

**МИНОБРНАУКИ РОССИИ**  
**Федеральное государственное бюджетное образовательное**  
**учреждение высшего образования "Пермский**  
**государственный национальный исследовательский**  
**университет"**

**Колледж профессионального образования**

Авторы-составители: **Серебрякова Наталия Александровна**  
**Бочкарев Алексей Михайлович**

Рабочая программа дисциплины  
**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**  
Код УМК 90897

Утверждено  
Протокол №8  
от «09» апреля 2020 г.

Пермь, 2020

## **1. Наименование дисциплины**

Информационная безопасность

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

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

Направление: **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)

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

#### 4. Объем и содержание дисциплины

<b>Направления 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>	7,8
<b>Объем дисциплины (з.е.)</b>	7
<b>Объем дисциплины (ак.час.)</b>	252
<b>Контактная работа с преподавателем (ак.час.), в том числе:</b>	182
<b>Проведение лекционных занятий</b>	84
<b>Проведение практических занятий, семинаров</b>	98
<b>Самостоятельная работа (ак.час.)</b>	70
<b>Формы текущего контроля</b>	Защищаемое контрольное мероприятие (1) Итоговое контрольное мероприятие (2) Письменное контрольное мероприятие (3)
<b>Формы промежуточной аттестации</b>	Дифференцированный зачет (7 триместр) 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

#### **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 равноуровневого доступа в АИС. Способы защиты. Разграничение и управление доступом к элементам защищаемой информации.

#### **Защита от компьютерных вирусов**

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 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. Криптографические методы защиты.

Модели и системы криптографической защиты информации

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

Правовые основы защиты информации

Правовые и законодательные меры по защите информации

Административные и организационные мероприятия информационной безопасности

## **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 аудиторные 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 ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2020. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // ЭБС Юрайт [сайт]. <https://urait.ru/bcode/451933>
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, 2020. — 238 с. — (Профессиональное образование). — ISBN 978-5-534-03964-1. — Текст : электронный // ЭБС Юрайт [сайт]. <https://urait.ru/bcode/451183>
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 ; ответственный редактор В. В. Трофимов. — перераб. и доп. — Москва : Издательство Юрайт, 2020. — 390 с. — (Профессиональное образование). — ISBN 978-5-534-03966-5. — Текст : электронный // ЭБС Юрайт [сайт]. <https://urait.ru/bcode/451184>
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>



## **9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины**

**<https://fstec.ru>** Стандарты в области защиты информации

## **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:

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

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**

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.

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**

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
<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 style="text-align: center;"><b>Неудовлетворител</b></p> <p>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 style="text-align: center;"><b>Удовлетворительн</b></p> <p>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 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</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<b>Отлично</b> 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

## Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Базовая

**Вид мероприятия промежуточной аттестации :** Дифференцированный зачет

**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 49 до 60

«неудовлетворительно» / «незачтено» менее 49 балла

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<b>ПК.4.4</b> Обеспечивать защиту программного обеспечения компьютерных систем программными средствами	Основные понятия и определения, эволюция подходов к обеспечению информационной безопасности <b>Письменное контрольное мероприятие</b>	знать основные понятия и определения, объекты, цели и задачи защиты информации; знать этапы эволюции подходов к обеспечению информационной безопасности.
<b>ПК.4.4</b> Обеспечивать защиту программного обеспечения компьютерных систем программными средствами	Функции и задачи защиты информации. Методы и системы защиты информации <b>Письменное 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>ПК.4.4</b> Обеспечивать защиту программного обеспечения компьютерных систем программными средствами	Организация безопасности в автоматизированных информационных системах АИС <b>Итоговое контрольное мероприятие</b>	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. Принципы организации равноуровневого доступа в АИС. Принципы организации равноуровневого доступа в АИС. Способы защиты. Разграничение и управление доступом к элементам защищаемой информации. 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.

### **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: **30**

Проходной балл: **15**

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

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

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**

Показатели оценивания	Баллы
100 % правильных ответов на вопросы теста	30
50 % правильных ответов на вопросы теста	15

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

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

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

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

Проходной балл: **19**

Показатели оценивания	Баллы
100 % правильных ответов на вопросы теста	40
50 % правильных ответов на вопросы теста	20

**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 49 до 60

«неудовлетворительно» / «незачтено» менее 49 балла

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<b>ПК.4.4</b> Обеспечивать защиту программного обеспечения компьютерных систем программными средствами	Защита от компьютерных вирусов <b>Письменное контрольное мероприятие</b>	Проблема вирусного заражения программ. Классификация и характеристика вирусов. Вред наносимый информации компьютерными вирусами. Структура современных антивирусных программ и перспективные методы антивирусной защиты. Структура современных антивирусных программ. Методы борьбы с компьютерными вирусами.

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<b>ПК.4.4</b> Обеспечивать защиту программного обеспечения компьютерных систем программными средствами	Защита от утечки информации по техническим причинам <b>Защищаемое 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>ПК.4.4</b> Обеспечивать защиту программного обеспечения компьютерных систем программными средствами	Организационно правовое обеспечение информационной 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

#### Защита от компьютерных вирусов

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**

Показатели оценивания	Баллы
100 % правильных ответов на вопросы теста	30
50 % правильных ответов на вопросы теста	15

#### Защита от утечки информации по техническим причинам

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**

Показатели оценивания	Баллы
Письменная работа соответствует всем требованиям, предъявляемым к рефератам. Тема письменной работы полностью раскрыта, четко выражена авторская позиция, имеются логичные и обоснованные выводы, работа оформлена на высоком уровне. Автор свободно ориентируется в материале, оперирует научной терминологией по рассматриваемой проблеме, может аргументировано отстаивать свою точку зрения и ответить на	30



возникающие вопросы.	
Тема письменной работы в целом раскрыта, прослеживается авторская позиция, сформулированы необходимые выводы; использованы соответствующая основная и дополнительная литература. Автор уверенно ориентируется в материале. Имеются замечания /неточности в части изложения и отдельные недостатки по оформлению работы.	25
Тема письменной работы раскрыта недостаточно полно, использовались только основные источники; имеются ссылки на литературные источники, однако не выражена авторская позиция; выводы не обоснованы; материал изложен непоследовательно, без соответствующей аргументации и необходимого анализа. Имеются недостатки в оформлении.	15

### **Организационно правовое обеспечение информационной 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: **19**

<b>Показатели оценивания</b>	<b>Баллы</b>
Знать нормативную базу, основные определения категории национальной безопасности, классификацию и перечень угроз национальной безопасности	10
Знать понятия информации как объекта защиты, юридические аспекты оборота информации	5
Знать правовую основу обеспечения информационной безопасности Российской Федерации	5
Знать правовую основу ограничения доступа к информации, отнесенной к категории защищенной	5
Знать структуру правового обеспечения информационной безопасности	5
Знать особенности обеспечения информационной безопасности в системе национальной безопасности Российской Федерации	5
Знать особенности подходов к защите государственной тайны, коммерческой тайны и персональных данных	5