компьютер/ноутбук, меловая (и) или маркерная доска.  
Аудитория для практических занятий и текущего контроля: лаборатория информационных ресурсов/ лаборатория вычислительной техники, архитектуры персонального компьютера и периферийных устройств. Оснащение согласно паспорту кабинета/ лаборатории.  
Групповые (индивидуальные) консультации: меловая (и) или маркерная доска.  
Аудитория для самостоятельной работы - помещения Научной библиотеки ПГНИУ: компьютерная техника с возможностью подключения к сети «Интернет», обеспеченная доступом в электронную информационно-образовательную среду университета.

При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ ([student.psu.ru](http://student.psu.ru)).

При организации дистанционной работы и проведении занятий в режиме онлайн могут использоваться:

система видеоконференцсвязи на основе платформы BigBlueButton (<https://bigbluebutton.org/>).

система LMS Moodle (<http://e-learn.psu.ru/>), которая поддерживает возможность использования текстовых материалов и презентаций, аудио- и видеоконтент, а так же тесты, проверяемые задания,

задания для совместной работы.

система тестирования Indigo (<https://indigotech.ru/>).

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

Windows 10

Microsoft Office

Microsoft Access 2016 (в составе пакета Office)

1С Предприятие

Windows Server 2008

Microsoft SQL Server Express

My SQL Server

WPS Office

Dev C++

ABC Pascal

Android Studio

Симулятор сети передачи данных Cisco Packet Tracer

СДО Колледжа профессионального образования

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:

1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

2. Читальный зал гуманитарной литературы, корп. 2, ауд. 418. Оборудован 7 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

3. Читальный зал естественной литературы, корп.6, ауд. 107а. Оборудован 5 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

4. Отдел иностранной литературы, корп.2 ауд. 207. Оборудован 1 персональным компьютером с доступом к локальной и глобальной компьютерным сетям.

5. Библиотека юридического факультета, корп.9, ауд. 4. Оборудована 11 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

6. Читальный зал географического факультета, корп.8, ауд. 419. Оборудован 6 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

Все компьютеры, установленные в помещениях научной библиотеки, оснащены следующим программным обеспечением:

Операционная система ALT Linux;

Офисный пакет Libreoffice.

Справочно-правовая система «КонсультантПлюс»

**Фонды оценочных средств для аттестации по дисциплине  
Информационная безопасность**

**Планируемые результаты обучения по дисциплине для формирования компетенции и  
критерии их оценивания**

<b>Компетенция</b>	<b>Планируемые результаты обучения</b>	<b>Критерии оценивания результатов обучения</b>
<p><b>ОК.1</b> Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам</p>	<p>знать основные средства и методы защиты компьютерных систем программными и аппаратными средствами;</p>	<p align="center"><b>Неудовлетворител</b> не знает основные средства и методы защиты компьютерных систем программными и аппаратными средствами</p> <p align="center"><b>Удовлетворительн</b> фрагментарно знает основные средства и методы защиты компьютерных систем программными и аппаратными средствами</p> <p align="center"><b>Хорошо</b> в целом успешно, но с пробелами знает основные средства и методы защиты компьютерных систем программными и аппаратными средствами</p> <p align="center"><b>Отлично</b> знать основные средства и методы защиты компьютерных систем программными и аппаратными средствами</p>
<p><b>ПК.4.4</b> Обеспечивать защиту программного обеспечения компьютерных систем программными средствами</p>	<p>знать основные средства и методы защиты компьютерных систем программными и аппаратными средствами; уметь использовать методы защиты программного обеспечения компьютерных систем; анализировать риски и характеристики качества программного обеспечения; выбирать и использовать методы и средства защиты компьютерных систем программными и аппаратными средствами</p>	<p align="center"><b>Неудовлетворител</b> не знает основные средства и методы защиты компьютерных систем программными и аппаратными средствами; не умеет использовать методы защиты программного обеспечения компьютерных систем; не умеет анализировать риски и характеристики качества программного обеспечения; не умеет выбирать и использовать методы и средства защиты компьютерных систем программными и аппаратными средствами</p> <p align="center"><b>Удовлетворительн</b> фрагментарно знает основные средства и методы защиты компьютерных систем программными и аппаратными средствами; частично умеет использовать методы защиты программного обеспечения компьютерных систем; допускает грубые ошибки в анализе рисков и характеристиках качества</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p style="text-align: center;"><b>Удовлетворительн</b></p> <p>программного обеспечения.</p> <p style="text-align: center;"><b>Хорошо</b></p> <p>в целом успешно, но с пробелами знает основные средства и методы защиты компьютерных систем программными и аппаратными средствами; с незначительными ошибками умеет использовать методы защиты программного обеспечения компьютерных систем; анализировать риски и характеристики качества программного обеспечения; выбирать и использовать методы и средства защиты компьютерных систем программными и аппаратными средствами</p> <p style="text-align: center;"><b>Отлично</b></p> <p>знать основные средства и методы защиты компьютерных систем программными и аппаратными средствами; уметь использовать методы защиты программного обеспечения компьютерных систем; анализировать риски и характеристики качества программного обеспечения; выбирать и использовать методы и средства защиты компьютерных систем программными и аппаратными средствами</p>

## Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Базовая

**Вид мероприятия промежуточной аттестации :** Экзамен

**Способ проведения мероприятия промежуточной аттестации :** Оценка по дисциплине в рамках промежуточной аттестации определяется на основе баллов, набранных обучающимся на контрольных мероприятиях, проводимых в течение учебного периода.

**Максимальное количество баллов :** 100

### Конвертация баллов в отметки

«отлично» - от 81 до 100

«хорошо» - от 61 до 80

«удовлетворительно» - от 48 до 60

«неудовлетворительно» / «незачтено» менее 48 балла

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<b>Входной контроль</b>	Основные понятия и определения, эволюция подходов к обеспечению информационной безопасности <b>Входное тестирование</b>	знать основные понятия и определения, объекты, цели и задачи защиты информации; знать этапы эволюции подходов к обеспечению информационной безопасности.
<b>ОК.1</b> Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам <b>ПК.4.4</b> Обеспечивать защиту программного обеспечения компьютерных систем программными средствами	Алгоритмы шифрования <b>Защищаемое контрольное мероприятие</b>	Знать понятие угрозы защиты информации, источники угроз, защита от несанкционированного доступа, модели, и основные принципы защиты информации. Угрозы информации в ЭВМ. Классификация угроз и их характеристики. Угроза безопасности информации в компьютерных системах. Основные свойства защищаемой информации. Методы и средства защиты информации от традиционных шпионажей и диверсий. Методы и средства защиты информации от электромагнитных излучений и наводок

<b>Компетенция</b>	<b>Мероприятие текущего контроля</b>	<b>Контролируемые элементы результатов обучения</b>
<b>ОК.1</b> Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	Сертификация ПО <b>Письменное контрольное мероприятие</b>	Безопасность компьютерных сетей. Элементы сети. Возможности угрозы целостности информации сети. Программные и технические средства защиты информации в сети. Программные и технические средства защиты информации в сети. Защита информации в компьютерных сетях. Инженерная защита объектов. Защита информации от утечки по техническим каналам.
<b>ОК.1</b> Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам <b>ПК.4.4</b> Обеспечивать защиту программного обеспечения компьютерных систем программными средствами	Нормативное, организационное и правовое регулирование информационной безопасности в организациях. Политика безопасности <b>Итоговое контрольное мероприятие</b>	Знать основные нормативно-правовые акты в области информационной безопасности. Правовые особенности и структура правового обеспечения безопасности конфиденциальной информации и государственной тайны. Категории конфиденциальной информации и принципы ее защиты.

### **Спецификация мероприятий текущего контроля**

#### **Основные понятия и определения, эволюция подходов к обеспечению информационной безопасности**

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **0**

Проходной балл: **0**

<b>Показатели оценивания</b>	<b>Баллы</b>
полные формулировки основных понятий и определений информационной безопасности	5
характеристика этапов эволюции подходов к обеспечению информационной безопасности	5
полное описание основных объектов защиты информации	5
определение целей и задач защиты информации	5
определение этапов эволюции подходов к обеспечению информационной безопасности	5
классификация основных объектов защиты информации	5

#### **Алгоритмы шифрования**

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**

Проходной балл: **15**

<b>Показатели оценивания</b>	<b>Баллы</b>
100 % правильных ответов на вопросы теста	30
50 % правильных ответов на вопросы теста	20
менее 50 % правильных ответов на вопросы теста	15

### **Сертификация ПО**

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**

Проходной балл: **15**

<b>Показатели оценивания</b>	<b>Баллы</b>
от 90 до 100 % правильных ответов на вопросы теста	30
50 % правильных ответов на вопросы теста	20
менее 50 % правильных ответов на вопросы теста	15

### **Нормативное, организационное и правовое регулирование информационной безопасности в организациях. Политика безопасности**

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**

Проходной балл: **18**

<b>Показатели оценивания</b>	<b>Баллы</b>
Знать нормативную базу, основные определения категории национальной безопасности, классификацию и перечень угроз национальной безопасности. Знать особенности обеспечения информационной безопасности в системе национальной безопасности Российской Федерации. Знать особенности подходов к защите государственной тайны, коммерческой тайны и персональных данных. Знать структуру правового обеспечения информационной безопасности	40
Знать особенности обеспечения информационной безопасности в системе национальной безопасности Российской Федерации. Знать особенности подходов к защите государственной тайны, коммерческой тайны и персональных данных. Знать структуру правового обеспечения информационной безопасности	30
Знать правовую основу ограничения доступа к информации, отнесенной к категории защищенно. Знать правовую основу обеспечения информационной безопасности Российской Федерации	20
Знать структуру правового обеспечения информационной безопасности	18