МИНОБРНАУКИ РОССИИ
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**
**«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**
**(ФГБОУ ВО «ВГУ»)**

**УТВЕРЖДАЮ**
заведующий кафедрой
кибербезопасности
информационных систем
С.Л. Кенин

22.03.2024

# РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
# Б1.О.41 Защита в операционных системах

**1. Код и наименование направления подготовки/специальности:**

**10.05.01 Компьютерная безопасность**

**2. Профиль подготовки / специализация / магистерская программа:**

**Безопасность компьютерных систем и сетей**

**Математические методы защиты информации**

**3. Квалификация (степень) выпускника: специалист**

**4. Форма обучения: очная**

**5. Кафедра, отвечающая за реализацию дисциплины: кибербезопасности информационных систем**

**6. Составители программы: Сафронов Виталий Владимирович, к.т.н, доцент кафедры кибербезопасности информационных систем**

**7. Рекомендована: НМС факультета ПММ, протокол № 5 от 22.03.2024**

_____

*отметки о продлении вносятся вручную)*

**8. Учебный год: 2026/2027** **Семестр(ы): 6**

**9**.**Цели и задачи учебной дисциплины:**

*Целями освоения учебной дисциплины являются:*

изучение принципов и методов оценки безопасности компьютерных систем на основе комплексного подхода к определению актуальных угроз безопасности в таких системах в рамках обеспечения безопасности информационных систем и технологий в целом, изучение математических основ моделирования процессов оценки безопасности компьютерных систем, получение профессиональных компетенций в области современных технологий оценки безопасности компьютерных систем.

*Задачи учебной дисциплины:*

- обучение студентов базовым понятиям современных методов оценки безопасности компьютерных систем;
- обучение студентов базовым методам оценки безопасности компьютерных систем;
- овладение практическими навыками применения методов оценки безопасности компьютерных систем;
- раскрытие физической сущности построения и эксплуатации компьютерных систем с точки зрения определения актуальных угроз безопасности в таких системах с целью корректного решения задач по применению методов оценки безопасности компьютерных систем.

**10. Место учебной дисциплины в структуре ОПОП**:

обязательная часть блока Б1

**11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников) и индикаторами их достижения**:

| Код и название компетенции | Код и название индикатора компетенции | Знания, умения, навыки |
|---|---|---|
| ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации; | ОПК-9.11 знает основные тенденции развития методов защиты информации в операционных системах и системах управления базами данных | Знает основные тенденции развития методов защиты информации в операционных системах и системах управления базами данных |
| ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации; | ОПК-9.12 знает общие и специфические угрозы безопасности операционных систем и систем управления баз данных; | Знает общие и специфические угрозы безопасности операционных систем и систем управления баз данных |

| | | |
|---|---|---|
| ОПК-11 Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации; | ОПК-11.6 знает средства и методы хранения и передачи аутентификационной информации | Знает средства и методы хранения и передачи аутентификационной информации |
| ОПК-11 Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации; | ОПК-11.7 знает основные требования к подсистеме аудита и политике аудита | Знает основные требования к подсистеме аудита и политике аудита |
| ОПК-11 Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации; | ОПК-11.8 знает защитные механизмы и средства обеспечения безопасности операционных систем | Знает защитные механизмы и средства обеспечения безопасности операционных систем |
| ОПК-11 Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации; | ОПК-11.9 умеет формулировать и настраивать политику безопасности основных операционных систем | Умеет формулировать и настраивать политику безопасности основных операционных систем |
| ОПК-11 Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации; | ОПК-11.10 умеет формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем | Умеет формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем |
| ОПК-12 Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения; | ОПК-12.2 знает принципы разработки специального программного обеспечения, предназначенного для преодоления защиты современных операционных систем с использованием их недокументированных возможностей. | Знает принципы разработки специального программного обеспечения, предназначенного для преодоления защиты современных операционных систем |
| ОПК-12 Способен администрировать операционные системы и выполнять работы по восстановлению | ОПК-12.4 владеет навыками системного программирования | Владеет навыками системного программирования |

| | | |
|---|---|---|
| работоспособности прикладного и системного программного обеспечения; | | |
| ОПК-13 Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности; | ОПК-13.1 умеет формулировать и настраивать политику безопасности основных операционных систем | Умеет формулировать и настраивать политику безопасности основных операционных систем |
| ОПК-13 Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности; | ОПК-13.2 владеет навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств | Владеет навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств |

## 12. Объем дисциплины в зачетных единицах/час:

3/108

## Форма промежуточной аттестации:

Зачет с оценкой

## 13.Трудоемкость по видам учебной работы

| Вид учебной работы | | Семестр 6 | Всего |
|---|---|---|---|
| Аудиторные занятия | | 72 | 72 |
| Лекционные занятия | | 36 | 36 |
| Практические занятия | | 0 | 0 |
| Лабораторные занятия | | 36 | 36 |
| Самостоятельная работа | | 36 | 36 |
| Курсовая работа | | | 0 |
| Промежуточная аттестация | | 0 | 0 |
| Часы на контроль | | | 0 |
| Всего | | 108 | 108 |

### 13.1 Содержание дисциплины

| п/п | Наименование раздела дисциплины | Содержание раздела дисциплины | Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК |
|---|---|---|---|
| **1. Лекции** | | | |
| 1.1 | Основы защиты информации в операционных системах | Общие требования к защите информации, технические и административные методы защиты, уровни доверия, политики безопасности, профили защиты | https://edu.vsu.ru/course/ |

| | | | |
|---|---|---|---|
| 1.2 | Управление доступом | Объекты, субъекты и методы доступа, модели управления доступом, изолированная программная среда | https://edu.vsu.ru/course/ |
| 1.3 | Аутентификация пользователей и проверка целостности информации | Факторы аутентификации, хранение паролей, аутентификация по открытому каналу, одноразовые пароли, многофакторная аутентификация | https://edu.vsu.ru/course/ |
| 1.4 | Разграничение доступа в Unix и Unix-подобных системах | Базовая модель разграничения доступа в UNIX-подобных системах, учет пользователей и хранение паролей, регистрация пользователей и вход в систему, PAM | https://edu.vsu.ru/course/ |
| 1.5 | Методы защиты информации в Linux | Возможности (capabilities) потоков в Linux, управление возможностями, списки контроля доступа Linux, дополнительные атрибуты файлов, изоляция (пространства имен) в Linux, система sudo, seccomp, SELinux, AppArmor | https://edu.vsu.ru/course/ |
| 1.6 | Методы защиты информации в Windows | Дескрипторы защиты и маркеры доступа, олицетворение, списки контроля доступа в Windows | https://edu.vsu.ru/course/ |
| 1.7 | Основы сетевой безопасности | Межсетевой экран Linux и Windows | https://edu.vsu.ru/course/ |
| 1.8 | Аудит в операционных системах | Журналы аудита Linux и Windows, фильтры аудита | https://edu.vsu.ru/course/ |
| **2. Практические занятия** | | | |
| **3. Лабораторные работы** | | | |
| 3.1 | Управление пользователями в Linux | Создание учетной записи, присоединение к группе, замена | https://edu.vsu.ru/course/ |

| | | | |
|---|---|---|---|
| | | программы (оболочки) пользователя, создание псевдопользователя для запуска программы | |
| 3.2 | Контроль целостности файлов в Linux | Вычисление и проверка контрольной суммы, проверка целостности программы при запуске | https://edu.vsu.ru/course/ |
| 3.3 | Изучение PAM | Реализация модуля PAM, реализующего аутентификацию по серийному номеру устройства USB | https://edu.vsu.ru/course/ |
| 3.4 | Изучение возможностей (capabilities) Linux | Установка возможностей программы для выполнения привилегированных действий без использования root | https://edu.vsu.ru/course/ |
| 3.5 | Изучение изоляции ресурсов Linux | Создание изолированной сетевой среды, создание сетевого туннеля для доступа к изолированной среде, утилита unshare, файловая система /sys/fs/cgroup/ | https://edu.vsu.ru/course/ |
| 3.6 | Изучение подсистемы sudo | Создание правила для конкретного пользователя | https://edu.vsu.ru/course/ |
| 3.7 | Изучение подсистемы seccomp | Ограничение запуска программ и доступа к файлам за счет реализации фильтра системных вызовов | https://edu.vsu.ru/course/ |
| 3.8 | Изучение межсетевого экрана Linux | Создание правил для netfilter, ограничивающих доступ к отдельным сетевым протоколам и портам | https://edu.vsu.ru/course/ |
| 3.9 | Изучение механизмов ограничения запуска программ в Windows | Создание правил политики ограничения запуска программ | https://edu.vsu.ru/course/ |
| 3.10 | Изучение межсетевого экрана Windows | Создание правил для netfilter, ограничивающих доступ к отдельным сетевым протоколам и портам | https://edu.vsu.ru/course/ |

## 13.2 Темы (разделы) дисциплины и виды занятий

| № п/п | Наименование темы (раздела) | Лекционные занятия | Практические занятия | Лабораторные занятия | Самостоятельная работа | Всего |
|---|---|---|---|---|---|---|
| 1 | Основы защиты информации в операционных системах | 4 | 0 | 0 | 2 | 6 |
| 2 | Управление доступом | 2 | 0 | 0 | 2 | 4 |
| 3 | Аутентификация пользователей и проверка целостности информации | 4 | 0 | 0 | 2 | 6 |
| 4 | Разграничение доступа в Unix и Unix-подобных системах | 4 | 0 | 0 | 2 | 6 |
| 5 | Методы защиты информации в Linux | 6 | 0 | 0 | 2 | 8 |
| 6 | Методы защиты информации в Windows | 6 | 0 | 0 | 2 | 8 |
| 7 | Основы сетевой безопасности | 6 | 0 | 0 | 2 | 8 |
| 8 | Аудит в операционных системах | 4 | 0 | 0 | 2 | 6 |
| 9 | Управление пользователями в Linux | 0 | 0 | 2 | 2 | 4 |
| 10 | Контроль целостности файлов в Linux | 0 | 0 | 2 | 2 | 4 |
| 11 | Изучение PAM | 0 | 0 | 4 | 2 | 6 |
| 12 | Изучение возможностей (capabilities) Linux | 0 | 0 | 4 | 2 | 6 |
| 13 | Изучение изоляции ресурсов Linux | 0 | 0 | 6 | 2 | 8 |
| 14 | Изучение подсистемы sudo | 0 | 0 | 4 | 2 | 6 |
| 15 | Изучение подсистемы seccomp | 0 | 0 | 4 | 2 | 6 |
| 16 | Изучение механизмов ограничения запуска программ в Windows | | | 2 | 2 | 4 |

| № п/п | Наименование темы (раздела) | Лекционные занятия | Практические занятия | Лабораторные занятия | Самостоятельная работа | Всего |
|---|---|---|---|---|---|---|
| 17 | Изучение межсетевого экрана Linux | 0 | 0 | 4 | 2 | 6 |
| 18 | Изучение межсетевого экрана Windows | 0 | 0 | 4 | 2 | 6 |
| | | 36 | 0 | 36 | 36 | 108 |

## 14. Методические указания для обучающихся по освоению дисциплины

Работа с конспектами лекций, выполнение лабораторных заданий, заданий текущей и промежуточной аттестаций.

При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей по работе на LMS-платформе, своевременно подключаться к online-занятиям, соблюдать рекомендации по организации самостоятельной работы

.

## 15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

| № п/п | Источник |
|---|---|
| 1 | Технологии обеспечения безопасности информационных систем : учебное пособие / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов и др. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. // ЭБС Университетская библиотека. – URL: https://biblioclub.ru/index.php?page=book_red&id=598988 |

б) дополнительная литература:

| № п/п | Источник |
|---|---|
| 1 | Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова ; Самарский государственный архитектурно-строительный университет. – Самара : Самарский государственный архитектурно-строительный университет, 2014. – 113 с. // ЭБС Университетская библиотека. – URL: https://biblioclub.ru/index.php?page=book&id=438331 |

в) информационные электронно-образовательные ресурсы:

| № п/п | Источник |
|---|---|
| 1 | Библиотека ВГУ, http://www.lib.vsu.ru |
| 2 | Образовательный портал "Электронный университет ВГУ", http://edu.vsu.ru |

## 16. Перечень учебно-методического обеспечения для самостоятельной работы

| № п/п | Источник |
|---|---|
| 1 | Образовательный портал "Электронный университет ВГУ", http://edu.vsu.ru |

## 17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):

При реализации дисциплины используются модульно-рейтинговая и личностно-ориентированные технологии обучения (ориентированные на индивидуальность студента, компьютерные и коммуникационные технологии). В рамках дисциплины предусмотрены следующие виды лекций: информационная, лекция-визуализация, лекция с применением обратной связи.

Дисциплина реализуется с применением электронного обучения и дистанционных образовательных технологий, для организации самостоятельной работы обучающихся используется онлайн-курс, размещенный на платформе Электронного университета ВГУ (LMS moodle), а также другие Интернет-ресурсы, приведенные в п.15в

## 18. Материально-техническое обеспечение дисциплины:

Лекционная аудитория должна быть оборудована учебной мебелью, компьютером, мультимедийным оборудованием (проектор, экран, средства звуковоспроизведения), допускается переносное оборудование.

Лабораторные занятия должны проводиться в специализированной аудитории, оснащенной учебной мебелью и персональными компьютерами с доступом в сеть Интернет (компьютерные классы, студии), мультимедийным оборудованием (мультимедийный проектор, экран, средства звуковоспроизведения). Число рабочих мест в аудитории должно быть таким, чтобы обеспечивалась индивидуальная работа студента на отдельном персональном компьютере.

Для самостоятельной работы необходимы компьютерные классы, помещения, оснащенные компьютерами с доступом к сети Интернет.

Программное обеспечение (см. файл МТО):
ОС GNU/Linux;

ОС Windows 8 (10).

## 19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

| № п/п | Разделы дисциплины (модули) | Код компетенции | Код индикатора | Оценочные средства для текущей аттестации |
|---|---|---|---|---|
| 1 | Основы защиты информации в операционных системах | ОПК-9 | ОПК-9.11 | КИМы для проведения текущей аттестации собеседования |
| 2 | Основы защиты информации в операционных системах | ОПК-9 | ОПК-9.12 | КИМы для проведения текущей аттестации собеседования |
| 3 | Аутентификация пользователей и проверка целостности информации | ОПК-11 | ОПК-11.6 | КИМы для проведения текущей аттестации собеседования |
| 4 | Аудит в операционных системах | ОПК-11 | ОПК-11.7 | КИМы для проведения текущей аттестации собеседования |
| 5 | Управление доступом<br>Разграничение доступа в Unix и Unix-подобных системах<br>Методы защиты информации в Linux<br>Методы защиты информации в Windows<br>Основы сетевой безопасности | ОПК-11 | ОПК-11.8 | КИМы для проведения текущей аттестации собеседования |

| | | | | |
|---|---|---|---|---|
| 6 | Управление пользователями в Linux<br>Изучение подсистемы sudo<br>Контроль целостности файлов в Linux | ОПК-11 | ОПК-11.9 | Лабораторные работы |
| 7 | Изучение межсетевого экрана Linux<br>Изучение межсетевого экрана Windows | ОПК-11 | ОПК-11.10 | Лабораторные работы |
| 8 | Методы защиты информации в Linux<br>Методы защиты информации в Windows | ОПК-12 | ОПК-12.2 | КИМы для проведения текущей аттестации собеседования |
| 9 | Изучение возможностей (capabilities) Linux<br>Изучение изоляции ресурсов Linux<br>Изучение подсистемы seccomp | ОПК-12 | ОПК-12.4 | Лабораторные работы |
| 10 | Управление пользователями в Linux<br>Изучение подсистемы sudo<br>Изучение механизмов ограничения запуска программ в Windows | ОПК-13 | ОПК-13.1 | Лабораторные работы |
| 11 | Изучение PAM | ОПК-13 | ОПК-13.2 | Лабораторные работы |

Промежуточная аттестация

Форма контроля - Зачет с оценкой, Контрольная работа

**Оценочные средства для промежуточной аттестации**

1. Собеседование
2. Контрольная работа

## 20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах: устного опроса; защиты лабораторных работ, выполнения контрольных работ.

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования. Промежуточная аттестация по итогам освоения дисциплины проводится в форме зачета с оценкой и экзамена. Для получения положительной итоговой оценки необходимо выполнение всех лабораторных и контрольных работ.

### 20.1. Текущий контроль успеваемости

Текущий контроль успеваемости выполняется по лабораторным работам.

По каждой выполненной работе должен быть предоставлен отчет, включающий исходный код разработанных программ и описание полученных результатов. По отчету преподаватель вправе задать дополнительные
вопросы для уточнения уровня понимания материала. Лабораторная работа оценивается максимум в 100 баллов.

### 20.2. Промежуточная аттестация

#### Задания к контрольной работе

1. В операционной системе GNU/Linux создайте учетную запись псевдопользователя для запуска программы
   date
2. В операционной системе GNU/Linux определите правило sudo, которое позволяет пользователю user1 выполнять от имени user2 команды mkdir и rmdir
3. В операционной системе MS Windows создайте учетную запись пользователя Windows и разрешите ему вход в систему только с понедельника по пятницу с 8 до 17 часов
4. В операционной системе GNU/Linux определите правило sudo, которое позволяет членам группы operaror выполнять команды /mount и /umount без ввода пароля
5. В операционной системе GNU/Linux создайте правило межсетевого экрана для запрета доступа с локального компьютера к сайту www.anekdot.ru
6. В операционной системе MS Windows с использованием командной строки создайте правило брэндмауэра для блокировки входящих эхо-запросов в публичных сетях
7. В операционной системе GNU/Linux создайте учетную запись пользователя с созданием пароля при первом входе пользователя в систему и ограничьте срок действия пароля до 10 дней
8. В операционной системе MS Windows создайте учетную запись нового пользователя Windows и ограничьте срок ее действия до 10 дней
9. В операционной системе MS Windows запретите запуск редактора реестра
10. В операционной системе GNU/Linux создайте сообщение, которое будет отображаться в консоли при каждом входе пользователя в систему

#### Описание технологии проведения

Контрольные работы выполняются на компьютере и на проверку сдается исходный код или листинг команды интерфейса командной строки

#### Требования к выполнению заданий (или шкалы и критерии оценивания)

В контрольной работе все задания оцениваются в 5 баллов (максимально возможная сумма при выполнении всех заданий – 50 баллов). При ошибках в выполнении задания или не полном выполнении оценка за задание снижается. Оценка за контрольную работу определяется как сумма баллов, набранных за все задания.

#### Перечень вопросов к собеседованию

1. Общие требования к защите информации. Технические и административные методы защиты.
2. Политика безопасности.
3. Уровень доверия. Оценочные уровни доверия. Профиль защиты.
4. Управление доступом. Объекты, субъекты, методы доступа. Право доступа. Привилегия. Полномочия. Роль. Суперпользователь.
5. Типовые модели управления доступом (дать общее определение дискреционного управления доступом, мандатного управление доступом и изолированной программной среды)

6. Дискреционное управление доступом. Матрица доступа. Мандат возможностей. Список контроля доступа.
7. Мандатное управление доступом. Модель Белла-Лападулы.
8. Изолированная программная среда.
9. Аутентификация пользователей. Факторы аутентификации. Одноразовый пароль.
10. Многофакторная аутентификация. Хранение паролей.
11. Алгоритм проверки целостности HMAC.
12. Аутентификация HOTP на основе одноразовых паролей.
13. Аутентификация TOTP на основе одноразовых паролей.
14. Алгоритм OCRA - алгоритм взаимной аутентификации на основе взаимодействия запросответ.
15. Базовая модель разграничения доступа в UNIX-подобный системах. Маска доступа для файлов и каталогов.
16. Учет пользователей в UNIX-подобный системах. Файл /etc/passwd. Учет групп. Хранение паролей в UNIX-подобный системах.
17. Псевдопользователи. Стандартные пользователи и группы в UNIX-подобный системах. Создание нового пользователя.
18. Файлы конфигурации системы учета пользователей в Linux. Инициализация домашнего каталога нового пользователя. Стандартные утилиты управления учетными записями в Linux.
19. Linux: Вход пользователя в систему.
20. PAM. Модули PAM. Конфигурация PAM. Критерии успешной аутентификации. Расширенный стиль конфигурации в Linux.
21. Списки контроля доступа и дополнительные атрибуты файлов в файловых системах Linux.
22. Система sudo. Правила sudo. Файл sudoers. Журнал sudo.
23. Обязательный контроль целостности и контроль учетных записей в Windows
24. Ограничение использования приложений в Windows
25. Межсетевой экран Linux
26. Межсетевой экран Windows
27. Аудит безопасности в Linux
28. Аудит безопасности в Windows

**Описание технологии проведения**

Собеседование производится в форме устного ответа на заданный вопрос. При необходимости преподаватель может задавать уточняющие вопросы.

**Требования к выполнению заданий, шкалы и критерии оценивания**

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины, осуществляется в ходе текущей и промежуточной аттестаций. При оценивании результатов промежуточной аттестации используется количественная шкала оценок. Оценки за контрольную работу и лабораторные работы складываются с оценкой, полученной на собеседовании, результат нормируется к 100 бальной шкале. Полученное значение определяет уровень сформированности компетенций и итоговую оценку (достаточный – удовлетворительно, хорошо, отлично или недостаточный – неудовлетворительно) согласно следующей шкале:

- оценка «отлично» – 90…100 баллов
- оценка «хорошо» – 70…89 баллов
- оценка «удовлетворительно» – 50...69 баллов
- оценка «неудовлетворительно» – 0...49 баллов

## 20.3 Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

**ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации;**

1) закрытые задания (тестовые, средний уровень сложности):

### Аудит безопасности

| | | | |
|---|---|---|---|
| Аудит системных событий в операционной системе позволяет | | | *MA* |
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Показать количество правильных ответов после окончания:** | Да |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| # | **Ответы** | **Отзыв** | **Оценка** |
| A. | Своевременно обнаружить попытки нарушений политики безопасности | | *33.3* |
| B. | Своевременно обнаружить изменения важных для безопасности системных настроек | | *33.3* |
| C. | Своевременно обнаружить изменения режима доступа к объектам или возможностей пользователей | | *33.3* |
| D. | Запретить запуск указанных программ с идентификацией программ по расположению в файловой системе или по хэш-коду файла программы | | *-100* |
| | **Общий отзыв к вопросу:** | | |
| | **Для любого правильного ответа:** | Ваш ответ верный. | |
| | **Для любого неправильного ответа:** | Ваш ответ неправильный. | |
| | **Для любого частично правильного ответа:** | Ваш ответ частично правильный. | |
| | **Подсказка 1:** | | |
| | **Показать количество правильных ответов (Подсказка 1):** | Нет | |
| | **Удалить некорректные ответы (Подсказка 1):** | Нет | |
| | **Теги:** | | |
| *Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)* | | | |

### Защита в Linux

| | | | |
|---|---|---|---|
| Возможности (capabilities) потоков в Linux позволяют | | | *MC* |
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| # | **Ответы** | **Отзыв** | **Оценка** |

| | | | |
|---|---|---|---|
| | Возможности (capabilities) потоков в Linux позволяют | | *MC* |
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| **#** | **Ответы** | **Отзыв** | **Оценка** |
| A. | Разделить возможности суперпользователя на несколько отдельных возможностей, которые могут быть разрешены независимо на уровне потока | | *100* |
| B. | Ограничить использование потоком процессорного времени | | *0* |
| C. | Разрешить прямой доступ к объектам ядра | | *0* |
| | **Общий отзыв к вопросу:** | | |
| | **Для любого правильного ответа:** | Ваш ответ верный. | |
| | **Для любого неправильного ответа:** | Ваш ответ неправильный. | |
| | **Подсказка 1:** | | |
| | **Показать количество правильных ответов (Подсказка 1):** | Нет | |
| | **Удалить некорректные ответы (Подсказка 1):** | Нет | |
| | **Теги:** | | |
| *Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)* | | | |

## Защита в MS Windows

| | | | |
|---|---|---|---|
| | В MS Windows под термином олицетворение (impersonation) понимают | | *MC* |
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| **#** | **Ответы** | **Отзыв** | **Оценка** |
| A. | Возможность выполнения потока в контексте безопасности, отличном от контекста безопасности своего процесса | | *100* |
| B. | Возможность идентифицировать владельца потока | | *0* |
| C. | Возможность удаленного запуска потока с использованием механизма RPC | | *0* |
| | **Общий отзыв к вопросу:** | | |
| | **Для любого правильного ответа:** | Ваш ответ верный. | |
| | **Для любого неправильного ответа:** | Ваш ответ неправильный. | |
| | **Подсказка 1:** | | |
| | **Показать количество правильных ответов (Подсказка 1):** | Нет | |
| | **Удалить некорректные ответы (Подсказка 1):** | Нет | |
| | **Теги:** | | |
| *Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)* | | | |

## Защита в MS Windows

| | | | |
|---|---|---|---|
| | Контроль учетных записей (User Account Control, UAC) в MS Windows реализует | | *MC* |
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| **#** | **Ответы** | **Отзыв** | **Оценка** |

| | | | |
|---|---|---|---|
| | Контроль учетных записей (User Account Control, UAC) в MS Windows реализует | | *MC* |
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| # | **Ответы** | **Отзыв** | **Оценка** |
| A. | Механизм защиты от вредоносных программ | | *100* |
| B. | Ограничение срока действия учетной записи | | *0* |
| C. | Контроль уровеня доверия к учетной записи | | *0* |
| | **Общий отзыв к вопросу:** | | |
| | **Для любого правильного ответа:** | Ваш ответ верный. | |
| | **Для любого неправильного ответа:** | Ваш ответ неправильный. | |
| | **Подсказка 1:** | | |
| | **Показать количество правильных ответов (Подсказка 1):** | Нет | |
| | **Удалить некорректные ответы (Подсказка 1):** | Нет | |
| | **Теги:** | | |
| *Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)* | | | |

## Защита в MS Windows

| | | | |
|---|---|---|---|
| | При одновременном присутствии в списке контроля доступа разрешающей и запрещающей записи по одному и тому же виду доступа для одного и того же субъекта доступа в современных реализациях ОС MS Windows | | *MC* |
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| # | **Ответы** | **Отзыв** | **Оценка** |
| A. | Запрещающая запись имеет приоритет | | *100* |
| B. | Разрешающая запись имеет приоритет | | *0* |
| C. | Поведение системы не определено | | *0* |
| | **Общий отзыв к вопросу:** | | |
| | **Для любого правильного ответа:** | Ваш ответ верный. | |
| | **Для любого неправильного ответа:** | Ваш ответ неправильный. | |
| | **Подсказка 1:** | | |
| | **Показать количество правильных ответов (Подсказка 1):** | Нет | |
| | **Удалить некорректные ответы (Подсказка 1):** | Нет | |
| | **Теги:** | | |
| *Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)* | | | |

2) открытые задания (мини-кейсы, средний уровень сложности):

| |
|---|
| Подключаемые модули аутентификации (Pluggable Authentication Modules, PAM) в Linux. Архитектура и основные принципы работы. |

| | Шаблон ответа | Информация для оценивающих |
|---|---|---|
| | | Подключаемые модули аутентификации позволяют унифицировать решение задачи аутентификации пользователей для всех приложений в системе. Исключается дублирование кода, снижается вероятность наличия необнаруженных ошибок и уязвимостей. Архитектура PAM включает стандартный API для аутентификации пользователей, единую конфигурацию и набор модулей ядра, фактически выполняющих проверки.<br>Определено 4 типа модулей<br>• Модули аутентификации (auth) - выполняют аутентификацию на основе учетных данных пользователей и признаков аутентификации (token)<br>• Модули управления учетными записями (account) - используются после успешной аутентификации для дополнительной проверки специальных ограничений (например, разрешенное время работы)<br>• Модули управления сеансами (session) - используются после успешной аутентификации для инициализации рабочего окружения пользователя<br>• Модули управления паролями (password) - позволяют сменить аутентификации (token)<br>Аутентификация в PAM выполняется в соответствии с заданным сценарием и может задействовать несколько модулей. Сценарий аутентификации описывается в текстовом файле. Каждая строка файла сценария имеет формат: type control module-path module-arguments, здесь type - тип модуля: auth, account, session или password; control – флаг, который определяет, как следует реагировать на отказ или успех аутентификации при выполнении модуля (requisite (необходимый), required (требуемый), sufficient (достаточный) или optional (необязательный)); module-path – файл модуля; module-arguments – необязательное поле параметров модуля.<br>Критерии успешной аутентификации<br>• Все необходимые (requisite) и требуемые (required) модули в списке завершились успешно. Если необходимый модуль завершился с ошибкой, дальнейшее выполнение сценария прекращается<br>• Достаточный (sufficient) модуль выполнился успешно и все предшествующие требуемые модули завершились успешно, при этом дальнейшее выполнение сценария прекращается<br>• В сценарии нет необходимых и требуемых модулей и хотя бы один необязательный (optional) модуль завершился успешно, при этом сценарий выполняется полностью<br>Обучающийся описал архитектуру PAM, перечислил состав и назначение модулей, объяснил структуру файла сценария, описал действие флагов и критерии успешной аутентификации - 3 балла<br>Обучающийся описал архитектуру PAM, перечислил состав и назначение модулей, объяснил структуру файла сценария, описал действие флагов и критерии успешной аутентификации. Ответ содержит незначительные неточности - 2 балла<br>Обучающийся не полно описал архитектуру PAM, не перечислил все возможные типы модулей PAM, не полно объяснил структуру файла сценария, не описал действие флагов модулей. Ответ не содержит грубых ошибок или неточностей - 1 балл<br>Обучающийся не полно описал архитектуру PAM, не перечислил все возможные типы модулей PAM, не полно объяснил структуру файла сценария, не описал действие флагов модулей и критерии успешной аутентификации. Ответ содержит грубые ошибки и неточности - 0 баллов |

| |
|---|
| Учет пользователей и хранение паролей в операционных системах GNU/Linux. |

| | Шаблон ответа | Информация для оценивающих |
|---|---|---|
| | | В операционных системах GNU/Linux список зарегистрированных пользователей хранится в текстовом файле /etc/passwd. Одна строка файла описывает одного пользователя и содержит логин пользователя, хэш пароля, идентификатор пользователя и его первичной группы, произвольный комментарий, путь к домашнему каталогу пользователя и имя программы, которая должна быть запущена после интерактивного входа пользователя в систему. Файл /etc/passwd доступен на чтение всем, поэтому в современных реализациях операционных систем хэши паролей обычно выносятся из /etc/passwd в более защищенный файл, например /etc/shadow в Ubuntu, чтобы исключить подбор пароля под хэш.<br>Обучающийся точно описал модель учета пользователей и хранения паролей. Описал формат файла /etc/passwd, обосновал целесообразность хранения хэшей паролей в отдельном файле - 3 балла.<br>Обучающийся точно описал модель учета пользователей и хранения паролей. Описал формат файла /etc/passwd, обосновал целесообразность хранения хэшей паролей в отдельном файле. Ответ содержит незначительные неточности - 2 балла.<br>Обучающийся не полно описал модель учета пользователей и хранения паролей. Фрагментарно описал формат файла /etc/passwd, не полно обосновал целесообразность хранения хэшей паролей в отдельном файле. Ответ не содержит грубых ошибок и неточностей - 1 балл<br>Обучающийся не полно описал модель учета пользователей и хранения паролей. Фрагментарно описал формат файла /etc/passwd, не полно обосновал целесообразность хранения хэшей паролей в отдельном файле. Ответ содержит грубые ошибки или неточности - 0 баллов. |

**ОПК-11 Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации;**

1) закрытые задания (тестовые, средний уровень сложности):

## Защита в UNIX-подобных системах

| | | | |
|---|---|---|---|
| | В UNIX-подобных системах атрибут разрешение исполнения (x) применительно к каталогу разрешает | | *MC* |
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| # | **Ответы** | **Отзыв** | **Оценка** |
| A. | Получить список имен файлов из каталога | | *0* |
| B. | Создавать файлы в каталоге | | *0* |
| C. | Удалять файлы в каталоге | | *0* |
| D. | Переходить в каталог | | *100* |
| | **Общий отзыв к вопросу:** | | |
| | **Для любого правильного ответа:** | Ваш ответ верный. | |
| | **Для любого неправильного ответа:** | Ваш ответ неправильный. | |
| | **Подсказка 1:** | | |
| | **Показать количество правильных ответов (Подсказка 1):** | Нет | |
| | **Удалить некорректные ответы (Подсказка 1):** | Нет | |
| | **Теги:** | | |
| *Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)* | | | |

## Защита в UNIX-подобных системах

| | | | |
|---|---|---|---|
| | Выберите критерии успешной аутентификации пользователя при использовании модели PAM (Pluggable Authentication Modules) | | *MA* |
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Показать количество правильных ответов после окончания:** | Да |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| # | **Ответы** | **Отзыв** | **Оценка** |
| A. | Все необходимые (requisite) и требуемые (required) модули в списке завершились успешно | | *50* |
| B. | Достаточный (sufficient) модуль выполнился успешно и все предшествующие требуемые (required) модули завершились успешно | | *50* |
| C. | Хотя бы один необходимый (requisite) модуль завершился успешно | | *-50* |
| D. | Все достаточные (sufficient) модули выполнился успешно | | *-50* |
| | **Общий отзыв к вопросу:** | | |
| | **Для любого правильного ответа:** | Ваш ответ верный. | |
| | **Для любого неправильного ответа:** | Ваш ответ неправильный. | |
| | **Для любого частично правильного ответа:** | Ваш ответ частично правильный. | |
| | **Подсказка 1:** | | |
| | **Показать количество правильных ответов (Подсказка 1):** | Нет | |
| | **Удалить некорректные ответы (Подсказка 1):** | Нет | |
| | **Теги:** | | |
| *Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)* | | | |

## Контроль целостности

| | | | |
|---|---|---|---|
| | Выберите элементы, соответствующие задачам контроля целостности | | *MA* |
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Показать количество правильных ответов после окончания:** | Да |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| # | **Ответы** | **Отзыв** | **Оценка** |

| | | | |
|---|---|---|---|
| Выберите элементы, соответствующие задачам контроля целостности | | | *MA* |
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Показать количество правильных ответов после окончания:** | Да |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| # | **Ответы** | **Отзыв** | **Оценка** |
| A. | Защита от программных закладок | | *33.3* |
| B. | Проверка подлинности данных, полученных через открытый канал | | *33.3* |
| C. | Проверка подлинности данных, хранимых в ненадежном хранилище | | *33.3* |
| D. | Аутентификация пользователя | | *-100* |
| | **Общий отзыв к вопросу:** | | |
| | **Для любого правильного ответа:** | Ваш ответ верный. | |
| | **Для любого неправильного ответа:** | Ваш ответ неправильный. | |
| | **Для любого частично правильного ответа:** | Ваш ответ частично правильный. | |
| | **Подсказка 1:** | | |
| | **Показать количество правильных ответов (Подсказка 1):** | Нет | |
| | **Удалить некорректные ответы (Подсказка 1):** | Нет | |
| | **Теги:** | | |
| *Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)* | | | |

## Контроль целостности

| | | | |
|---|---|---|---|
| Для проверки подлинности данных, полученных через открытый канал или хранимых в ненадежном хранилище, может быть использован алгоритм | | | *MC* |
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| # | **Ответы** | **Отзыв** | **Оценка** |
| A. | HMAC – hash-based message authentication code | | *100* |
| B. | HOTP – HMAC-Based One-Time Password Algorithm | | *0* |
| C. | TOTP – Time-based One-Time Password Algorithm | | *0* |
| | **Общий отзыв к вопросу:** | | |
| | **Для любого правильного ответа:** | Ваш ответ верный. | |
| | **Для любого неправильного ответа:** | Ваш ответ неправильный. | |
| | **Подсказка 1:** | | |
| | **Показать количество правильных ответов (Подсказка 1):** | Нет | |
| | **Удалить некорректные ответы (Подсказка 1):** | Нет | |
| | **Теги:** | | |
| *Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)* | | | |

## Методы защиты в ОС

| | | | |
|---|---|---|---|
| | К техническим методы защиты относится | | *MA* |
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Показать количество правильных ответов после окончания:** | Да |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| # | **Ответы** | **Отзыв** | **Оценка** |
| A. | Разграничение доступа | | *25* |
| B. | Криптографическая защита | | *25* |
| C. | Контроль целостности информации | | *25* |
| D. | Аудит безопасности | | *25* |
| E. | Инструктаж пользователей и контроль соблюдения инструкций | | *-100* |
| | **Общий отзыв к вопросу:** | | |
| | **Для любого правильного ответа:** | Ваш ответ верный. | |
| | **Для любого неправильного ответа:** | Ваш ответ неправильный. | |
| | **Для любого частично правильного ответа:** | Ваш ответ частично правильный. | |
| | **Подсказка 1:** | | |
| | **Показать количество правильных ответов (Подсказка 1):** | Нет | |
| | **Удалить некорректные ответы (Подсказка 1):** | Нет | |
| | **Теги:** | | |
| *Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)* | | | |

## Управление доступом

| | | | |
|---|---|---|---|
| | Отметьте правильные утверждения относительно модели разграничения доступа типа изолированная программная среда | | *MA* |
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Показать количество правильных ответов после окончания:** | Да |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| # | **Ответы** | **Отзыв** | **Оценка** |

| | | |
|---|---|---|
| | Отметьте правильные утверждения относительно модели разграничения доступа типа изолированная программная среда | *MA* |
| | **Балл по умолчанию:** | 1 |
| | **Случайный порядок ответов** | Да |
| | **Нумеровать варианты ответов?** | 0 |
| | **Показать количество правильных ответов после окончания:** | Да |
| | **Штраф за каждую неправильную попытку:** | 33.3 |
| | **ID-номер:** | |

| # | Ответы | Отзыв | Оценка |
|---|---|---|---|
| A. | Возможность доступа к объекту однозначно определяется сочетанием тройки элементов субъект-объект-право | | *-50* |
| B. | Владелец объекта доступа может произвольно ограничить доступ к нему других субъектов доступа | | *33.3* |
| C. | Возможность доступа к объекту доступа однозначно определяется сочетанием четверки элементов субъект-объект-право-процесс | | *33.3* |
| D. | Для каждого субъекта доступа определен список процессов, которые данный субъект может создавать | | *33.3* |
| E. | Возможность доступа к объекту доступа однозначно определяется сочетанием четверки элементов субъект-объект-право-процесс и зависит от последовательности предшествующих действий | | *-50* |
| | **Общий отзыв к вопросу:** | | |
| | **Для любого правильного ответа:** | Ваш ответ верный. | |
| | **Для любого неправильного ответа:** | Ваш ответ неправильный. | |
| | **Для любого частично правильного ответа:** | Ваш ответ частично правильный. | |
| | **Подсказка 1:** | | |
| | **Показать количество правильных ответов (Подсказка 1):** | Нет | |
| | **Удалить некорректные ответы (Подсказка 1):** | Нет | |
| | **Теги:** | | |
| *Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)* | | | |

2) открытые задания (мини-кейсы, средний уровень сложности):

| | |
|---|---|
| Встроенный межсетевой экран Linux, архитектура, основные принципы работы и основные утилиты управления межсетевым экраном Linux из командной строки | *ES* |

| | | | |
|---|---|---|---|
| | | **Балл по умолчанию:** | 3 |
| | | **Формат ответа:** | HTML-редактор |
| | | **Требовать текст:** | Да |
| | | **Размер поля:** | 40 |
| | | **Разрешить вложения:** | 0 |
| | | **Требуемое число вложений:** | 0 |
| | | **Разрешенные типы файлов:** | |
| | | **ID-номер:** | |
| | **Шаблон ответа** | **Информация для оценивающих** | |
| | | Межсетевой экран (netfilter) встроен в ядро Linux. Основой структурой межсетевого экрана являются таблицы, содержащие правила фильтрации. В ядре определены следующие таблицы:<br>• ebtables - содержит правила фильтрации на основе канальных адресов<br>• arptables - содержит правила фильтрации для ARP пакетов<br>• iptables – фильтр для входящих и исходящих пакетов протокола IPv4<br>• ip6tables – фильтр для входящих и исходящих пакетов протокола IPv6<br>Каждая таблица содержит одну или более цепочек правил. Цепочка – это упорядоченная последовательность правил, результат фильтрации зависит от порядка правила в цепочке. К сетевому пакету последовательно применяются правила цепочки, пока пакет не будет одобрен или отброшен. Если все правила цепочки проверены, а решение о пакете еще не принято, то применяется действие по умолчанию, которое заранее определено для каждой цепочки (политика цепочки, например, все принимать или все отбрасывать).<br>Для управления правилами в цепочках таблиц определены соответствующие утилиты. Например, утилита ebtables позволяет настраивать цепочки таблицы ebtables, утилита iptables позволяет настраивать цепочки таблицы iptables и т.д. Например запрет всех входящих соединений может быть установлен следующим образом:<br>iptables -P INPUT DROP - устанавливает политику цепочки INPUT, которая отбрасывает все входящие пакеты, если они не будут явно одобрены правилами цепочки<br>iptables -A INPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT - правило цепочки INPUT, которое ободряет все пакеты, для которых установлено соединение (т.е. они являются ответами на наши исходящие пакеты)<br>Обучающийся описал архитектуру, перечислил основные таблицы, объяснил их назначение, описал основные утилиты управления межсетевым экраном - 3 балла<br>Обучающийся описал архитектуру, перечислил основные таблицы, объяснил их назначение, описал основные утилиты управления межсетевым экраном. Ответ содержит незначительные неточности - 2 балла<br>Обучающийся не полно описал архитектуру, не перечислил основные таблицы или не объяснил их назначение, не упомянул основные утилиты управления межсетевым экраном. Ответ не содержит грубых ошибок и неточностей - 1 балл<br>Обучающийся не полно описал архитектуру, не перечислил основные таблицы или не объяснил их назначение, не упомянул основные утилиты управления межсетевым экраном. Ответ содержит грубые ошибки или неточности - 0 баллов | |
| | **Общий отзыв к вопросу:** | | |
| | **Теги:** | | |
| *Допускает в ответе загрузить файл и/или ввести текст. Ответ должен быть оценен преподавателем вручную.* | | | |

## Управление доступом

| | | | |
|---|---|---|---|
| Определения объекта, субъекта, метода и права доступа. Типовые модели управления доступом. | | | *ES* |
| | | **Балл по умолчанию:** | 3 |
| | | **Формат ответа:** | HTML-редактор |
| | | **Требовать текст:** | Да |
| | | **Размер поля:** | 40 |
| | | **Разрешить вложения:** | 0 |
| | | **Требуемое число вложений:** | 0 |
| | | **Разрешенные типы файлов:** | |
| | | **ID-номер:** | |
| | **Шаблон ответа** | **Информация для оценивающих** | |
| | | Объект доступа – любой объект в ОС, доступ к которому регламентируется правилами разграничения доступа<br>Субъект доступа – любая сущность в ОС, действия которой по доступу к объектам доступа регламентируются правилами разграничения доступа<br>Метод доступа – любая операция, определенная для действий над объектом доступа<br>Право доступа – возможность субъекта доступа выполнять доступ к объекту доступа по некоторому методу доступа<br>Типовые модели управления доступом:<br>• Дискреционное (избирательное) управление доступом - возможность доступа к объекту однозначно определяется сочетанием тройки элементов субъект-объект-право<br>• Изолированная программная среда - возможность доступа к объекту доступа однозначно определяется сочетанием четверки элементов субъект-объект-право-процесс (процесс представляет программу, используемую для реализации доступа)<br>• Мандатное управление доступом - возможность доступа к объекту доступа однозначно определяется сочетанием четверки элементов субъект-объект-право-процесс и зависит от последовательности предшествующих действий<br>Обучающийся привел определения объекта, субъекта, метода и права доступа, описал модели разграничения - 3 балла<br>Обучающийся привел определения объекта, субъекта, метода и права доступа, описал модели разграничения. Ответ содержит незначительные неточности - 2 балла.<br>Обучающийся привел только некоторые определения, и описал только некоторые модели разграничения доступа. Ответ не содержит грубых ошибок и неточностей - 1 балл<br>Обучающийся привел только некоторые определения, и описал только некоторые модели разграничения доступа. Ответ содержит грубые ошибки или неточности - 0 баллов | |
| | **Общий отзыв к вопросу:** | | |
| | **Теги:** | | |
| *Допускает в ответе загрузить файл и/или ввести текст. Ответ должен быть оценен преподавателем вручную.* | | | |

**ОПК-12 Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения**

1) закрытые задания (тестовые, средний уровень сложности):

## Управление доступом

| | | | |
|---|---|---|---|
| | Отметьте правильные утверждения относительно мандатной модели разграничения доступа | | *MA* |
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Показать количество правильных ответов после окончания:** | Да |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| **#** | **Ответы** | **Отзыв** | **Оценка** |
| A. | Возможность доступа к объекту однозначно определяется сочетанием тройки элементов субъект-объект-право | | *-33.3* |
| B. | Владелец объекта доступа может произвольно ограничить доступ к нему других субъектов доступа | | *50* |
| C. | Возможность доступа к объекту доступа однозначно определяется сочетанием четверки элементов субъект-объект-право-процесс | | *-33.3* |
| D. | Для каждого субъекта доступа определен список процессов, которые данный субъект может создавать | | *-33.3* |
| E. | Возможность доступа к объекту доступа однозначно определяется сочетанием четверки элементов субъект-объект-право-процесс и зависит от последовательности предшествующих действий | | *50* |
| | **Общий отзыв к вопросу:** | | |
| | **Для любого правильного ответа:** | Ваш ответ верный. | |
| | **Для любого неправильного ответа:** | Ваш ответ неправильный. | |
| | **Для любого частично правильного ответа:** | Ваш ответ частично правильный. | |
| | **Подсказка 1:** | | |
| | **Показать количество правильных ответов (Подсказка 1):** | Нет | |
| | **Удалить некорректные ответы (Подсказка 1):** | Нет | |
| | **Теги:** | | |
| *Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)* | | | |

## Уровень доверия

| | | | |
|---|---|---|---|
| | Уровень доверия к операционной системе оценивается по результатам проверки выполнения требований доверия, включая | | *MA* |
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Показать количество правильных ответов после окончания:** | Да |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| **#** | **Ответы** | **Отзыв** | **Оценка** |

| | | | |
|---|---|---|---|
| | Уровень доверия к операционной системе оценивается по результатам проверки выполнения требований доверия, включая | | *MA* |
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Показать количество правильных ответов после окончания:** | Да |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| **#** | **Ответы** | **Отзыв** | **Оценка** |
| A. | Анализ принятых мер защиты | | *20* |
| B. | Проверку, что указанные меры защиты действительно применяются | | *20* |
| C. | Верификацию доказательств достаточности принятых мер защиты | | *20* |
| D. | Независимое функциональное тестирование системы защиты | | *20* |
| E. | Тестирование проникновения | | *20* |
| F. | Тестирование производительности | | *-100* |
| | **Общий отзыв к вопросу:** | | |
| | **Для любого правильного ответа:** | Ваш ответ верный. | |
| | **Для любого неправильного ответа:** | Ваш ответ неправильный. | |
| | **Для любого частично правильного ответа:** | Ваш ответ частично правильный. | |
| | **Подсказка 1:** | | |
| | **Показать количество правильных ответов (Подсказка 1):** | Нет | |
| | **Удалить некорректные ответы (Подсказка 1):** | Нет | |
| | **Теги:** | | |
| *Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)* | | | |

## Уровень доверия

| | | | |
|---|---|---|---|
| | Оценочный уровень доверия 1 обеспечивает | | *MC* |
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| **#** | **Ответы** | **Отзыв** | **Оценка** |

| | | | |
|---|---|---|---|
| | Оценочный уровень доверия 1 обеспечивает | | *MC* |
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| **#** | **Ответы** | **Отзыв** | **Оценка** |
| A. | Минимальный уровень доверия, который подтверждает только наличие в составе ОС некоторых средств защиты | | *100* |
| B. | Уровень доверия от невысокого до умеренного, достигаемый при отсутствии доступа к полной документации по разработке ОС, основанный на анализе структуры ОС с использованием полученной от разработчика ОС дополнительной информации. | | *0* |
| C. | Умеренный уровень доверия, основанный на всестороннем методическом исследовании функций безопасности и процесса разработки ОС | | *0* |
| D. | Уровень доверия от умеренного до высокого в отношении уже существующей ОС общего назначения, основанный на всестороннем методическом тестировании и проверке реализации функций безопасности ОС, на уверенности в правильном использовании типовых методов при проектирования ОС. | | *0* |
| E. | Высокий уровень доверия для разрабатываемой ОС, основанный на использовании полуформальных методов при проектировании и тестировании ОС. | | *0* |
| F. | Уверенность в безопасности ОС при работе в условиях высокого риска, где ценность защищаемых данных оправдывает дополнительные затраты, основанную на использовании полуформальных методов при верификации и тестировании ОС | | *0* |
| G. | Уверенность в безопасности ОС при работе в условиях чрезвычайно высокого риска, где высокая ценность защищаемых данных оправдывает повышенные затраты, основанную на использовании формальных методов при верификации и тестировании ОС | | *0* |
| | **Общий отзыв к вопросу:** | | |
| | **Для любого правильного ответа:** | Ваш ответ верный. | |
| | **Для любого неправильного ответа:** | Ваш ответ неправильный. | |
| | **Подсказка 1:** | | |
| | **Показать количество правильных ответов (Подсказка 1):** | Нет | |
| | **Удалить некорректные ответы (Подсказка 1):** | Нет | |
| | **Теги:** | | |
| *Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)* | | | |

## Защита в UNIX-подобных системах

| | | | |
|---|---|---|---|
| | В UNIX-подлобных системах Sticky-bit (атрибут T) установленный для каталога имеет следующее действие | | *MC* |
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| **#** | **Ответы** | **Отзыв** | **Оценка** |

| | | | |
|---|---|---|---|
| | В UNIX-подлобных системах Sticky-bit (атрибут T) установленный для каталога имеет следующее действие | | *MC* |
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| # | **Ответы** | **Отзыв** | **Оценка** |
| A. | Не оказывает никакого действия для каталогов в современных реализациях операционных систем | | *0* |
| B. | Для новых файлов группой-владельцем становится группа-владелец каталога | | *0* |
| C. | Пользователь может удалять из каталога только файлы, которыми он владеет | | *100* |
| D. | Файлы из каталога нельзя объявить исполняемыми | | *0* |
| | **Общий отзыв к вопросу:** | | |
| | **Для любого правильного ответа:** | Ваш ответ верный. | |
| | **Для любого неправильного ответа:** | Ваш ответ неправильный. | |
| | **Подсказка 1:** | | |
| | **Показать количество правильных ответов (Подсказка 1):** | Нет | |
| | **Удалить некорректные ответы (Подсказка 1):** | Нет | |
| | **Теги:** | | |
| *Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)* | | | |

## Защита в UNIX-подобных системах

| | | | |
|---|---|---|---|
| | В UNIX-подобных системах при вычислении хэша пароля используется дополнительный открытый ключ (соль), применение которого обеспечивает | | *MC* |
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| # | **Ответы** | **Отзыв** | **Оценка** |
| A. | Генерацию разного хэша для одинаковых паролей | | *100* |
| B. | Увеличение числа вариантов пароля | | *0* |
| | **Общий отзыв к вопросу:** | | |
| | **Для любого правильного ответа:** | Ваш ответ верный. | |
| | **Для любого неправильного ответа:** | Ваш ответ неправильный. | |
| | **Подсказка 1:** | | |
| | **Показать количество правильных ответов (Подсказка 1):** | Нет | |
| | **Удалить некорректные ответы (Подсказка 1):** | Нет | |
| | **Теги:** | | |
| *Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)* | | | |

2) открытые задания (мини-кейсы, средний уровень сложности):

| |
|---|
| Основы разграничения доступа в MS Windows |

| | Шаблон ответа | Информация для оценивающих |
|---|---|---|
| | | В Windows используется дискреционная модель разграничения доступа (DAC) на основе списков контроля доступа (ACL). Список контроля доступа является частью дескриптора защиты, который сопоставляется с каждым объектом доступа. Для гарантированной уникальности идентификаторов в Windows вместо числовых идентификаторов пользователей и групп используются глобально-уникальные идентификаторы безопасности (SID), которые могут иметь разную длину, но не менее 48 бит.<br>В Windows помимо традиционных видов доступа (чтение, запись, исполнение), определено множество дополнительных видов доступа, например, чтение и запись атрибутов файла, дополнение файла, чтение и изменение разрешений, удаление, смена владельца и др.<br>Для экономии места в файловой системе и упрощения настройки доступа к большому числу файлов в каталогах, в Windows также определен механизм наследования разрешений. При наследовании разрешений, вместо собственного списка контроля доступа объекта будет использоваться список его родительского объекта.<br>Управление списками контроля доступа и разрешениями может выполняться через графический интерфейс в проводнике Windows или из консоли с использованием команды ICACLS.<br>Обучающийся точно описал модель разграничения доступа в MS Windows, перечислил основные виды доступа, принятые в Windows, описал механизм наследования разрешений и инструменты управления списками контроля доступа - 3 балла<br>Обучающийся точно описал модель разграничения доступа в MS Windows, перечислил основные виды доступа, принятые в Windows, описал механизм наследования разрешений и инструменты управления списками контроля доступа. Ответ содержит незначительные неточности - 2 балла<br>Обучающийся не точно описал модель разграничения доступа в MS Windows, не перечислил основные виды доступа, принятые в Windows, не описал механизм наследования разрешений и инструменты управления списками контроля доступа. Ответ не содержит грубых ошибок и неточностей - 1 балл<br>Обучающийся не точно описал модель разграничения доступа в MS Windows, не перечислил основные виды доступа, принятые в Windows, не описал механизм наследования разрешений и инструменты управления списками контроля доступа. Ответ содержит грубые ошибки или неточности - 0 баллов |

**ОПК-13 Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности;**

1) закрытые задания (тестовые, средний уровень сложности):

## Уровень доверия

| | | | |
|---|---|---|---|
| Оценочный уровень доверия 4 (Наиболее высокий уровень доверия, достижимый при оценке существующих ОС общего назначения, так как боле высокий уровень доверия требует вмешательства в разработку ОС) обеспечивает | | | *MC* |
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| # | **Ответы** | **Отзыв** | **Оценка** |

| | | | |
|---|---|---|---|
| | Оценочный уровень доверия 4 (Наиболее высокий уровень доверия, достижимый при оценке существующих ОС общего назначения, так как боле высокий уровень доверия требует вмешательства в разработку ОС) обеспечивает | | *MC* |
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| **#** | **Ответы** | **Отзыв** | **Оценка** |
| A. | Некоторую уверенность в том, что подсистема безопасности ОС реализована в соответствии с документацией (в процессе реализации не были внесены неучтенные изменения) | | *0* |
| B. | Уверенность в том, что подсистема безопасности ОС реализована в соответствии с документацией | | *100* |
| C. | Высокую уверенность в том, что подсистема безопасности ОС реализована в соответствии с предъявляемыми требованиями | | *0* |
| | **Общий отзыв к вопросу:** | | |
| | **Для любого правильного ответа:** | Ваш ответ верный. | |
| | **Для любого неправильного ответа:** | Ваш ответ неправильный. | |
| | **Подсказка 1:** | | |
| | **Показать количество правильных ответов (Подсказка 1):** | Нет | |
| | **Удалить некорректные ответы (Подсказка 1):** | Нет | |
| | **Теги:** | | |
| *Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)* | | | |

## Уровень доверия

| | | | |
|---|---|---|---|
| Уровень доверия к операционной системе оценивается по результатам проверки выполнения требований доверия, включая | | | *MA* |
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Показать количество правильных ответов после окончания:** | Да |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| **#** | **Ответы** | **Отзыв** | **Оценка** |
| A. | Анализ принятых мер защиты | | *20* |
| B. | Проверку, что указанные меры защиты действительно применяются | | *20* |
| C. | Верификацию доказательств достаточности принятых мер защиты | | *20* |
| D. | Независимое функциональное тестирование системы защиты | | *20* |
| E. | Тестирование проникновения | | *20* |
| F. | Тестирование производительности | | *-100* |
| | **Общий отзыв к вопросу:** | | |
| | **Для любого правильного ответа:** | Ваш ответ верный. | |
| | **Для любого неправильного ответа:** | Ваш ответ неправильный. | |
| | **Для любого частично правильного ответа:** | Ваш ответ частично правильный. | |
| | **Подсказка 1:** | | |
| | **Показать количество правильных ответов (Подсказка 1):** | Нет | |
| | **Удалить некорректные ответы (Подсказка 1):** | Нет | |
| | **Теги:** | | |
| *Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)* | | | |

## Политика безопасности

| | | |
|---|---|---|
| | Политика безопасности это | *MC* |

| | | | |
|---|---|---|---|
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| # | **Ответы** | **Отзыв** | **Оценка** |
| A. | Набор правил, регламентирующих порядок хранения и обработки информации | | *100* |
| B. | Перечень требуемых программ технической защиты информации и их настроек | | *0* |
| C. | Список ограничений на действия пользователей | | *0* |
| | **Общий отзыв к вопросу:** | | |
| | **Для любого правильного ответа:** | Ваш ответ верный. | |
| | **Для любого неправильного ответа:** | Ваш ответ неправильный. | |
| | **Подсказка 1:** | | |
| | **Показать количество правильных ответов (Подсказка 1):** | Нет | |
| | **Удалить некорректные ответы (Подсказка 1):** | Нет | |
| | **Теги:** | | |
| *Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)* | | | |

## Сетевая безопасность в ОС

| | | | |
|---|---|---|---|
| Встроенный программный межсетевой экран в Linux и MS Windows обеспечивает | | | *MC* |
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| # | **Ответы** | **Отзыв** | **Оценка** |
| A. | Фильтрацию сетевого трафика в соответствии с заданными правилами для предотвращения возможности использования злоумышленником уязвимостей сетевых протоколов и программного обеспечения | | *100* |
| B. | Шифрование и контроль целостности пакетов в сетевом трафике для защиты от подмены данных | | *0* |
| | **Общий отзыв к вопросу:** | | |
| | **Для любого правильного ответа:** | Ваш ответ верный. | |
| | **Для любого неправильного ответа:** | Ваш ответ неправильный. | |
| | **Подсказка 1:** | | |
| | **Показать количество правильных ответов (Подсказка 1):** | Нет | |
| | **Удалить некорректные ответы (Подсказка 1):** | Нет | |
| | **Теги:** | | |
| *Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)* | | | |

## Управление доступом

| | | | |
|---|---|---|---|
| Отметьте правильные утверждения относительно дискреционной модели разграничения доступа | | | *MA* |
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Показать количество правильных ответов после окончания:** | Да |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| # | **Ответы** | **Отзыв** | **Оценка** |

| | | | |
|---|---|---|---|
| | Отметьте правильные утверждения относительно дискреционной модели разграничения доступа | | *MA* |
| | | **Балл по умолчанию:** | 1 |
| | | **Случайный порядок ответов** | Да |
| | | **Нумеровать варианты ответов?** | 0 |
| | | **Показать количество правильных ответов после окончания:** | Да |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| **#** | **Ответы** | **Отзыв** | **Оценка** |
| A. | Возможность доступа к объекту однозначно определяется сочетанием тройки элементов субъект-объект-право | | *50* |
| B. | Владелец объекта доступа может произвольно ограничить доступ к нему других субъектов доступа | | *50* |
| C. | Возможность доступа к объекту доступа однозначно определяется сочетанием четверки элементов субъект-объект-право-процесс | | *-33.3* |
| D. | Для каждого субъекта доступа определен список процессов, которые данный субъект может создавать | | *-33.3* |
| E. | Возможность доступа к объекту доступа однозначно определяется сочетанием четверки элементов субъект-объект-право-процесс и зависит от последовательности предшествующих действий | | *-33.3* |
| | **Общий отзыв к вопросу:** | | |
| | **Для любого правильного ответа:** | Ваш ответ верный. | |
| | **Для любого неправильного ответа:** | Ваш ответ неправильный. | |
| | **Для любого частично правильного ответа:** | Ваш ответ частично правильный. | |
| | **Подсказка 1:** | | |
| | **Показать количество правильных ответов (Подсказка 1):** | Нет | |
| | **Удалить некорректные ответы (Подсказка 1):** | Нет | |
| | **Теги:** | | |
| *Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)* | | | |

2) открытые задания (тестовые, средний уровень сложности):

## Защита в Linux

| | | | |
|---|---|---|---|
| | Процесс запущен пользователем UID=1000 с использованием sudo и выполняется от имени суперпользователя. Чему равен эффективный идентификатор процесса (EUID)? | | *NUM* |
| | | **Балл по умолчанию:** | 2 |
| | | **Штраф за каждую неправильную попытку:** | 33.3 |
| | | **ID-номер:** | |
| **#** | **Ответы** | **Отзыв** | **Оценка** |
| A. | 0 | | *100* |
| | **Общий отзыв к вопросу:** | | |
| | **Подсказка 1:** | | |
| | **Показать количество правильных ответов (Подсказка 1):** | Нет | |
| | **Удалить некорректные ответы (Подсказка 1):** | Нет | |
| | **Теги:** | | |
| *Импортирование этого типа вопроса не поддерживается.* | | | |

**Задания раздела 20.3 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных результатов освоения данной дисциплины (знаний, умений, навыков).**