ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

*Утверждено:*
на заседании кафедры
протокол№ 8 от « 24 » февраля 2021 г.
Зав. кафедрой _____ /Исмагилова А.С.

Согласовано:
Председатель УМК института
_____ / Гильмутдинова Р.А.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

Дисциплина
**Информационная безопасность операционных систем**

Обязательная часть (Б1.О.10)

**программа магистратуры**

Направление подготовки
10.04.01 Информационная безопасность

Направленность (профиль) подготовки
Информационная безопасность цифровых технологий

Квалификация
магистр

| | |
|---|---|
| Разработчик (составитель)<br>Старший преподаватель | _____ / Салов И.В. |

Для приема: 2021 г.

Уфа 2021 г.

Составитель: Салов Игорь Владимирович

Рабочая программа дисциплины *утверждена* на заседании кафедры протокол от «_24_» _февраля_____ 2021 г. № _8_

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании
кафедры_____
_____
_____,
протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой / Исмагилова А.С. /

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании
кафедры_____
_____
_____,
протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой _____/ Исмагилова А.С. /

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры
_____
_____
_____,
протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой _____/ _____Ф.И.О./

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры
_____
_____
_____,
протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой _____/ _____Ф.И.О./

**Список документов и материалов**

## 1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

По итогам освоения дисциплины обучающийся должен достичь следующих результатов обучения:

| **Категория (группа) компетенций** (при наличии ОПК) | **Формируемая компетенция (с указанием кода)** | **Код и наименование индикатора достижения компетенции** | **Результаты обучения по дисциплине** |
|---|---|---|---|
| | ПК-1. Способен проводить предпроектное обследование служебной деятельности и информационных потребностей автоматизируемых подразделений. | ПК-1.1 Знает методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений. | Знать методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений. |
| | | ПК-1.2 Знает методы проведения предпроектного обследования информационных потребностей автоматизируемых подразделений. | Знать методы проведения предпроектного обследования информационных потребностей автоматизируемых подразделений. |
| | | ПК-1.3 Умеет применять основные методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений. | Уметь применять основные методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений. |
| | | ПК-1.4 Умеет применять основные методы проведения предпроектного обследования информационных потребностей автоматизируемых подразделений. | Уметь применять основные методы проведения предпроектного обследования информационных потребностей автоматизируемых подразделений. |
| | | ПК-1.5. Владеет навыками проведения предпроектного | Владеть навыками проведения предпроектного |

| | | | |
|---|---|---|---|
| | | обследования служебной деятельности и информационных потребностей автоматизируемых подразделений. | обследования служебной деятельности и информационных потребностей автоматизируемых подразделений. |
| | | ПК-1.6 Владеет навыками проведения предпроектного обследования информационных потребностей автоматизируемых подразделений. | Владеть навыками проведения предпроектного обследования информационных потребностей автоматизируемых подразделений. |
| | ПК-2. Способен разрабатывать проектные решения по защите информации в автоматизированных системах. | ПК-2.1. Знает основные методы разработки проектных решений по защите информации в автоматизированных системах. | Знать основные методы разработки проектных решений по защите информации в автоматизированных системах. |
| | | ПК-2.2. Знает методы информационно-аналитической деятельности и моделирования процессов для разработки проектных решений по защите информации в автоматизированных системах. | Знать методы информационно-аналитической деятельности и моделирования процессов для разработки проектных решений по защите информации в автоматизированных системах. |
| | | ПК-2.3. Знает технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах. | Знать технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах. |
| | | ПК-2.4. Умеет применять основные методы и технологии разработки проектных решений по защите информации в автоматизированных системах. | Уметь применять основные методы и технологии разработки проектных решений по защите информации в автоматизированных системах. |
| | | ПК-2.5. Умеет применять методы информационно-аналитической деятельности для разработки проектных решений по защите информации в | Уметь применять методы информационно-аналитической деятельности для разработки проектных решений по защите информации в |

| | | | |
|---|---|---|---|
| | | автоматизированных системах. | автоматизированных системах. |
| | | ПК-2.6. Умеет применять технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах. | Уметь применять технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах. |
| | | ПК-2.7. Способен участвовать в разработке проектных решений по защите информации в автоматизированных системах. | Владеть способностью участвовать в разработке проектных решений по защите информации в автоматизированных системах. |
| | | ПК-2.8. Имеет навыки применения методов информационно-аналитической деятельности, методов моделирования процессов и систем защиты информации для разработки проектных решений по защите информации в автоматизированных системах. | Владеть навыками применения методов информационно-аналитической деятельности, методов моделирования процессов и систем защиты информации для разработки проектных решений по защите информации в автоматизированных системах. |
| | | ПК-2.9. Имеет навыки разработки проектных решений по защите информации в автоматизированных системах. | Владеть навыками разработки проектных решений по защите информации в автоматизированных системах. |
| | | ПК-2.10. Имеет навыки применения технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах. | Владеть навыками применения технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах. |

## 2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Аттестация объектов информатизации по требованиям безопасности» относится к части, формируемой участниками образовательных отношений, дисциплинам по выбору.

Дисциплина изучается на 2 курсе магистратуры в 3 семестре.

Целью учебной дисциплины «Аттестация объектов информатизации по требованиям безопасности» является формирование навыков проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений, разработки проектных решений по защите информации в автоматизированных системах.

## 3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)

Содержание рабочей программы представлено в Приложении № 1.

## 4. Фонд оценочных средств по дисциплине

### 4.1. Перечень компетенций и индикаторов достижения компетенций с указанием соотнесенных с ними запланированных результатов обучения по дисциплине. Описание критериев и шкал оценивания результатов обучения по дисциплине.

**ПК-1.** Способен проводить предпроектное обследование служебной деятельности и информационных потребностей автоматизируемых подразделений.

| **Код и наименование индикатора достижения компетенции** | **Результаты обучения по дисциплине** | Критерии оценивания результатов обучения | | | |
|---|---|---|---|---|---|
| | | 2 («Не удовлетворительно») | 3 («Удовлетворительно») | 4 («Хорошо») | 5 («Отлично») |
| ПК-1.1 Знает методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений. | Знать методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений. | Не знает или показывает очень слабые знания. | Знает основные методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений, но допускает ошибки при их применении. | Знает основные методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений. | Знает методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений. |
| ПК-1.2 Знает | Знать методы | Не умеет. | Знает основные | Знает основные | Знает методы |

| | | | | | |
|---|---|---|---|---|---|
| методы проведения предпроектного обследования информационных потребностей автоматизируемых подразделений. | проведения предпроектного обследования информационных потребностей автоматизируемых подразделений. | | методы проведения предпроектного обследования информационных потребностей автоматизируемых подразделений, но допускает ошибки при их применении. | методы проведения предпроектного обследования информационных потребностей автоматизируемых подразделений. | проведения предпроектного обследования информационных потребностей автоматизируемых подразделений. |
| ПК-1.3 Умеет применять основные методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений. | Уметь применять основные методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений. | Не владеет. | Умеет применять некоторые основные методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений, но допускает ошибки при их применении. | Умеет применять некоторые основные методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений. | Умеет применять основные методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений. |
| ПК-1.4 Умеет применять основные методы проведения предпроектного обследования информационных | Уметь применять основные методы проведения предпроектного обследования | Не умеет. | Умеет применять некоторые основные | Умеет применять некоторые основные | Умеет применять основные методы проведен |

| | | | | | |
|---|---|---|---|---|---|
| потребностей автоматизируемых подразделений. | информационных потребностей автоматизируемых подразделений. | | методы проведения предпроектного обследования информационных потребностей автоматизируемых подразделений, но допускает ошибки при их использовании. | методы проведения предпроектного обследования информационных потребностей автоматизируемых подразделений. | ия предпроектного обследования информационных потребностей автоматизируемых подразделений. |
| ПК-1.5. Владеет навыками проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений. | Владеть навыками проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений. | Не владеет. | Владеет основными навыками проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений, но допускает ошибки при их использовании. | Владеет основными навыками проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений. | Владеет навыками проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений. |
| ПК-1.6 Владеет навыками проведения предпроектного обследования информационных потребностей автоматизируемых подразделений. | Владеть навыками проведения предпроектного обследования информационных потребностей | Не владеет. | Владеет основными навыками проведения предпрое | Владеет основными навыками проведения предпрое | Владеет навыками проведения предпроектного обследов |

| | | | | | |
|---|---|---|---|---|---|
| | автоматизируемых подразделений. | | ктного обследования информационных потребностей автоматизируемых подразделений, но допускает ошибки при их использовании. | ктного обследования информационных потребностей автоматизируемых подразделений. | ания информационных потребностей автоматизируемых подразделений. |

**ПК-2.** Способен разрабатывать проектные решения по защите информации в автоматизированных системах.

| **Код и наименование индикатора достижения компетенции** | **Результаты обучения по дисциплине** | Критерии оценивания результатов обучения | | | |
|---|---|---|---|---|---|
| | | 2 («Неудовлетворительно») | 3 («Удовлетворительно») | 4 («Хорошо») | 5 («Отлично») |
| ПК-2.1. Знает основные методы разработки проектных решений по защите информации в автоматизированных системах. | Знать основные методы разработки проектных решений по защите информации в автоматизированных системах. | Не знает или показывает очень слабые знания. | Знает некоторые основные методы разработки проектных решений по защите информации в автоматизированных системах, но допускает ошибки при их использовании. | Знает некоторые основные методы разработки проектных решений по защите информации в автоматизированных системах. | Знает основные методы разработки проектных решений по защите информации в автоматизированных системах. |
| ПК-2.2. Знает методы информационно-аналитической деятельности и моделирования процессов для разработки проектных | Знать методы информационно-аналитической деятельности и моделирования процессов для разработки | Не знает или показывает очень слабые знания. | Знает основные методы информационно-аналитической | Знает основные методы информационно-аналитической | Знает методы информационно-аналитической деятельнос |

| | | | | | |
|---|---|---|---|---|---|
| решений по защите информации в автоматизированных системах. | проектных решений по защите информации в автоматизированных системах. | | деятельности и моделирования процессов для разработки проектных решений по защите информации в автоматизированных системах, но допускает ошибки при их использовании. | деятельности и моделирования процессов для разработки проектных решений по защите информации в автоматизированных системах. | ти и моделирования процессов для разработки проектных решений по защите информации в автоматизированных системах. |
| ПК-2.3. Знает технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах. | Знать технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах. | Не знает или показывает очень слабые знания. | Знает основные технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах, но допускает ошибки при их использовании. | Знает основные технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах. | Знает технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах. |

| | | | | | |
|---|---|---|---|---|---|
| ПК-2.4. Умеет применять основные методы и технологии разработки проектных решений по защите информации в автоматизированных системах. | Уметь применять основные методы и технологии разработки проектных решений по защите информации в автоматизированных системах. | Не умеет. | Умеет применять некоторые основные методы и технологии разработки проектных решений по защите информации в автоматизированных системах, но допускает ошибки при их использовании. | Умеет применять некоторые основные методы и технологии разработки проектных решений по защите информации в автоматизированных системах. | Умеет применять основные методы и технологии разработки проектных решений по защите информации в автоматизированных системах. |
| ПК-2.5. Умеет применять методы информационно-аналитической деятельности для разработки проектных решений по защите информации в автоматизированных системах. | Уметь применять методы информационно-аналитической деятельности для разработки проектных решений по защите информации в автоматизированных системах. | Не умеет. | Умеет применять основные методы информационно-аналитической деятельности для разработки проектных решений по защите информации в автоматизированных системах, но допускает ошибки при их использовании. | Умеет применять основные методы информационно-аналитической деятельности для разработки проектных решений по защите информации в автоматизированных системах. | Умеет применять методы информационно-аналитической деятельности для разработки проектных решений по защите информации в автоматизированных системах. |

| | | | | | |
|---|---|---|---|---|---|
| ПК-2.6. Умеет применять технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах. | Уметь применять технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах. | Не умеет. | Умеет применять основные технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах, но допускает ошибки при их использовании. | Умеет применять основные технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах. | Умеет применять технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах. |
| ПК-2.7. Способен участвовать в разработке проектных решений по защите информации в автоматизированных системах. | Владеть способностью участвовать в разработке проектных решений по защите информации в автоматизированных системах. | Не владеет. | Способен участвовать в некоторых этапах разработки проектных решений по защите информации в автоматизированных системах, но допускает при этом ошибки. | Способен участвовать в некоторых этапах разработки проектных решений по защите информации в автоматизированных системах. | Способен участвовать в разработке проектных решений по защите информации в автоматизированных системах. |

| | | | | | |
|---|---|---|---|---|---|
| ПК-2.8. Имеет навыки применения методов информационно-аналитической деятельности, методов моделирования процессов и систем защиты информации для разработки проектных решений по защите информации в автоматизированных системах. | Владеть навыками применения методов информационно-аналитической деятельности, методов моделирования процессов и систем защиты информации для разработки проектных решений по защите информации в автоматизированных системах. | Не владеет. | Имеет основные навыки применения методов информационно-аналитической деятельности, методов моделирования процессов и систем защиты информации для разработки проектных решений по защите информации в автоматизированных системах, но допускает ошибки при их использовании. | Имеет основные навыки применения методов информационно-аналитической деятельности, методов моделирования процессов и систем защиты информации для разработки проектных решений по защите информации в автоматизированных системах. | Имеет навыки применения методов информационно-аналитической деятельности, методов моделирования процессов и систем защиты информации для разработки проектных решений по защите информации в автоматизированных системах. |
| ПК-2.9. Имеет навыки разработки проектных решений по защите информации в автоматизированных системах. | Владеть навыками разработки проектных решений по защите информации в автоматизированных системах. | Не владеет. | Имеет основные навыки разработки проектных решений по защите информации в автоматизированных системах, но допускае | Имеет основные навыки разработки проектных решений по защите информации в автоматизированных системах. | Имеет навыки разработки проектных решений по защите информации в автоматизированных системах. |

| | | | | | |
|---|---|---|---|---|---|
| | | | т при этом ошибки. | | |
| ПК-2.10. Имеет навыки применения технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах. | Владеть навыками применения технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах. | Не владеет. | Имеет основные навыки применения технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах, но допускает ошибки при их применении. | Имеет основные навыки применения технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах. | Имеет навыки применения технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах. |

### 4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине

**ПК-1.** Способен проводить предпроектное обследование служебной деятельности и информационных потребностей автоматизируемых подразделений.

| Код и наименование индикатора достижения компетенции | Результаты обучения по дисциплине | Оценочные средства |
|---|---|---|
| ПК-1.1 Знает методы проведения предпроектного обследования служебной деятельности и | Знать методы проведения предпроектного обследования служебной деятельности и | тестирование, практическое задание; лабораторная работа |

| | | |
|---|---|---|
| информационных потребностей автоматизируемых подразделений. | информационных потребностей автоматизируемых подразделений. | |
| ПК-1.2 Знает методы проведения предпроектного обследования информационных потребностей автоматизируемых подразделений. | Знать методы проведения предпроектного обследования информационных потребностей автоматизируемых подразделений. | тестирование, практическое задание; лабораторная работа |
| ПК-1.3 Умеет применять основные методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений. | Уметь применять основные методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений. | тестирование, практическое задание; лабораторная работа |
| ПК-1.4 Умеет применять основные методы проведения предпроектного обследования информационных потребностей автоматизируемых подразделений. | Уметь применять основные методы проведения предпроектного обследования информационных потребностей автоматизируемых подразделений. | тестирование, практическое задание; лабораторная работа |
| ПК-1.5. Владеет навыками проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений. | Владеть навыками проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений. | тестирование, практическое задание; лабораторная работа |
| ПК-1.6 Владеет навыками проведения предпроектного обследования информационных потребностей автоматизируемых подразделений. | Владеть навыками проведения предпроектного обследования информационных потребностей автоматизируемых подразделений. | тестирование, практическое задание; лабораторная работа |

**ПК-2.** Способен разрабатывать проектные решения по защите информации в автоматизированных системах.

| **Код и наименование индикатора достижения компетенции** | **Результаты обучения по дисциплине** | **Оценочные средства** |
|---|---|---|
| ПК-2.1. Знает основные методы разработки проектных решений по | Знать основные методы разработки проектных решений по защите информации в | тестирование, практическое задание; лабораторная работа |

| | | |
|---|---|---|
| защите информации в автоматизированных системах. | автоматизированных системах. | |
| ПК-2.2. Знает методы информационно-аналитической деятельности и моделирования процессов для разработки проектных решений по защите информации в автоматизированных системах. | Знать методы информационно-аналитической деятельности и моделирования процессов для разработки проектных решений по защите информации в автоматизированных системах. | тестирование, практическое задание; лабораторная работа |
| ПК-2.3. Знает технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах. | Знать технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах. | тестирование, практическое задание; лабораторная работа |
| ПК-2.4. Умеет применять основные методы и технологии разработки проектных решений по защите информации в автоматизированных системах. | Уметь применять основные методы и технологии разработки проектных решений по защите информации в автоматизированных системах. | тестирование, практическое задание; лабораторная работа |
| ПК-2.5. Умеет применять методы информационно-аналитической деятельности для разработки проектных решений по защите информации в автоматизированных системах. | Уметь применять методы информационно-аналитической деятельности для разработки проектных решений по защите информации в автоматизированных системах. | тестирование, практическое задание; лабораторная работа |
| ПК-2.6. Умеет применять технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах. | Уметь применять технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах. | тестирование, практическое задание; лабораторная работа |
| ПК-2.7. Способен участвовать в разработке проектных решений по защите информации в автоматизированных системах. | Владеть способностью участвовать в разработке проектных решений по защите информации в автоматизированных системах. | тестирование, практическое задание; лабораторная работа |
| ПК-2.8. Имеет навыки применения методов информационно-аналитической деятельности, методов моделирования процессов и систем защиты | Владеть навыками применения методов информационно-аналитической деятельности, методов моделирования процессов и систем защиты информации для разработки | тестирование, практическое задание; лабораторная работа |

| | | |
|---|---|---|
| информации для разработки проектных решений по защите информации в автоматизированных системах. | проектных решений по защите информации в автоматизированных системах. | |
| ПК-2.9. Имеет навыки разработки проектных решений по защите информации в автоматизированных системах. | Владеть навыками разработки проектных решений по защите информации в автоматизированных системах. | тестирование, практическое задание; лабораторная работа |
| ПК-2.10. Имеет навыки применения технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах. | Владеть навыками применения технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах. | тестирование, практическое задание; лабораторная работа |

Критериями оценивания при модульно-рейтинговой системе являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины (для экзамена: текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10; для зачета: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).
Шкалы оценивания:

(для экзамена:

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;

от 80 баллов – «отлично».

для зачета:

зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),

не зачтено – от 0 до 59 рейтинговых баллов).

**Рейтинг – план дисциплины**
**«Информационная безопасность операционных систем»**

Специальность: 10.04.01 Информационная безопасность

курс 2, семестр 3

| Виды учебной деятельности студентов | Балл за конкретное задание | Число заданий за семестр | Баллы | |
|---|---|---|---|---|
| | | | Минимальный | Максимальный |
| Модуль 1. Архитектура операционных систем. | | | | |
| Текущий контроль | | | | |
| Лабораторная работа | 4 | 4 | 0 | 16 |
| Практическая работа | 4 | 4 | 0 | 16 |
| Рубежный контроль | | | | |

| | | | | |
|---|---|---|---|---|
| Тест | 8 | 1 | 0 | 8 |
| Всего | | | 0 | 40 |
| Модуль 2. Защита информации в современных операционных системах. | | | | |
| Текущий контроль | | | | |
| Лабораторная работа | 3 | 4 | 0 | 12 |
| Практическая работа | 3 | 4 | 0 | 12 |
| Рубежный контроль | | | | |
| Тест | 6 | 1 | 0 | 6 |
| Всего | | | 0 | 30 |
| Поощрительные баллы | | | | |
| 1. Участие в студенческой олимпиаде по дисциплине | 3 | 1 | 0 | 3 |
| 2.Публикация научной статьи | 4 | 1 | 0 | 4 |
| 3.Участие в научно-практической конференции по профилю | 3 | 1 | 0 | 3 |
| Всего | | 3 | 0 | 10 |
| Посещаемость (баллы вычитаются из общей суммы набранных баллов) | | | | |
| 1. Посещение лекционных занятий | | | 0 | -6 |
| 2. Посещение практических (семинарских, лабораторных занятий) | | | 0 | -10 |
| | | | | |
| Итоговый контроль | | | | |
| 1.Экзамен | 30 | 1 | 0 | 30 |

**Экзамен**

Структура экзаменационного билета

Экзаменационный билет состоит из двух вопросов, отражающих соответственно материал первого и второго модуля.

Экзаменационные материалы

1. Функции и структура операционной системы (аппаратные средства, процессы, файловая система, память и пр.).
2. Классификация операционных систем (ОС).
3. Технологии построения ядра ОС (монолитный и микроядерный подходы).
4. Модели организация оперативной памяти.
5. Страничная организация виртуальной памяти.
6. Сегментная организация виртуальной памяти.
7. Защита памяти и контроль доступа.
8. Файловая система: функции и организация хранения данных, физический уровень.
9. Способы адресация объектов файловой системы. Абсолютный и относительный пути.
10. Операции манипулирования объектами файловых систем.
11. Операции доступа к данным в файловых системах.
12. Файловые дескрипторы и потоки.
13. Структура файловой системы ОС UNIX (стандарт FHS).
14. Внутренняя структура файловой системы ОС UNIX на основе i-node.
15. Символьные и жесткие ссылки: назначение, команды, различия.
16. Обобщение понятия файла. Устройства.
17. Символьные и блочные устройства: различия, примеры.
18. Идентификация и монтирование дисковых разделов (привести примеры).

19. Виртуальные устройства (привести примеры).
20. Пользователи и группы. Идентификаторы UID и GID.
21. Суперпользователь root: особенности и привилегии.
22. Учетные записи пользователей и групп и связанные с ними системные файлы.
23. Классическая дискреционная система прав доступа: режим доступа на основе базовых 9 бит.
24. Классическая дискреционная система прав доступа: дополнительные 3 бита (SetUID, SetGID, Sticky bit).
25. Режим доступа по умолчанию.
26. Понятие процесса. Режимы и состояния процесса.
27. Контекст процесса.
28. Создание и завершение процесса.
29. Синхронизация выполнения родительского и дочернего процессов.
30. Переменные окружения (привести перечень основных переменных).
31. Типы процессов.
32. Приоритет процессов.
33. Обзор средств взаимодействия процессов с приведением круга решаемых задач.
34. Механизм сигналов.
35. Перечень основных сигналов.
36. Стандартные потоки ввода-вывода и неименованные каналы. Привести примеры конвейерной обработки.
37. Средства межпроцессного взаимодействия: именованные каналы.
38. Средства межпроцессного взаимодействия: сокеты.
39. Средства межпроцессного взаимодействия: семафоры, очереди сообщений, разделяемая память.
40. Командная оболочка как основной интерфейс пользователя.
41. Алфавитно-цифровые терминалы.
42. Удаленный сетевой доступ. Протоколы.
43. Графическая система X Window: принцип построения.
44. Терминалы типа Тонкий клиент?
45. Этапы загрузки и инициализации ОС.
46. Функции процесса init и связанные с ним системные файлы.
47. Уровни выполнения. Команды изменения уровня выполнения.
48. Распределение функций по обеспечению безопасности автоматизированных систем.
49. Организационно-распорядительные документы по обеспечению безопасности автоматизированных систем.
50. Обязанности пользователей и ответственных за обеспечение информационной безопасности в подразделениях
51. Проблема человеческого фактора.
52. Общие правила обеспечения безопасности.
53. Обязанности ответственного за обеспечение безопасности информации в подразделении.
54. Ответственность за нарушения требований обеспечения безопасности.
55. Порядок работы с носителями ключевой информации.
56. Регламентация работ по обеспечению безопасности автоматизированных систем
57. Регламентация правил парольной и антивирусной защиты.
58. Регламентация порядка допуска к работе и изменения полномочий пользователей автоматизированной системы.
59. Регламентация порядка изменения конфигурации аппаратно-программных средств автоматизированной системы.

60. Регламентация процессов разработки, испытания, опытной эксплуатации, внедрения и сопровождения задач.
61. Категорирование и документирование защищаемых ресурсов ....
62. Определение градаций важности и соответствующих уровней обеспечения защиты ресурсов.
63. Категорирование защищаемых ресурсов.
64. Проведение информационных обследований и документирование защищаемых ресурсов.
65. Концепция информационной безопасности. Планы защиты и обеспечения непрерывной работы и восстановления подсистем автоматизированной системы.
66. Концепция информационной безопасности организации.
67. План защиты информации.
68. План обеспечения непрерывной работы и восстановления подсистем автоматизированной системы.
69. Назначение и возможности средств защиты информации от несанкционированного доступа.
70. Основные механизмы защиты автоматизированных систем.
71. Защита периметра компьютерных сетей и управление механизмами защиты.
72. Страхование информационных рисков.
73. Аппаратно-программные средства защиты информации от несанкционированного доступа.
74. Рекомендации по выбору средств защиты информации от несанкционированного доступа.
75. Обзор существующих на рынке средств защиты информации от несанкционированного доступа.
76. Средства аппаратной поддержки.
77. Способы аутентификации.
78. Применение штатных и дополнительных средств защиты информации от несанкционированного доступа
79. Стратегия безопасности Microsoft.
80. Защита от вмешательства в процесс нормального функционирования автоматизированной системы.
81. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы.
82. Оперативное оповещение о зарегистрированных попытках несанкционированного доступа.
83. Защита данных от несанкционированной модификации, копирования и перехвата средствами шифрования.
84. Обеспечение безопасности компьютерных сетей.
85. Проблемы обеспечения безопасности в компьютерных сетях.
86. Типовая корпоративная сеть.
87. Уровни информационной инфраструктуры корпоративной сети.
88. Уязвимости и их классификация.
89. Классификация атак.
90. Средства защиты сетей.
91. Защита периметра корпоративной сети.
92. Угрозы, связанные с периметром корпоративной сети.
93. Составляющие защиты периметра.
94. Межсетевые экраны.
95. Анализ содержимого почтового и веб-трафика.
96. Виртуальные частные сети.
97. Обнаружение и устранение уязвимостей. Возможности сканеров безопасности.

98. Управление уязвимостями.
99. Архитектура систем управления уязвимостями.
100. Особенности сетевых агентов сканирования.
101. Средства анализа защищенности системного уровня.
102. Мониторинг событий безопасности
103. Введение в управление журналами событий.
104. Категории журналов событий.
105. Инфраструктура управления журналами событий.
106. Введение в технологию обнаружения атак.
107. Классификация систем обнаружения атак.

Пример экзаменационного билета:

Форма 1.4.-33

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ
КАФЕДРА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Специальность 10.04.01 Информационная безопасность

Дисциплина Информационная безопасность операционных систем

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1.Технологии построения ядра ОС (монолитный и микроядерный подходы).
2. Основные механизмы защиты автоматизированных систем.

Зав. Кафедрой УИБ А.С. Исмагилова

Кафедра управления информационной безопасностью

Критерии оценивания результатов экзамена для ОФО:

Критерии оценки (в баллах):

- 25-30 баллов выставляется студенту, если студент дал полные, развернутые ответы на все теоретические вопросы билета, продемонстрировал знание терминологии, основных понятий, умение применять теоретические знания при выполнении практических заданий. Студент без затруднений ответил на все дополнительные вопросы.

- 17-24 баллов выставляется студенту, если студент раскрыл в основном теоретические вопросы, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности.

- 10-16 баллов выставляется студенту, если при ответе на теоретические вопросы студентом допущено несколько существенных ошибок в толковании основных понятий. Логика и полнота ответа страдают заметными изъянами. Заметны пробелы в знании основных методов. Теоретические вопросы в целом изложены достаточно, но с пропусками материала. Имеются принципиальные ошибки в логике построения ответа на вопрос.

- 1-10 баллов выставляется студенту, если ответ на теоретические вопросы свидетельствует о непонимании и крайне неполном знании основных понятий и методов.

Обнаруживается отсутствие навыков применения теоретических знаний при выполнении практических заданий. Студент не смог ответить ни на один дополнительный вопрос.

Устанавливается следующая градация перевода оценки из многобалльной в четырехбалльную:

Экзамены:

- отлично – от 80 до 110 баллов (включая 10 поощрительных баллов),
- хорошо – от 60 до 79 баллов,
- удовлетворительно – от 45 до 59 баллов,
- неудовлетворительно – менее 45 баллов.

## Примерная тематика курсовых проектов (работ)

Курсовое проектирование не предусмотрено

## Тестовые задания

При изучении дисциплины используются тестовые задания закрытого типа. Каждое тестовое задание включает вопрос и варианты ответов к нему. Тестирование выполняется в письменной форме.
Необходимо выбрать один ответ из предложенных вариантов.

### Модуль 1. Архитектура операционных систем.

1.Многозадачность на основе режима разделения времени называется …
1.Независимой
**2.Вытесняющей**
3.Совместной
4.Кооперативной
5.Невытесняющей

2.Некоторое число (номер) в диапазоне 0-255,указывающее на одну из 256 программ обработки прерываний, адреса которых хранятся в таблице прерываний, называется … прерывания (ий)
1.Адресом
**2.Вектором**
3.Адресом обработчика
4.Номером
5.Номером обработчика

3.Для упорядочивания работы обработчиков прерываний в ОС применяется механизм:
1.Очередей без приоритета
2.Очередей реального времени
**3.Приоритетных очередей**

4.Возможность интерактивного взаимодействия пользователя и программы возникает с появлением:
1.Мультипрограммных вычислительных систем
2.Систем пакетной обработки
**3.Систем разделения времени**

5.Способ реализации системных вызовов зависит от структурной организации ОС, связанной с особенностями:
1.Оперативной памяти
2.Внешней памяти
**3.Обработки прерываний**

4.Приоритетного обслуживания
5.Аппаратной платформы

6.Устройствам, которые используют векторные прерывания, назначается:
1.Приоритет прерывания
2.Драйвер
**3.Вектор прерываний**
4.Диспетчер прерывания
5.Процедура обработки прерывания

7.Выберите верные утверждения:
**1.Дескриптор процесса содержит необходимую ядру информацию о процессе, не зависимо от того, находится ли образ процесса в оперативной памяти или выгружен на диск. К этой информации можно отнести состояние процесса, значения приоритета и идентификатор пользователя, создавшего процесс**
2.Дескриптор процесса содержит необходимую ядру информацию о процессе для возобновления его выполнения с прерванного места. К этой информации можно отнести содержимое регистров процессора, описатели открытых данным процессом файлов

8.Как правило, повышать приоритеты потоков в системе (в определенных пределах) могут:
1.Разработчики программ
2.Некоторые пользователи
**3.Администраторы**
4.Все
5.Все пользователи

9.Синхронизация потоков заключается:
1.В согласованном доступе к аппаратным средствам
2.В согласованном выполнении системных вызовов этими потоками
**3.В согласовании их скоростей путем приостановки потоков**

10.Программный модуль ОС, ответственный за чтение отдельных команд или их последовательности из командного файла, называют командным ...
**1.Интерпретатором**
2. Компилятором
3. Экстрактором
4. Семафором

11.Примеры необходимости прерываний в работе мультипрограммной ОС:
1.В оперативной памяти отсутствуют данные, необходимые активной задаче
**2.Загружена новая задача**
3.Более приоритетной задаче требуется процессор
4.Произошло событие
**5.Менее приоритетной задаче требуется процессор**

12.Если код ОС написан так, что дополнения и изменения могут вноситься без нарушения целостности системы, то такую ОС называют…
**1.Расширяемой**
2.Обновляемой
3.Структуризированной
4.Независимой
5.Дополняемой

13.В ОС имеются подсистемы управления:
1.Устройствами ввода-вывода
**2.Потоками**
**3.Файлами**
4.Прерываниями
**5.Памятью**
6.Процессами
**7.Заданиями**

14.Обработчики прерываний принадлежат:

1.Конкретному процессу
2.Планировщику
3.Диспетчеру
4.Конкретному потоку
**5.ОС**

15.Процессорное время выделяется:

**1.Потокам**
2.Процессам
3.Процессам, а затем перераспределяется между потоками этих процессов
4.Процессам и потокам

16.Способ организации вычислительного процесса в системах с несколькими процессорами называется:

1.Мультизадачная обработка
2.Мультипроцессная обработка
**3.Мультипроцессорная обработка**
4.Мультипрограммная обработка

17.Для надежного управления выполнением приложений, а также распределения ресурсов вычислительной машины, ОС должна обладать определенными привилегиями по отношению к пользовательским приложениям. Это достигается:

**1.Совместно программными и аппаратными средствами**
2.Программными средствами ОС
3.Аппаратными средствами вычислительной машины

18.В ОС Unix новый процесс можно создать, используя:

1.командуу CMD CreateProcess
2.библиотеку WIn32API NewProcess
3. прерывание Sleep
**4. системный вызов Fork**

19.Фиксация определенных событий в ОС называется:

1.Логическим входом
2.Аутентификацией
3.Легализацией
4.Авторизацией
**5.Аудитом**

20.В большинстве случаев ОС присваивает приоритеты потокам:

1.Случайным образом
2.В зависимости от обстоятельств
3.По решению пользователя
4.По решению администратора
**5.По умолчанию**

21.Функции аудита ОС заключаются в:

**1.Фиксации всех событий, от которых зависит безопасность**
2.Контроле действий процессов на доступ к системным ресурсам
3.Запрещении пользователям определенных действий, указанных администратором
4.Проверке прав пользователя на доступ к ОС

22.Posix – это:

1.Название ОС
2.Название архитектуры вычислительной машины
**3.Совокупность стандартов, используемых в ОС Unix**
4.Модуль ядра ОС Unix, работающий в пользовательском режиме

23.Одно из требований к современной ОС – расширяемость – означает:

1.Возможность добавления драйверов новых устройств при перекомпиляции ядра ОС

**2.Возможность внесения изменений и дополнений в операционную систему без нарушения целостности системы**

3.Возможность объединения двух и более ОС для совместной работы

4.Возможность совместной работы двух и более процессоров

24.Одно из требований к современной ОС – переносимость – означает:

**1.Код ОС должен легко переноситься с процессора одного типа на процессор другого типа**

2.Наличие в ОС средств для выполнения приложений, написанных для других ОС

25.Всякий потребляемый, полезный для потребителя объект(независимо от формы его существования), в терминах ОС является:

1.Мьютексом

2.Событием

3.Потоком

**4.Ресурсом**

## Модуль 2. Защита информации в современных операционных системах.

1. Защита исполняемых файлов обеспечивается

**а) обязательным контролем попытки запуска**

б) криптографией

в) специальным режимом запуска

г) дополнительным хостом

2. Защита от форматирования жесткого диска со стороны пользователей обеспечивается

**а) аппаратным модулем, устанавливаемым на системную шину ПК**

б) системным программным обеспечением

в) специальным программным обеспечением

г) аппаратным модулем, устанавливаемым на контроллер

3. Из перечисленного ACL-список содержит:

**а) срок действия маркера доступа;**

б) домены, которым разрешен доступ к объекту;

в) операции, которые разрешены с каждым объектом;

**г) тип доступа**

4. Из перечисленного базовыми услугами для обеспечения безопасности компьютерных систем и сетей являются:

**а) аутентификация;**

б) идентификация;

**в) целостность;**

**г) контроль доступа;**

д) контроль трафика;

**е) причастность**

5. Из перечисленного в обязанности сотрудников группы информационной безопасности входят:

**а) управление доступом пользователей к данным;**

**б) расследование причин нарушения защиты;**

в) исправление ошибок в программном обеспечении;

д) устранение дефектов аппаратной части

6. Из перечисленного в ОС UNIX существуют администраторы:

**а) системных утилит;**

б) службы контроля;

**в) службы аутентификации;**

г) тиражирования;

**д) печати;**

**е) аудита**

7. Из перечисленного в файловых системах ОС UNIX права доступа к файлу определяются для:

**а) владельца;**
**б) членов группы владельца;**
в) конкретных заданных пользователей;
г) конкретных заданных групп пользователей;
**д) всех основных пользователей**

8. Из перечисленного для аутентификации по отпечаткам пальцев терминальных пользователей используются методы:

а) сравнение отдельных случайно выбранных фрагментов;
б) сравнение характерных деталей в графическом представлении;
**в) непосредственное сравнение изображений;**
**г) сравнение характерных деталей в цифровом виде**

9. Из перечисленного для разграничения доступа к файлу применяются флаги, разрешающие:

а) копирование;
**б) чтение;**
**в) запись;**
**г) выполнение;**
д) удаление

10. Из перечисленного доступ к объекту в многоуровневой модели может рассматриваться как:

**а) чтение;**
б) удаление;
в) копирование;
**г) изменение**

11. Из перечисленного контроль доступа используется на уровнях:

**а) сетевом;**
**б) транспортном;**
в) сеансовом;
г) канальном;
**д) прикладном;**
е) физическом

12. Из перечисленного методами защиты потока сообщений являются:

**а) нумерация сообщений;**
**б) отметка времени;**
**в) использование случайных чисел;**
г) нумерация блоков сообщений;
д) копирование потока сообщений

13. Из перечисленного на транспортном уровне рекомендуется применение услуг:

а) идентификации;
**б) конфиденциальности;**
в) контроля трафика;
**г) контроля доступа;**
**д) целостности;**
**е) аутентификации**

14. Из перечисленного подсистема управления криптографическими ключами структурно состоит из:

**а) центра распределения ключей;**
**б) программно-аппаратных средств;**
в) подсистемы генерации ключей;
г) подсистемы защиты ключей

15. В чем заключается метод защиты информации - разделение доступа (привилегий)?

**а) В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы.**

б) В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям.

в) В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями.

г) В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении ее к неявному виду.

д) В исполнении существующих в стране или введении новых законов, положений, постановлений и инструкций, регулирующих юридическую ответственность должностных лиц-пользователей и обслуживающего технического персонала за утечку, потерю или модификацию доверенной ему информации, подлежащей защите, в том числе за попытки выполнить аналогичные действия за пределами своих полномочий, а также ответственности посторонних лиц за попытку преднамеренного несанкционированного доступа к аппаратуре и информации.

16. В чем заключается метод защиты информации - разграничение доступа?

**а) В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями.**

б) В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям.

в) В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы.

г) В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении ее к неявному виду.

д) В исполнении существующих в стране или введении новых законов, положений, постановлений и инструкций, регулирующих юридическую ответственность должностных лиц-пользователей и обслуживающего технического персонала за утечку, потерю или модификацию доверенной ему информации, подлежащей защите, в том числе за попытки выполнить аналогичные действия за пределами своих полномочий, а также ответственности посторонних лиц за попытку преднамеренного несанкционированного доступа к аппаратуре и информации.

17. В чем заключается метод защиты информации - ограничение доступа?

**а) В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям.**

б) В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями.

в) В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы.

г) В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении ее к неявному виду.

д) В исполнении существующих в стране или введении новых законов, положений, постановлений и инструкций, регулирующих юридическую ответственность должностных лиц-пользователей и обслуживающего технического персонала за утечку, потерю или модификацию доверенной ему информации, подлежащей защите,

в том числе за попытки выполнить аналогичные действия за пределами своих полномочий, а также ответственности посторонних лиц за попытку преднамеренного несанкционированного доступа к аппаратуре и информации.

18. На чем основан принцип работы антивирусных мониторов?

**а) На перехватывании вирусоопасных ситуаций и сообщении об этом пользователю.**

б) На проверке файлов, секторов и системной памяти и поиске в них известных и новых(неизвестных сканеру) вирусов. Для поиска известных вирусов используются маски.

в) На подсчете контрольных сумм для присутствующих на диске файлов или системных секторов. Эти суммы затем сохраняются в базе данных антивируса, а также другая информация: длина файлов, дата их последней модификации и т. д.

г) На защите системы от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженные.

19. На чем основан принцип работы антивирусных иммунизаторов?

**а) На защите системы от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженные.**

б) На проверке файлов, секторов и системной памяти и поиске в них известных и новых(неизвестных сканеру) вирусов. Для поиска известных вирусов используются маски.

в) На подсчете контрольных сумм для присутствующих на диске файлов или системных секторов. Эти суммы затем сохраняются в базе данных антивируса, а также другая информация: длина файлов, дата их последней модификации и т. д.

г) На перехватывании вирусоопасных ситуаций и сообщении об этом пользователю.

20. Что необходимо сделать при обнаружении файлового вируса?

**а) Компьютер необходимо отключить от сети и проинформировать системного администратора.**

б) Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются.

в) Вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен.

21. Что необходимо сделать при обнаружении загрузочного вируса?

**а) Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются.**

б) Компьютер необходимо отключить от сети и проинформировать системного администратора.

в) Вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен.

22. Что необходимо сделать при обнаружении макровируса?

**а) Вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен.**

б) Компьютер необходимо отключить от сети и проинформировать системного администратора.

в) Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются.

23. В чем заключается принцип работы сетевого вируса?

**а) Вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.**

б) Вирусы либо различными способами внедряются в выполняемые файлы, либо создают файлы-двойники, либо используют особенности организации файловой системы;

в) Вирусы записывают себя либо в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик винчестера, либо меняют указатель на активный boot-сектор.

г) Вирусы заражают файлы-документы и электронные таблицы популярных редакторов.

24. Источником каких угроз информации являются санкционированные программно-аппаратные средства?

**а) запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.); возникновение отказа в работе операционной системы.**

б) стихийные бедствия; магнитные бури; радиоактивное излучение.

в) внедрение агентов в число персонала системы; вербовка персонала или отдельных пользователей, имеющих определенные полномочия; угроза несанкционированного копирования секретных данных пользователем; разглашение, передача или утрата атрибутов разграничения доступа.

г) нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях); заражение компьютера вирусами с деструктивными функциями.

25. Какие угрозы информации относятся к искусственным?

**а) ошибки человека как звена системы; схемные и системотехнические ошибки разработчиков; структурные, алгоритмические и программные ошибки; действия человека, направленные на несанкционированные воздействия на информацию.**

б) отказы и сбои аппаратуры; помехи на линиях связи от воздействий внешней среды; аварийные ситуации; стихийные бедствия.

в) аварийные ситуации; стихийные бедствия; ошибки человека как звена системы; схемные и системотехнические ошибки разработчиков.

Критерии оценки тестовых заданий

| Структура работы | Критерии оценки | Распределение баллов |
|---|---|---|
| Один вопрос теста (25 вопросов в варианте)<br>Модуль 1<br>Модуль 2 | Неправильный ответ / Правильный ответ | <br><br><br>0,24<br>0,32 |

## Лабораторные работы

Цель проведения лабораторных работы – практическое освоение материала дисциплины.

Темы лабораторных работ

1. Файловая система в ОЗУ.
2. Файловая система: контроль доступа
3. Создание и управление процессами
4. Время запаздывания прерываний.
5. Защищаемая информация.

6. Построение системы защиты информации АС.
7. Способы аутентификации.
8. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы.

**Лабораторная работа №7**

**Модуль 2. Защита информации в современных операционных системах.**

**Тема:** Способы аутентификации.

**Цель:** Овладение практическими навыками составления пароля вручную, разработки и программирования вычислительного процесса идентификация и аутентификация пользователя.

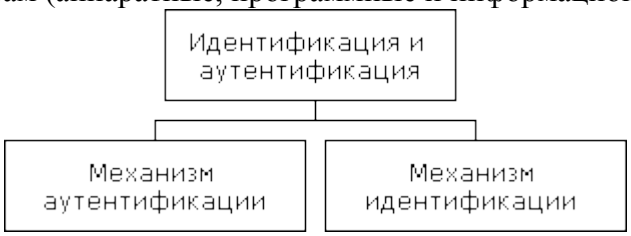
**Задание:** Научить некоторым методам, применяемым для установления подлинности различных объектов и своевременному обнаружению несанкционированных действий пользователя; правилам составления пароля; рассчитывать среднее время безопасности пароля. Формировать умения применять некоторые методы защиты информации от преднамеренного доступа (при применении простых средств хранения и обработки информации); оценивать время раскрытия пароля и возможность несанкционированного доступа к данным по среднему времени безопасности пароля.

Аппаратура. Для выполнения лабораторной работы необходим персональный компьютер.

Программное обеспечение. Для выполнения лабораторной работы необходима операционная система с поддержкой графического окружения, установленный офисный пакет приложений, векторный графический редактор, редактор диаграмм и блок-схем.

**Порядок выполнения:**

1. Идентификация и аутентификации применяются для ограничения доступа случайных и незаконных субъектов (пользователи, процессы) информационных систем к ее объектам (аппаратные, программные и информационные ресурсы).




Общий алгоритм работы таких систем заключается в том, чтобы получить от субъекта (например, пользователя) информацию, удостоверяющую его личность, проверить ее подлинность и затем предоставить (или не предоставить) этому пользователю возможность работы с системой.

Наличие процедур аутентификации и/или идентификации пользователей является обязательным условием любой защищенной системы, поскольку все механизмы защиты информации рассчитаны на работу с поименованными субъектами и объектами информационных систем.

Дадим определения этих понятий.

Идентификация – присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

Аутентификация (установление подлинности) – проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

При построении систем идентификации и аутентификации возникает проблема выбора идентификатора, на основе которого осуществляются процедуры идентификации и аутентификации пользователя. В качестве идентификаторов обычно используют:

· набор символов (пароль, секретный ключ, персональный идентификатор и т. п.), который пользователь запоминает или для их запоминания использует специальные средства хранения (электронные ключи);

· физиологические параметры человека (отпечатки пальцев, рисунок радужной оболочки глаза и т. п.) или особенности поведения (особенности работы на клавиатуре и т. п.).

Наиболее распространенными простыми и привычными являются методы аутентификации, основанные на паролях – конфиденциальных идентификаторах субъектов. В этом случае при вводе субъектом своего пароля подсистема аутентификации сравнивает его с паролем, хранящимся в базе эталонных данных в зашифрованном виде. В случае совпадения паролей подсистема аутентификации разрешает доступ к ресурсам системы.

Парольные методы аутентификации по степени изменяемости паролей делятся на:

· методы, использующие постоянные (многократно используемые) пароли;

· методы, использующие одноразовые (динамично изменяющиеся) пароли.

Использование одноразовых или динамически меняющихся паролей является более надежным методом парольной защиты.

В последнее время получили распространение комбинированные методы идентификации и аутентификации, требующие, помимо знания пароля, наличие карточки (token) – специального устройства, подтверждающего подлинность субъекта.

Карточки разделяют на два типа:

· пассивные (карточки с памятью);

· активные (интеллектуальные карточки).

Самыми распространенными являются пассивные карточки с магнитной полосой, которые считываются специальным устройством, имеющим клавиатуру и процессор. При использовании указанной карточки пользователь вводит свой идентификационный номер. В случае его совпадения с электронным вариантом, закодированным в карточке, пользователь получает доступ в систему. Это позволяет достоверно установить лицо, получившее доступ к системе и исключить несанкционированное использование карточки злоумышленником (например, при ее утере). Такой способ часто называют двукомпонентной аутентификацией.

Интеллектуальные карточки кроме памяти имеют собственный микропроцессор. Это позволяет реализовать различные варианты парольных методов защиты, например, многоразовые пароли, динамически меняющиеся пароли.

Методы аутентификации, основанные на измерении биометрических параметров человека, обеспечивают почти 100 % идентификацию, решая проблемы утери или утраты паролей и личных идентификаторов. Однако эти методы нельзя использовать при идентификации процессов или данных (объектов данных), они только начинают развиваться, требуют пока сложного и дорогостоящего оборудования. Это обусловливает их использование пока только на особо важных объектах.

Примерами внедрения указанных методов являются системы идентификации пользователя по рисунку радужной оболочки глаза, по почерку, по тембру голоса и др.

Новейшим направлением аутентификации является доказательство подлинности удаленного пользователя по его местонахождению. Данный защитный механизм основан на использовании системы космической навигации, типа GPS (Global Positioning System). Пользователь, имеющий аппаратуру GPS, многократно посылает координаты заданных спутников, находящихся в зоне прямой видимости. Подсистема аутентификации, зная орбиты спутников, может с точностью до метра определить месторасположение пользователя. Высокая надежность аутентификации определяется тем, что орбиты спутников подвержены колебаниям, предсказать которые достаточно трудно. Кроме того, координаты постоянно меняются, что исключает их перехват. Такой метод аутентификации может быть использован в случаях, когда авторизованный удаленный пользователь должен находиться в нужном месте.

Механизм идентификация и аутентификация пользователей

Общая процедура идентификации и аутентификации пользователя при его доступе в защищенную информационную систему заключается в следующем.

Пользователь предоставляет системе свой личный идентификатор (например, вводит пароль или предоставляет палец для сканирования отпечатка). Далее система сравнивает полученный идентификатор со всеми хранящимися в ее базе идентификаторами. Если результат сравнения успешный, то пользователь получает доступ к системе в рамках установленных полномочий. В случае отрицательного результата система сообщает об ошибке и предлагает повторно ввести идентификатор. В тех случаях, когда пользователь превышает лимит возможных повторов ввода информации (ограничение на количество повторов является обязательным условием для защищенных систем) система временно блокируется и выдается сообщение о несанкционированных действиях (причем, может быть, и незаметно для пользователя).

Если в процессе аутентификации подлинность субъекта установлена, то система защиты информации должна определить его полномочия (совокупность прав). Это необходимо для последующего контроля и разграничения доступа к ресурсам.

В целом аутентификация по уровню информационной безопасности делится на три категории:

1. Статическая аутентификация.
2. Устойчивая аутентификация.
3. Постоянная аутентификация.

Первая категория обеспечивает защиту только от несанкционированных действий в системах, где нарушитель не может во время сеанса работы прочитать аутентификационную информацию. Примером средства статической аутентификации являются традиционные постоянные пароли. Их эффективность преимущественно зависит от сложности угадывания паролей и, собственно, от того, насколько хорошо они защищены.

Устойчивая аутентификация использует динамические данные аутентификации, меняющиеся с каждым сеансом работы. Реализациями устойчивой аутентификации являются системы, использующие одноразовые пароли и электронные подписи. Устойчивая аутентификация обеспечивает защиту от атак, где злоумышленник может перехватить аутентификационную информацию и использовать ее в следующих сеансах работы.

Однако устойчивая аутентификация не обеспечивает защиту от активных атак, в ходе которых маскирующийся злоумышленник может оперативно (в течение сеанса аутентификации) перехватить, модифицировать и вставить информацию в поток передаваемых данных.

Постоянная аутентификация обеспечивает идентификацию каждого блока передаваемых данных, что предохраняет их от несанкционированной модификации или вставки. Примером реализации указанной категории аутентификации является использование алгоритмов генерации электронных подписей для каждого бита пересылаемой информации.

При санкционированном доступе в информационную систему пользователь должен идентифицировать себя, а система — проверить подлинность идентификации (произвести аутентификацию).

Идентификация — это присвоение какому-либо объекту или субъекту, реализующему доступ к ИС, уникального имени (логина), образа или числового значения. Установление подлинности (аутентификация) заключается в проверке, является ли данный объект (субъект) в самом деле тем, за кого себя выдает. Конечная цель идентификации и установления подлинности объекта в вычислительной системе — его допуск к информации ограниченного пользования в случае положительного результата проверки или отказ в допуске при отрицательном результате.

Как правило, любая процедура идентификации предполагает ввод пользователем своего логина (login) и пароля (password). В зависимости от особенностей функционирования системы пароль выбирается самим пользователем либо назначается администратором (или же иногда его генерирует сама система).

Пароль должен быть таким, чтобы его нельзя было легко раскрыть. Для этого при выборе и использовании пароля рекомендуется руководствоваться следующими правилами:

1) пароль не должен содержать личных данных пользователя (таких, как фамилия, имя, серия или номер паспорта либо другого документа, удостоверяющего личность, дата рождения, адрес и т. п.);

2) пароль не должен быть словом из какого-либо словаря (входить в какой-либо тезаурус), так как перебор слов заданного словаря — технически достаточно простая задача;

3) пароль не должен быть слишком коротким (подобрать сочетание символов в этом случае также не представляет сложности);

4) пароль не должен состоять из повторяющихся букв или фрагментов текста;

5) пароль не должен состоять из символов, соответствующих подряд идущим клавишам на клавиатуре (например, «QWERTY» — образец недопустимого пароля);

6) желательно включать в пароль символы в разных регистрах (прописные и строчные буквы, кириллицу и латиницу), знаки препинания, цифры и др.;

Меры предосторожности, которые необходимо соблюдать при использовании пароля:

1) старайтесь сохранять пароль в тайне (лучше всего его запоминать, а не записывать;

2) периодически (при регулярном обращении к системе — не реже одного раза в месяц) заменяйте пароль на новый, но он не должен выдаваться пользователю в конце сеанса работы. Заметим, что в разное время могут применяться различные пароли;

3) в паспорте пользователя пароль должен храниться в зашифрованном виде. Наиболее подходящими для этих целей являются методы необратимого шифрования (при которых обратное преобразование невозможно). Введенный пользователем пароль тоже должен шифроваться, а уже затем сравниваться с хранящимся.

*Несоблюдение этих и ряда других правил ведет к раскрытию пароля и к возможности несанкционированного доступа к данным.

Среднее время безопасности пароля определяется по формуле

$$\mathbf{T} = \left( d + \frac{m}{n} \right) \bullet \frac{S}{2}$$

где d — промежуток времени между двумя неудачными попытками несанкционированного входа в систему, т — количество символов в пароле, п — скорость набора пароля (количество символов, набираемых в единицу времени), S — количество всевозможных паролей указанной длины.

Таким образом, среднее время безопасности пароля фактически равно времени, за которое можно ввести (перебрать) половину всевозможных паролей заданной длины. Однако большинство информационных систем предусматривают возможность ввода идентифицирующих данных не более заданного количества раз (как правило не более трех раз за один сеанс работы).

В некоторых случаях процесс идентификации и аутентификации включает реализацию какого-либо несложного алгоритма. При этом после анализа логина и пароля система может, в частности, выдать на экран несколько значений данных указанного типа (например, сгенерированных чисел или последовательностей символов). Пользователь должен произвести с ними манипуляции в соответствии с некоторым алгоритмом (в простейшем случае — в соответствии с заданной формулой). Система тоже производит указанные манипуляции с этими данными, а затем сверяет полученный результат с введенным пользователем.

порядок выполнения работы

1. Изучить теоретическую часть по приведенным выше данным и дополнительной литературе.

2. С использованием одного из языков программирования составить программу, которая выполняет действия, указанные в таблице с номером вашего варианта.

Задание

Таблица вариант 1

| Задание | Алгоритм |
|---|---|
| 1 | 2 |
| Пусть на экран выведены следующие три слова: «Sony», «Hewlett» и «Packard».<br>Составить программу, которая записывает пароль следующим образом | Исходные данные — строковые константы<br>1. В строку <результат> в качестве первого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и третьем словах; если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26.<br>2. В качестве второго символа записать букву, которая в алфавите предшествует букве, являющейся последним символом второго слова на экране; если это буква «a», записать «z».<br>3. Если третье слово содержит нечетное количество букв, то в качестве третьего символа записать букву, которая в алфавите следует за буквой, являющейся средним символом третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z».<br>4. в качестве первого символа записать букву, которая в алфавите следует за буквой, являющейся первым символом первого слова на экране; если это буква «z», записать «a».<br>5. Вывести полученную строку. |
| Дополнить полученную программу средствами аутентификации | 1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*».<br>2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ.<br>3. Вывести результат аутентификации: пароль верен или неверен? |
| Пусть на экран выведены следующие три слова: «scleroses», «scoliosis», «paradantoz».<br>Составить программу, которая записывает пароль следующим образом | Исходные данные — строковые константы<br>1. В строку <результат> в качестве первого символа записать букву, которая в алфавите следует за буквой, являющейся вторым символом первого слова на экране; если это буква «z», записать «a».<br>2. В качестве второго символа записать букву, которая в алфавите предшествует предпоследней букве, являющейся последним символом второго слова на экране; если это буква «a», записать «z».<br>3. Если третье слово содержит нечетное количество букв, то в качестве третьего символа записать букву, которая в алфавите следует за буквой, являющейся предшественником среднего символа третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z».<br>4. В качестве четвертого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме |

| | |
|---|---|
| | количеств символов в первом и третьем словах плюс 1 символ;<br>если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26.<br>5. Вывести полученную строку. |
| Дополнить полученную программу средствами аутентификации | 1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*».<br>2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ.<br>3. Вывести результат аутентификации: пароль верен или неверен? |

Таблица вариант 2

| Задание | Алгоритм |
|---|---|
| 1 | 2 |
| Пусть на экран выведены следующие три слова: «computer», «maus», «scanner».<br>Составить программу, которая записывает пароль следующим образом | Исходные данные — строковые константы<br>1. В строку <результат> в качестве первого символа записать букву, которая в алфавите следует за буквой, являющейся последним символом первого слова на экране; если это буква «z», записать «a».<br>2. В качестве второго символа записать букву, которая в алфавите следует за буквой, являющейся последним символом второго слова на экране; если это буква «a», записать «z».<br>3. Если третье слово содержит нечетное количество букв, то в качестве третьего символа записать букву, которая в алфавите следует через пять позиций за буквой, являющейся средним символом третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z».<br>4. В качестве четвертого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в третьем и втором словах;<br>если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26.<br>5. Вывести полученную строку. |
| Дополнить полученную программу средствами аутентификации | 1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*».<br>2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ.<br>3. Вывести результат аутентификации: пароль верен или неверен? |
| Пусть на экран выведены следующие три слова: «mathematic», «physic», «hemi».<br>Составить | Исходные данные — строковые константы<br>1. Если первое слово содержит нечетное количество букв, то в качестве первого символа в строку <результат> записать букву, которая в алфавите следует через три позиции за буквой, являющейся средним символом третьего слова; если это буква |

| | |
|---|---|
| программу, которая записывает пароль следующим образом | «z», записать «a». Если же первое слово содержит четное количество символов, то в качестве первого символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов первого слова; если это буква «a», записать «z».<br>2. В качестве второго символа записать букву, которая в алфавите предшествует букве, являющейся последним символом второго слова на экране; если это буква «a», записать «z».<br>3. В качестве третьего символа записать букву, которая в алфавите следует за буквой, являющейся первым символом третьего слова на экране; если это буква «z», записать «a».<br>4. В качестве четвертого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и втором словах минус 1 символ;<br>если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26.<br>5. Вывести полученную строку. |
| Дополнить полученную программу средствами аутентификации | 1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*».<br>2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ.<br>3. Вывести результат аутентификации: пароль верен или неверен? |

Таблица вариант 3

| Задание | Алгоритм |
|---|---|
| 1 | 2 |
| Пусть на экран выведены следующие три слова: «pero», «ruchka», «bumaga».<br>Составить программу, которая записывает пароль следующим образом | Исходные данные — строковые константы<br>1. В строку <результат> в качестве первого символа записать букву, которая в алфавите следует за буквой, являющейся третьим символом первого слова на экране; если это буква «z», записать «a».<br>2. В качестве второго символа записать букву, которая в алфавите предшествует букве, являющейся первым символом второго слова на экране; если это буква «a», записать «z».<br>3. Если третье слово содержит нечетное количество букв, то в качестве третьего символа записать букву, которая в алфавите следует за буквой, являющейся средним символом третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z».<br>4. В качестве четвертого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и втором словах;<br>если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26.<br>5. Ввести полученную строку. |

| | |
|---|---|
| Дополнить полученную программу средствами аутентификации | 1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*».<br>2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ.<br>3. Вывести результат аутентификации: пароль верен или неверен? |
| Пусть на экран выведены следующие три слова: «Sony», «Hewlett» и «Packard».<br>Составить программу, которая записывает пароль следующим образом | Исходные данные — строковые константы<br>1. В строку <результат> в качестве первого символа записать букву, которая в алфавите следует за буквой, являющейся вторым от конца символом первого слова на экране; если это буква «z», записать «a».<br>2. В качестве второго символа записать букву, которая в алфавите предшествует букве, являющейся последним символом второго слова на экране; если это буква «a», записать «z».<br>3. Если третье слово содержит нечетное количество букв, то в качестве третьего символа записать букву, которая в алфавите следует за через две позицииза буквой, являющейся средним символом третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z».<br>4. В качестве четвертого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и втором словах плюс 2 символ;<br>если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26.<br>5. Вывести полученную строку. |
| Дополнить полученную программу средствами аутентификации | 1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*».<br>2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ.<br>3. Вывести результат аутентификации: пароль верен или неверен? |

Таблица вариант 4

| Задание | Алгоритм |
|---|---|
| 1 | 2 |
| Пусть на экран выведены следующие три слова: «Kats», «milk», «smitten».<br>Составить программу, которая записывает пароль следующим образом | Исходные данные — строковые константы<br>1. В строку <результат> в качестве первого символа записать букву, которая в алфавите следует за буквой, являющейся первым символом третьего слова на экране; если это буква «z», записать «a».<br>2. В качестве второго символа записать букву, которая в алфавите предшествует букве, являющейся первым символом второго слова на экране; если это буква «a», записать «z».<br>3. Если третье слово содержит нечетное количество букв, |

| | |
|---|---|
| | то в качестве третьего символа записать букву, которая в алфавите следует за буквой, являющейся средним символом третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z».<br>4. В качестве четвертого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и втором словах минус 2 символ;<br>если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26.<br>5. Вывести полученную строку. |
| Дополнить полученную программу средствами аутентификации | 1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*».<br>2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ.<br>3. Вывести результат аутентификации: пароль верен или неверен? |
| Пусть на экран выведены следующие три слова: «dog», «zaps», «budge».<br>Составить программу, которая записывает пароль следующим образом | Исходные данные — строковые константы<br>1. В строку <результат> в качестве первого символа записать букву, которая в алфавите следует за буквой, являющейся первым символом второго слова на экране; если это буква «z», записать «a».<br>2. В качестве второго символа записать букву, которая в алфавите предшествует букве, являющейся предпоследним символом второго слова на экране; если это буква «a», записать «z».<br>3. Если третье слово содержит нечетное количество букв, то в качестве третьего символа записать букву, которая в алфавите следует за буквой, которая предшествует среднему символу третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z».<br>4. В качестве четвертого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и втором словах;<br>если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26.<br>5. Вывести полученную строку. |
| Дополнить полученную программу средствами аутентификации | 1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*».<br>2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ.<br>3. Вывести результат аутентификации: пароль верен или неверен? |

Таблица вариант 5

| Задание | Алгоритм |
|---|---|
| 1 | 2 |
| Пусть на экран выведены следующие три слова: «pipers», «hauls», «polios».<br>Составить программу, которая записывает пароль следующим образом | Исходные данные — строковые константы<br>1. В строку <результат> в качестве первого символа записать букву, которая в алфавите следует за буквой, являющейся вторым символом третьего слова на экране; если это буква «z», записать «a».<br>2. В качестве второго символа записать букву, которая в алфавите предшествует букве, являющейся вторым символом второго слова на экране; если это буква «a», записать «z».<br>3. Если третье слово содержит нечетное количество букв, то в качестве третьего символа записать букву, которая в алфавите следует за буквой, являющейся последним символом третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z».<br>4. В качестве четвертого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и втором словах плюс 3 символа;<br>если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26.<br>5. Вывести полученную строку. |
| Дополнить полученную программу средствами аутентификации | 1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*».<br>2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ.<br>3. Вывести результат аутентификации: пароль верен или неверен? |
| Пусть на экран выведены следующие три слова: «student», «pedagogy», «buck».<br>Составить программу, которая записывает пароль следующим образом | Исходные данные — строковые константы<br>1. В строку <результат> в качестве первого символа записать букву, которая в алфавите следует за буквой, являющейся третьим символом третьего слова на экране; если это буква «z», записать «a».<br>2. В качестве второго символа записать букву, которая в алфавите предшествует букве, являющейся предпоследним символом второго слова на экране; если это буква «a», записать «z».<br>3. Если третье слово содержит нечетное количество букв, то в качестве третьего символа записать букву, которая в алфавите следует за буквой, являющейся первым символом третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z».<br>4. В качестве четвертого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме |

| | |
|---|---|
| | количеств символов в первом и втором словах минус 3 символа;<br>если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26.<br>5. Вывести полученную строку. |
| Дополнить полученную программу средствами аутентификации | 1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*».<br>2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ.<br>3. Вывести результат аутентификации: пароль верен или неверен? |

Таблица вариант 6

| Задание | Алгоритм |
|---|---|
| 1 | 2 |
| Пусть на экран выведены следующие три слова: «basic», «compilation», «programs».<br>Составить программу, которая записывает пароль следующим образом | Исходные данные — строковые константы<br>1. В строку <результат> в качестве первого символа записать букву, которая в алфавите следует за буквой, являющейся первым символом с конца первого слова на экране; если это буква «z», записать «a».<br>2. В качестве второго символа записать букву, которая в алфавите следует за буквой, являющейся последним символом второго слова на экране; если это буква «a», записать «z».<br>3. Если третье слово содержит нечетное количество букв, то в качестве третьего символа записать букву, которая в алфавите следует за буквой, являющейся вторым символом третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z».<br>4. В качестве четвертого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и втором словах;<br>если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26.<br>5 Вывести полученную строку. |
| Дополнить полученную программу средствами аутентификации | 1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*».<br>2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ.<br>3. Вывести результат аутентификации: пароль верен или неверен? |
| Пусть на экран выведены следующие три слова: «gourd», «speckle», «capote».<br>Составить программу, которая | Исходные данные — строковые константы<br>1. В строку <результат> в качестве 2-х первых символов записать буквы, которые в алфавите следуют за буквой, являющейся первым символом первого слова на экране; если это буква «z», записать «a».<br>2. В качестве третьего символа записать букву, которая |

| | |
|---|---|
| записывает пароль следующим образом | в алфавите следует за буквой, являющейся предпоследним символом второго слова на экране; если это буква «a», записать «z».<br>3. Если третье слово содержит нечетное количество букв, то в качестве четвертого символа записать букву, которая в алфавите следует за буквой, являющейся предпоследним символом третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве чеитвертого символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z».<br>4. В качестве пятого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и втором словах плюс 4 символа;<br>если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26.<br>5. Ввести полученную строку. |
| Дополнить полученную программу средствами аутентификации | 1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*».<br>2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ.<br>3. Вывести результат аутентификации: пароль верен или неверен? |

Таблица вариант 7

| Задание | Алгоритм |
|---|---|
| 1 | 2 |
| Пусть на экран выведены следующие три слова: «worship», «outreach», «luck».<br>Составить программу, которая записывает пароль следующим образом | Исходные данные — строковые константы<br>1. В строку <результат> в качестве в качестве 2-х первых символов записать буквы, которые в алфавите следуют за буквой, являющейся первым символом второго слова на экране; если это буква «z», записать «a».<br>2. В качестве второго символа записать букву, которая в алфавите предшествует букве, являющейся средним символом второго слова на экране; если это буква «a», записать «z».<br>3. Если третье слово содержит нечетное количество букв, то в качестве третьего символа записать букву, которая в алфавите следует за буквой, являющейся третьим символом третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z».<br>4. В качестве четвертого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и втором словах минус 4 символа;<br>если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26.<br>5. Вывести полученную строку. |

| | |
|---|---|
| Дополнить полученную программу средствами аутентификации | 1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*».<br>2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ.<br>3. Вывести результат аутентификации: пароль верен или неверен? |
| Пусть на экран выведены следующие три слова: «starved», «carp», «shuck».<br>Составить программу, которая записывает пароль следующим образом | Исходные данные — строковые константы<br>1. В строку <результат> в качестве в качестве 2-х первых символов записать буквы, которые в алфавите следуют за буквой, являющейся первым символом третьего слова на экране; если это буква «z», записать «a».<br>2. В качестве второго символа записать букву, которая в алфавите предшествует букве, являющейся третьим символом второго слова на экране; если это буква «a», записать «z».<br>3. Если третье слово содержит нечетное количество букв, то в качестве третьего символа записать букву, которая в алфавите следует за буквой, являющейся четвертым символом третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z».<br>4. В качестве четвертого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и втором словах;<br>если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26.<br>5. Вывести полученную строку. |
| Дополнить полученную программу средствами аутентификации | 1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*».<br>2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ.<br>3. Вывести результат аутентификации: пароль верен или неверен? |

2. Ответить на контрольные вопросы:
   a) Что такое идентификация?
   b) Что такое аутентификация?
   c) Что такое авторизация?
   d) Правила выбора и использования пароля.
   e) Объекты идентификации и установления подлинности в информационной системе.
   f) Особенности разделения привилегий и разграничения доступа?
   g) Меры предосторожности, которые необходимо соблюдать при использовании пароля?
3. Защита лабораторной работы. Проводится в форме устного опроса после выполнения работы.

Критерии оценки лабораторной работы

| Структура работы | Критерии оценки | Распределение баллов |
|---|---|---|
| Одно лабораторное задание | работа выполнена с ошибками и | |

| | | |
|---|---|---|
| Модуль 1<br>Модуль 2 | не получены ответы на все контрольные вопросы/ работа выполнена, но не получены ответы на все контрольные вопросы/ работа выполнена и получены ответы на все контрольные вопросы | 0/2/4<br>0/1/3 |

**Практические работы**

Цель проведения практических работ – практическое освоение материала дисциплины.

Темы практических работ

1. Функции и структура операционной системы.
2. Интерфейсы передачи..
3. Файловая система: контроль доступа.
4. Создание и управление процессами.
5. Механизмы аутентификации.
6. Способы аутентификации.
7. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы.
8. Построение системы защиты информации в КС.

**Практическая работа №7**

**Модуль 2. Защита информации в современных операционных системах.**

**Тема:** Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы.

**Цель:** Изучить возможностями Windows и Linux по ограничению доступа к объектам ОС, изучить основные инструменты управления доступом.

**Задание:** Ознакомиться с возможностями Windows и Linux по ограничению доступа к объектам ОС, изучить основные инструменты управления доступом. Изучить теоретическую часть. Выполнить по порядку все заданные действия.

Аппаратура. Для выполнения лабораторной работы необходим персональный компьютер.

Программное обеспечение. Для выполнения лабораторной работы необходима операционная система с поддержкой графического окружения, установленный офисный пакет приложений, векторный графический редактор, редактор диаграмм и блок-схем.

**Порядок выполнения:**

1. Системы линейки Windows 9x не являются многопользовательскими в том понимании, что не позволяют разграничить доступ к ресурсам, а лишь позволяют выбрать профиль - способ отображения данных в соответствии с настройками того или иного пользователя. В системах линейки Linux и Windows NT доступ к объектам управляется операционной системой. Перечень объектов, к которым может разграничиваться доступ зависит от конкретного типа ОС. Например, в Windows защищаемыми объектами могут быть файлы, устройства, каналы, задания, процессы, потоки, объекты синхронизации, порты ввода-вывода, разделы общей памяти, сетевые ресурсы, разделы реестра и др.

Управление доступом заключается в предоставлении пользователям, группам и компьютерам определенных разрешений на доступ к объектам ОС.

Разрешение представляет собой правило, связанное с объектом ОС, которое определяет, каким пользователям и какого типа доступ к объекту разрешен.

Назначаемые разрешения зависят от вида объекта. Например, в Windows разрешения, которые могут быть назначены для файла, отличаются от разрешений, допустимых для раздела реестра.

Владение объектами

При создании объекта ему назначается владелец. По умолчанию владельцем объекта становится его создатель. Какие разрешения ни были бы установлены для объекта, владелец объекта всегда может изменить эти разрешения.

Наследование разрешений

Механизм наследования облегчает администраторам задачи назначения разрешений и управления ими. Благодаря этому механизму разрешения, установленные для контейнера, автоматически распространяются на все объекты этого контейнера. Например, файлы, создаваемые в папке, наследуют разрешения этой папки.

2. Управление доступом в Windows

Как уже было сказано в л/р №1, для каждого зарегистрированного пользователя система создает свою учетную запись. Учетные записи всех пользователей хранятся в некой системной базе данных.

База данных учетных записей

| Имя | Пароль | SID |
|---|---|---|
| User1 | Pass1 | SID1 |
| User2 | Pass2 | SID2 |
| | ... | |
| UserN | Pass3 | SIDN |

Для каждой учетной записи система хранит имена, пароли и уникальные идентификаторы - SID(Security Identifier). Последний используется системой в дальнейшем везде, где нужно однозначно сослаться на ту или иную учетную запись. База данных учетных записей содержит сведения не только о пользователях, но и группах пользователей (например, "Администраторы"), которые также имеют SID. Группы позволяют нескольким пользователям задать общие права доступа. Управление учетными записями с помощью групп позволяет упростить работу администратора по контролю доступа пользователей к ресурсам.

Для каждого объекта или ресурса ОС, поддерживается контрольный список доступа (Access Control List - ACL). Он определяет перечень пользователей, которым разрешен доступ к данному объекту, а также тех, кому запрещен.

Каждый список контроля доступа (ACL) представляет собой набор элементов контроля доступа (Access Control Entries, или ACE).

| ACL | | |
|---|---|---|
| SID | Вид доступа | Разрешить/запретить |
| SID1 | Чтение | Разрешить |
| SID1 | Запись | Запретить |
| SID2 | Полный доступ | Разрешить |

ACE

ACE бывает двух типов (разрешающий и запрещающий доступ) и обязательно содержит три поля:

- SID пользователя или группы, к которому применяется данное правило;
- Вид доступа, на которое распространяется данное правило;
- Тип ACE - разрешающий или запрещающий.

Таким образом, ACL, изображенный на рис.2, устанавливает следующие правила: пользователю SID1 разрешить доступ на чтение объекта, но запретить доступ на запись, а пользователю SID2 - разрешить полный доступ к объекту.

Кроме того, к дескриптору безопасности применимы следующие правила:

- Если ACL отсутствует, то объект считается незащищенным, т. е. все имеют к нему неограниченный доступ;

- Если ACL существует, но не содержит ни одного ACE, то доступ к объекту закрыт для всех.

Теоретически может сложиться такая ситуация, когда два ACE противоречат друг другу. Например, один ACE дает полный доступ членам определенной группы, а другой - запрещает доступ определенному пользователю из этой группы. Получит ли этот пользователь доступ к объекту зависит от того, в каком порядке ACE расположены.

Когда процесс запрашивает определенный вид доступа к защищенному объекту, система действует по следующему алгоритму:

· Просматриваются все ACE в ACL от первого к последнему. Определяющую роль играет первый встреченный элемент, дающий возможность пользователю воспользоваться запрошенной услугой или отказывающий в этом.

· Если хотя бы один из видов запрошенного доступа не предоставлен (запрещен или достигнут конец ACL), система принимает решение отказать в доступе к объекту. Из этого можно сделать вывод, что запрещающие элементы не имеет смысла размещать внизу ACL, так как если перед ними нет соответствующих разрешающих, доступ все равно будет закрыт. Запрещающие элементы обычно размещают вверху списка, особенно если нужно запретить доступ конкретному пользователю, который может его получить, воспользовавшись членством в группе. В Windows XP запрещающие элементы автоматически помещаются вверху ACL.

Управление доступом к файловой системе

Базовые разрешения объектов файловой системы Windows приведены в таблице.

| Базовое разрешение | Значение для папок | Значение для файлов |
|---|---|---|
| Чтение (Read) | Разрешает обзор папок и просмотр списка файлов и подпапок | Разрешает просмотр и доступ к содержимому файла |
| Запись (Write) | Разрешает добавление файлов и подпапок | Разрешает запись данных в файл |
| Чтение и Выполнение (Read & Execute) | Разрешает обзор папок и просмотр списка файлов и подпапок; наследуется файлами и папками | Разрешает просмотр и доступ к содержимому файла, а также запуск исполняемого файла |
| Список содержимого папки (List Folder Contents) | Разрешает обзор папок и просмотр списка файлов и подпапок; наследуется только папками | Не применимо |
| Изменить (Modify) | Разрешает просмотр содержимого и создание файлов и подпапок; допускает удаление папки | Разрешает чтение и запись данных в файл; допускает удаление файла |
| Полный доступ (Full Control) | Разрешает просмотр содержимого, а также создание, изменение и удаление файлов и подпапок | Разрешает чтение и запись данных, а также изменение и удаление файла |

При вычислении действующих разрешений пользователя принимаются во внимание все разрешения назначенные пользователю, а также группам, членом которых он является.

Помимо базовых разрешений существуют также особые разрешения объектов. В отличие от базовых они более конкретны и используются для более точной настройки разрешений к файловым объектам.

Взаимосвязь между базовыми и особыми разрешениями приведены в таблице

| Особые разрешения | Полный доступ (Full Control) | Изменить (Modify) | Чтение и выполнение (Read & Execute) | Чтение (Read) | Запись (Write) |
|---|---|---|---|---|---|
| Выполнение файлов (Execute File) | + | + | + | | |
| Чтение данных (Read Data) | + | + | + | + | |
| Чтение атрибутов (Read Attributes) | + | + | + | + | |
| Чтение дополнительных атрибутов (Read Extended Attributes) | + | + | + | + | |
| Запись данных (Write Data) | + | + | | | + |
| Дозапись данных (Append Data) | + | + | | | + |
| Запись атрибутов (Write Attributes) | + | + | | | + |
| Запись дополнительных атрибутов (Write Extended Attributes) | + | + | | | + |
| Удаление (Delete) | + | + | | | |
| Чтение разрешений (Read Permissions) | + | + | + | + | + |
| Смена разрешений (Change Permissions) | + | | | | |
| Смена владельца (Take Ownership) | + | | | | |

Взаимосвязь между базовыми и особыми разрешениями папок приведены в таблице

| Особые разрешения | Полный доступ (Full Control) | Изменить (Modify) | Чтение и выполнение (Read & Execute) | Список содержимого папки (List Folder Contents) | Чтение (Read) | Запись (Write) |
|---|---|---|---|---|---|---|
| Обзор папок (Traverse Folder) | + | + | + | + | | |
| Содержание папки (List Folder) | + | + | + | + | + | |
| Чтение атрибутов (Read Attributes) | + | + | + | + | + | |
| Чтение дополнительных атрибутов (Read Extended Attributes) | + | + | + | + | + | |
| Создание файлов (Create Files) | + | + | | | | + |
| Создание папок (Create Folders) | + | + | | | | + |
| Запись атрибутов (Write Attributes) | + | + | | | | + |
| Запись дополнительных атрибутов (Write Extended Attributes) | + | + | | | | + |

| | | | | | | |
|---|---|---|---|---|---|---|
| Удаление подпапок и файлов(Delete Subfolders and Files) | + | + | | | | |
| Удаление (Delete) | + | | | | | |
| Чтение разрешений (Read Permissions) | + | + | + | + | + | + |
| Смена разрешений (Change Permissions) | + | | | | | |
| Смена владельца (Take Ownership) | + | | | | | |

Управление доступом к реестру

Реестр Windows представляет собой реляционную базу данных, в которой аккумулируется вся необходимая для нормального функционирования компьютера информация о настройках операционной системы, а также об используемом совместно с Windows программном обеспечениии оборудовании. Все хранящиеся в реестре данные представлены в стандартизированной форме и четко структурированы согласно предложенной разработчиками Windows иерархии.

HKEY_CLASSES_ROOT

Ветвь HKEY_CLASSES_ROOT, обычно обозначаемая в технической документации аббревиатуройHKCR, включает в себя ряд подразделов, в которых содержатся сведения о расширениях всех зарегистрированных в системе типов файлов и данные о COM-серверах, зарегистрированных на компьютере. Фактически, данную ветвь с функциональной точки зрения можно считать аналогом ключа HKEY_LOCAL_MACHINE\Software, поскольку здесь собраны все необходимые операционной системе данные о файловых ассоциациях.

HKEY_CURRENT_USER

В ветви HKEY_CURRENT_USER, обозначаемой в документации аббревиатурой HKCU, содержится информация о пользователе, ведущем на компьютере текущий сеанс работы, который обслуживается реестром. В ее подразделах находится информация о переменных окружения, группах программ данного пользователя, настройках Рабочего стола, цветах экрана, сетевых соединениях, принтерах и дополнительных настройках приложений (переменные окружения используются в Windows в сценариях, записях реестра и других приложениях в качестве подстановочных параметров). Эта информация берется из подраздела Security ID (SID) ветви HKEY_USERS для текущего пользователя. Фактически, в данной ветви собраны все сведения, относящиеся к профилю пользователя, работающего с Windows в настоящий момент.

HKEY_LOCAL_MACHINE

HKEY_LOCAL_MACHINE (HKLM) — это ветвь, в которой содержится информация, относящаяся к операционной системе и оборудованию, например тип шины компьютера, общий объем доступной памяти, список загруженных в данный момент времени драйверов устройств, а также сведения о загрузке Windows. Данная ветвь включает наибольшее количество информации в системном реестре Windows и нередко используется для тонкой настройки аппаратной конфигурации компьютера. Следует понимать, что хранящиеся в этой ветви данные справедливы для всех профилей, зарегистрированных в системе пользователей.

HKEY_USERS

Ветвь HKEY_USERS (HKU) содержит подразделы с информацией обо всех профилях пользователей данного компьютера. Один из ее подразделов всегда соотносится с подразделом HKEY_CURRENT_USER (через параметр Security ID (SID) пользователя). Другой подраздел, HKEY_USERS\DEFAULT, содержит информацию о настройках системы в момент времени, предшествующий началу сеанса текущего пользователя.

HKEY_CURRENT_CONFIG

Ветвь HKEY_CURRENT_CONFIG (HKCC) содержит подразделы с информацией обо всех профилях оборудования, используемого в данном сеансе работы. Профили оборудования позволяют выбрать драйверы поддерживаемых устройств для заданного сеанса работы (например, не использовать активацию порта док-станции переносного компьютера, когда он не подключен к станции). Эта информация берется из подразделов HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet.

Вполне очевидно также, что некорректное изменение хранящейся в реестре информации вполне способно нарушить работоспособность Windows. Достаточно допустить ошибку в записи значения какого-либо ключа или параметра, и пользователь больше не сможет загрузить компьютер. Именно по этой причине разработчики Windows заметно ограничили доступ к реестру, и редактировать параметры реестра, касающиеся безопасности, могут только пользователи Windows, имеющие в системе учетную запись Администратора.

Для редактирования и управления доступом к реестру предназначена стандартная утилита Regedit. Управление доступом осуществляется аналогично управлению доступом к файловой системе, с тем отличием, что ACL устанавливаются не для папок и файлов, а для разделов и ключей реестра.

Управление доступом к общим (сетевым) ресурсам

Файлы и папки, хранящиеся на локальном компьютере, в сети или в Интернете, можно передавать в общий доступ. Файлы и папки, находящиеся в общем доступе, менее защищены, чем при отсутствии общего доступа к ним. Пользователи, имеющие доступ к компьютеру по сети, в зависимости от установленных разрешений, могут просматривать, копировать, изменять, создавать или удалять файлы, содержащиеся в общей папке.

В общем случае, лучше всего задавать разрешения с помощью файловой системы NTFS – в этом случае применяются более строгие разрешения. Однако имеется возможность задавать собственные разрешения для общих (сетевых) ресурсов. Эти разрешения применяются только к пользователям, доступ которых к ресурсу осуществляется по сети. Они не применяются к пользователям, которые получают доступ к ресурсу на компьютере, на котором сохранен ресурс.

Разрешения применяются ко всем файлам и папкам общего ресурса. По этим причинам разрешения для общих ресурсов обеспечивают меньший уровень безопасности, чем разрешения NTFS. Однако эти разрешения являются единственным способом защиты сетевых ресурсов для томов с файловыми системами FAT и FAT32, поскольку разрешения NTFS не доступны для томов с файловыми системами FAT и FAT32.

Разрешениями определяются максимальные права доступа пользователя к общему ресурсу при работе в сети. Все эти свойства являются дополнением безопасности, предоставляемой файловой системой NTFS (т. е. разрешения файловой системы и собственные разрешения общего ресурса при доступе к нему по сети действуют в совокупности!).

Имеется возможность применять следующие типы разрешений доступа к общим папкам или дискам:

1. Чтение;
2. Изменить;
3. Полный доступ.

Разрешение «Чтение» позволяет:

- просматривать имена файлов и подкаталогов;
- просматривать подпапки;
- просматривать данные в файлах;
- выполнять программные файлы.

Разрешение «Изменить» включает разрешение «Чтение», а также позволяет:

- добавлять файлы и подпапки;
- изменять данные в файлах;
- удалять подпапки и файлы.

Разрешение «Полный доступ» используется по умолчанию для всех новых общих ресурсов. При общем использовании ресурса это разрешение назначается группе «Все». Разрешение «Полный доступ» включает разрешения «Изменить» и «Чтение», а также позволяет:

- изменять разрешения (только для файлов и папок NTFS);
- стать владельцем (только для файлов и каталогов NTFS).

Особые папки общего доступа.

Помимо папок общего доступа, которые создает пользователь в процессе своей работы, существуют особые общие ресурсы, которые называются административными или системными. Ниже приведен полный список такого рода ресурсов.

| Ресурс | Описание |
|---|---|
| имя диска$ | Представляет собой общий ресурс, который позволяет администраторам подключаться к корневому каталогу диска. |
| ADMIN$ | Это ресурс, который используется при удаленном администрировании компьютера. Путь к этому общему ресурсу всегда совпадает с путем к системному каталогу (т. е. каталогу, в котором установлена система, например C:\Windows). |
| IPC$ | Представляет собой ресурс совместного доступа к именованным каналам, которые обеспечивают связь между программами. Используется для удаленного администрирования компьютера и для просмотра общих ресурсов компьютера. Этот ресурс нельзя удалить. |
| PRINT$ | Общий ресурс, используемый для удаленного администрирования принтеров. |

3. Управление доступом в Linux

Классическая система управления доступом в Linux несколько отличается от рассмотренной выше системы в Windows, хотя присутствуют и общие черты.

В отличие от Windows большинство объектов разграничения доступа представлено в Linux в виде файлов. Т. о. образом разграничение доступа к файловой системе является в данной ОС важнейшей задачей системы управления доступом.

Управление доступом к файловой системе

Каждый пользователь в системе имеет свой уникальный идентификационный номер (user ID, или UID). Группы также имеют такой идентификатор, который называется group ID, или GID.

В свою очередь файлы имеют двух владельцев: пользователя (user owner) и группу пользователей (group owner). Для каждого файла есть индивидуальные права доступа, которые разбиты на три группы:

1. Доступ для пользователя-владельца файла (owner).
2. Доступ для группы-владельца файла (group).
3. Доступ для остальных пользователей (others).

Для каждой категории устанавливаются три вида доступа: (x) - право на запуск файла, (r) - право на чтение файла, (w) - право на изменение (редактирование) файла. Т. е. права доступа можно представить в виде битовой строки, в которой каждые 3 бита определяют права доступа для соответствующей категории пользователей. Эти биты отвечают за право на чтение, запись и исполнение файла или каталога. Если бит установлен в 1 – операция разрешена, если в 0 – запрещена. Т. о. права доступа к файлу или каталогу описываются тремя восьмеричными цифрами, самая левая из которых – права доступа владельца, средняя – права группы, правая – права доступа для всех остальных.

Право на чтение файла позволяет пользователю читать содержимое файла. Для каталога установка права на чтение позволяет читать файлы, находящиеся в этом каталоге.

Право на запись файла позволяет пользователю изменять его содержимое. Для каталога - создавать файлы внутри каталога.

Право на выполнение для файла позволяет запускать файл на выполнение в качестве программы. Для каталога установка этого права дает возможность пользователю входить в каталог и просматривать его содержимое.

Помимо прав доступа существуют так называемые модификаторы доступа. К наиболее используемым модификаторам доступа относятся SUID и SGID.

SUID. Если файлу установлен модификатор доступа SUID и файл исполняемый, то файл при запуске на выполнение получает не права пользователя, запустившего его, а права владельца файла. Такие приемы используются для того, чтобы пользователь мог работать с некоторыми системными файлами, владельцем которых является привилегированный пользователь. К примеру, для того, чтобы пользователь мог самостоятельно изменить свой пароль при помощи программы passwd, у этой программы, владельцем которой является пользователь root, должен быть установлен бит SUID, поскольку она работает с файлом shadow, модификацию которого имеет право производить только пользователь root.

SGID. Если файл имеет модификатор доступа SGID, то это аналогично установке бита SUID, только вместо владельца файла используется группа, которой принадлежит файл. В случае установки SGID для каталога файлы, содержащиеся в этом каталоге, будут иметь установки группы такие же, как у каталога.

Модификаторы доступа при правильном использовании представляют очень мощное и гибкое средство. С другой стороны, неправильная настройка системы с использованием этих модификаторов может свести все действия по обеспечению безопасности к нулю. Особенно опасной представляется ситуация, когда тот же SUID установлен на исполняемый файл, принадлежащий привилегированному пользователю. При выполнении файла запустивший его пользователь получает право выполнять операции, доступные только пользователю root. Если даже файл не выполняет никаких системных операций и не работает с системными файлами, неправильное его использование может привести к очень неприятным последствиям.

Примечание. Управление доступом к файловой системе возможно также с использованием ACL, подобно управлению в Windows. Однако для этого придется смонтировать файловую систему с определенными параметрами и установить дополнительные компоненты ОС.

4. Инструменты управления доступом к объектам в Windows

Управление доступом пользователей к локальной файловой системе можно осуществлять следующими способами:

1. Закладка «Безопасность» в диалоговом окне свойств папки или файла
2. Командная строка (CACLS)

Управление доступом пользователей к реестру можно осуществлять через стандартную утилиту Regedit.

Управление доступом пользователей к общим (сетевым) ресурсам можно осуществлять следующими способами:

1. Оснастка Общие папки (fsmgmt.msc)
2. Оснастка Управление компьютером (compmgmt.msc)
3. Закладка «Доступ» в диалоговом окне свойств файла или папки
4. Командная строка (NET FILE, NET SHARE, NET SESSION)
5. Инструменты управления доступом к объектам в Linux

Управление доступом пользователей к локальной файловой системе можно осуществлять следующими способами:

1. Закладка «Права» в диалоговом окне свойств папки или файла (Gnome)
2. Командная строка (ls -l, chmod)

Порядок выполнения работы

1. Изучить теоретический материал лабораторной работы.
2. Изучить управление доступом пользователей к локальной файловой системе Windows.

- через диалоговое окно свойств файловых объектов (папки, файлы)

Для вызова диалогового окна необходимо:

а) Нажать правой кнопкой мыши на защищаемом объекте (файле или папке) и выбрать «Свойства»

б) Перейти на закладку «Безопасность»

Примечание. Если закладка «Безопасность» в диалоговом окне отсутствует, то скорее всего необходимо отключить опцию «Использовать простой общий доступ» в настройках отображения папок. Для этого нажмите «Пуск» > Панель управления > Свойства папки. На закладке «Вид»уберите галочку «Использовать простой общий доступ» и нажмите «Применить».

- через командную строку

Для управления доступом пользователей к файловой системе необходимо:

а) Нажать Пуск > Выполнить

б) Набрать cmd и нажать ОК

в) Использовать команду CACLS

3. Изучить управление доступом к реестру Windows

Для управления доступом к реестру через Regedit необходимо:

а) Нажать Пуск > Выполнить

б) Набрать regedit и нажать ОК

в) Нажать правой кнопкой мыши на защищаемом объекте (разделе или ключе реестра) и выбрать «Разрешения»

4. Изучить управление доступом к общим (сетевым) ресурсам Windows

- через оснастку Общие папки

Для вызова оснастки необходимо:

а) Нажать Пуск > Выполнить

б) Набрать fsmgmt.msc и нажать ОК

- через диалоговое окно свойств файловых объектов (папки, файлы)

Для вызова диалогового окна необходимо:

а) Нажать правой кнопкой мыши на защищаемом объекте (файле или папке) и выбрать «Свойства»

б) Перейти на закладку «Доступ»

Примечание. Если закладка «Доступ» в диалоговом окне не позволяет настраивать общий доступ, то, скорее всего, необходимо отключить опцию «Использовать простой общий доступ» в настройках отображения папок. Для этого нажмите «Пуск» > Панель управления > Свойства папки. На закладке «Вид» уберите галочку «Использовать простой общий доступ» и нажмите «Применить».

- через командную строку

Для управления доступом к общим (сетевым) ресурсам через командную строку необходимо:

а) Нажать Пуск > Выполнить

б) Набрать cmd и нажать ОК

в) Использовать команды NET FILE, NET SHARE, NET SESSION

5. Изучить управление доступом пользователей к локальной файловой системе Linux.

- через командную строку

Для управления доступом пользователей к файловой системе необходимо:

а) В графическом режиме (например, в оболочке Gnome) выбрать Приложения -> Стандартные -> Root terminal

б) Ввести пароль учетной записи root

в) Использовать команды ls –l, chmod

2. Защита практической работы проводится в форме устного опроса после выполнения работы.

Критерии оценки практической работы

| Структура работы | Критерии оценки | Распределение баллов |
|---|---|---|

| | | |
|---|---|---|
| Одно практическое задание<br>Модуль 1<br>Модуль 2 | работа выполнена с ошибками и не получены ответы на все контрольные вопросы/ работа выполнена, но не получены ответы на все контрольные вопросы/ работа выполнена и получены ответы на все контрольные вопросы | <br>0/2/4<br>0/1/3 |

## 5. Учебно-методическое и информационное обеспечение дисциплины

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

**Основная литература**

1. Куль, Т. П. Операционные системы : учебное пособие : [16+] / Т. П. Куль. – Минск : РИПО, 2019. – 312 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=599951. – Библиогр. в кн. – ISBN 978-985-503-940-3. – Текст : электронный.
2. Басыня, Е. А. Системное администрирование и информационная безопасность : учебное пособие : [16+] / Е. А. Басыня. – Новосибирск : Новосибирский государственный технический университет, 2018. – 79 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=575325. – Библиогр. в кн. – ISBN 978-5-7782-3484-0. – Текст : электронный.

**Дополнительная литература**

3. Основы администрирования информационных систем : учебное пособие : [16+] / Д. О. Бобынцев, А. Л. Марухленко, Л. О. Марухленко и др. – Москва ; Берлин : Директ-Медиа, 2021. – 201 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=598955. – Библиогр. в кн. – ISBN 978-5-4499-1674-7. – DOI 10.23681/598955. – Текст : электронный.
4. Мартемьянов, Ю. Ф. Операционные системы. Концепции построения и обеспечения безопасности: учебное пособие для вузов / Ю. Ф. Мартемьянов, А. В. Яковлев, А. В. Яковлев. – Москва : Горячая линия – Телеком, 2010. – 316 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=253557. – Библиогр. в кн. – ISBN 978-5-9912-0128-5. – Текст : электронный.
5. Ложников, П. С. Средства безопасности операционной системы ROSA Linux : учебное пособие : [16+] / П. С. Ложников, А. О. Провоторский. – Омск : Омский государственный технический университет (ОмГТУ), 2017. – 94 с. : табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=493349. – Библиогр. в кн. – ISBN 978-5-8149-2502-2. – Текст : электронный.

### 5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы

1. Электронная библиотечная система «Университетская библиотека онлайн» - https://biblioclub.ru
2. Электронная библиотечная система «ЭБ БашГУ» - https://elib.bashedu.ru
3. Электронная библиотечная система БашГУ – www.bashlib.ru
4. Электронная библиотечная система издательства «Лань» - https://e.lanbook.com
5. Антиплагиат.ВУЗ. Договор № 81 от 27.04.2018 г. Срок действия лицензии до 04.05.2019 г.,

договор № 1104 от 18.04.2019 г. Срок действия лицензии до 04.05.2020 г

6. Банк нормативно-правовых актов РФ Министерства юстиции РФ - http://zakon.scli.ru/ru/legal_texts/index.php
7. Справочная правовая система Консультант Плюс. Договор №31705775411 от 07.12.2017 г. http://www.consultant-plus.ru
8. Национальные стандарты РФ в области информационной безопасности: http://www.iso27000.ru/standarty/gost-r-nacionalnye-standarty-rossiiskoi-federacii-v-oblasti-zaschity-informacii
9. Нормативные документы и материалы сайта ФСТЭК России (Федеральной службы по техническому и экспортному контролю России): https://fstec.ru/ Раздел «Национальные старты информационной безопасности» (https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/113-gosudarstvennye-standarty/377-gosudarstvennye-standarty )

**Государственные информационно-правовые системы:**

1. Научный центр правовой информации при министерстве Юстиций РФ - http://www.scli.ru
2. Официальный интернет-портал правовой информации - http://pravo.gov.ru
3. Информационно-правовая система «Законодательство России» - http://pravo.fso.gov.ru
4. Модуль «Документы - Президент России» - http://www.kremlin.ru/acts
5. Банк документов, подписанных Президентом России - http://kremlin.ru/acts/bank
6. База данных «Федеральные законы» - http://graph.garant.ru:8080/SESSION/PILOT/main.htm
7. Автоматизированная система обеспечения законодательной деятельности государственной думы (законопроекты и законодательные инициативы) - http://asozd.duma.gov.ru/
8. База данных «Издания по общественным и гуманитарным наукам» (на платформе East View) - Ссылка http://www.ebiblioteka.ru (вход из сети вуза без регистрации).
9. Банк данных "Библиотека копий официальных публикаций правовых актов» при ассоциации юристов России - http://alrf.consultant.ru/
10. Банк данных "Копии правовых актов: Российская Федерация» - http://giod.consultant.ru/
11. Банк данных "Нормативно-правовые акты Федерального Собрания Российской Федерации - http://duma.consultant.ru/

**Другие профессиональные базы данных и информационно-справочные системы:**

1. Электронная база данных диссертаций РГБ (авторизованный доступ по паролю в сети вуза) – Ссылка: http://dvs.rsl.ru
2. База данных «Вестники Московского университета» (на платформе East View) (вход без регистрации). - Ссылка http://www.ebiblioteka.ru/browse/udb/12.
3. Annual Reviews – обзор журналов по общественно-научной тематике и др. – доступ из сети вуза. – Ссылка: http://www.annualreviews.org/
4. Computers & Applied Sciences Complete (EBSCO) - доступ в сети вуза, язык английский. - Ссылка: http://search.ebscohost.com/
5. SCOPUS - наукометрическая, библиографическая и реферативная база данных издательской корпорации Elsevier. Язык английский, вход после регистрации или из сети вуза. – Ссылка: http://www.scopus.com/
6. Taylor and Francis – База полнотекстовых научных журналов, книг. Язык английский. – доступ из сети вуза. – Ссылка: http://www.tandf
7. Web of Science - наукометрическая, библиографическая и реферативная база данных издательской корпорации Thomson Reuters. Язык английский, вход после регистрации или из сети вуза. – Ссылка: http://apps.webofknowledge.com/
8. Wiley - Полнотекстовая база данных статей из 1400 журналов издательства Wiley по всем отраслям знаний. Язык английский. Доступ из сети вуза без регистрации. – Ссылка: http://onlinelibrary.wiley.com/

9. Сайт по информационной безопасности: http://securitypolicy.ru/; его раздел: «Документы, стандарты и методики по информационной безопасности»: http://securitypolicy.ru/
10. Докипедия: http://dokipedia.ru
11. Словари и энциклопедии On-Line- http://www.dic.academic.ru

**Программное обеспечение**

1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.
2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
3. Система централизованного тестирования БашГУ (Moodle).GNU General Public License. Лицензии бессрочные.

## 6.Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

| Наименование специальных помещений и помещений для самостоятельной работы | Вид Занятия | Оснащенность специальных помещений и помещений для самостоятельной работы |
|---|---|---|
| 1 | 2 | 3 |
| **1.** ***учебная аудитория для проведения занятий лекционного типа:*** аудитория № 403 (гуманитарный корпус), аудитория № 405 (гуманитарный корпус), аудитория № 413 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 515 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус).<br>**2.** ***учебная аудитория для проведения лабораторных работ:*** компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус).<br>**3.** ***учебная аудитория для проведения групповых и индивидуальных консультаций:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 | Лекции, практические занятия, самостоятельные работы, групповые и индивидуальные опросы | **Аудитория № 403**<br>Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия.<br>**Аудитория № 405**<br>Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт.<br>**Аудитория № 413**<br>Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт АРАРТ MA1225 – 1 шт.<br>**Аудитория № 415**<br>Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт АРАРТ MA1225 – 1 шт.<br>**Аудитория № 416**<br>Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт. |

| | | |
|---|---|---|
| (гуманитарный корпус).<br>**4.** ***учебная аудитория для текущего контроля и промежуточной аттестации:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус).<br>**5.** ***помещения для самостоятельной работы:*** читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус).<br>**6.** ***помещение для хранения и профилактического обслуживания учебного оборудования:***аудитория № 523 (гуманитарный корпус). | | **Аудитория № 418**<br>Учебная мебель, доска, Экран настенный Lumien Master Pikture 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт.<br>**Аудитория № 419**<br>Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт.<br>**Аудитория № 515**<br>Учебная мебель, доска, терминал видео конференц-связи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру IN-TEL Core i3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/Therm altake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром.<br>**Аудитория № 516**<br>Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран.<br>**Аудитория № 509**<br>Учебная мебель, доска, мобильное мультимедийное оборудование.<br>**Аудитория № 608**<br>Учебная мебель, доска, мобильное мультимедийное оборудование.<br>**Аудитория № 609**<br>Учебная мебель, доска, мобильное мультимедийное оборудование.<br>**Аудитория № 610**<br>Учебная мебель, доска, учебно-наглядные пособия, LED Телевизор TCLL55P6 USBLACK – 1 шт., кронштейн для телевизора NBP 5 – 1 шт., Кабель HDMI (m)-HDH(m)ver14,10м.<br>**Аудитория № 613**<br>Учебная мебель, доска, моноблок стационарный – 15 шт.<br>**Компьютерный класс аудитория № 420**<br>Учебная мебель, моноблоки стационарные 15 шт.<br>**Компьютерный класс аудитория № 404**<br>Учебная мебель, компьютеры -15 |

| | | |
|---|---|---|
| | | штук.<br>**Аудитория 402 читальный зал библиотеки**<br>Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные.<br>**Аудитория № 523**<br>Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт. |

Приложение № 1

ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

## СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины **Информационная безопасность операционных систем** на 3 семестр
___очная_ф/о___

| Вид работы | Объем дисциплины |
|---|---|
| Общая трудоемкость дисциплины (ЗЕТ / часов) | 3 ЗЕТ / 108 часов |
| Учебных часов на контактную работу с преподавателем: | 55,2 |
| лекций | 18 |
| практических/ семинарских | 18 |
| лабораторных | 18 |
| других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР) | 1,2 |
| из них, предусмотренные на выполнение курсовой работы / курсового проекта | – |
| Учебных часов на самостоятельную работу обучающихся (СР) | 16,8 |
| из них, предусмотренные на выполнение курсовой работы / курсового проекта | – |
| Учебных часов на подготовку к зачету (Контроль) | 36 |

Форма контроля
Экзамен 3 семестр

**Семестр 3**

| № | Тема и содержание | Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах) | | | | Задания по самостоятельной работе студентов | Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.) |
|---|---|---|---|---|---|---|---|
| | | ЛК | ПР / СЕМ | ЛР | СР | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 8 | 9 |
| 1 | Модуль 1. Архитектура операционных систем.<br>Тема: Принципы построения операционных систем.<br>Тема: Интерфейсы операционных систем.<br>Тема: Конфигурирование операционных систем.<br>Тема: Управление памятью и процессами в операционных системах. Управление файлами и вводом-выводом в операционных системах. Подсистема протоколирования.<br>Тема: Коммуникационных возможности операционных систем | <br>2<br>2<br>2<br>2<br>2 | <br>2<br>2<br>2<br>2<br>2 | <br>2<br>2<br>2<br>4<br> | <br>1<br>2<br>2<br>2<br>2 | Самостоятельное изучение рекомендуемой основной и дополнительной литературы | практическая работа, лабораторная работа, тест |
| 2 | Модуль 2. Защита информации в современных операционных системах.<br>Тема: Основные понятия и положения защиты информации в информационно-вычислительных системах.<br>Тема: Идентификация и аутентификация пользователей в операционных системах. Угрозы безопасности информации в информационно- | <br>2<br>2 | <br>2<br>2 | <br>2<br>2 | <br>2<br>2 | Самостоятельное изучение рекомендуемой основной и дополнительной литературы | практическая работа, лабораторная работа, тест |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | вычислительных системах. | | | | | | |
| | Тема: Требования к защите компьютерной информации. Модели безопасности основных операционных систем. | 2 | 2 | 2 | 2 | | |
| | Тема: Анализ защищенности современных операционных систем. Системы защиты программного обеспечения. Протоколирование и аудит. | 2 | 2 | 2 | 1,8 | | |
| Всего часов | | 18 | 18 | 18 | 16,8 | | |