Министерство науки и высшего образования РФ
ФГБОУ ВО «Ульяновский государственный университет»
Факультет математики, информационных и авиационных технологий

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ВЫПОЛНЕНИЯ ЛАБОРАТОРНЫХ РАБОТ И САМОСТОЯТЕЛЬНОЙ РАБОТЫ

СТУДЕНТОВ ПО ДИСЦИПЛИНЕ

«Защита в операционных системах»

для студентов специалитета по специальности
10.05.01 Компьютерная безопасность,

Ульяновск, 2021

Методические указания для выполнения лабораторных работ и самостоятельной работы студентов по дисциплине «Защита в операционных системах» для студентов специальности 10.05.01 «Компьютерная безопасность» / составитель: Клочков А.Е. - Ульяновск: УлГУ, 2021.

Настоящие методические указания предназначены для студентов специалитета по специальности 10.05.01 «Компьютерная безопасность», изучающих дисциплину «Защита в операционных системах». В работе приведены рекомендуемая литература по дисциплине, основные темы курса и вопросы в рамках каждой темы, указания по выполнению лабораторных работ.

Студентам следует использовать данные методические указания при выполнении лабораторных работ и при подготовке к экзамену по данной дисциплине.

Рекомендованы к введению в образовательный процесс Ученым советом факультета математики, информационных и авиационных технологий УлГУ (протокол № 4/21 от 18 мая 2021 г.)

СПИСОК РЕКОМЕНДОВАННОЙ ЛИТЕРАТУРЫ

1. Гостев, И. М. Операционные системы : учебник и практикум для вузов / И. М. Гостев. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 164 с. — (Высшее образование). — ISBN 978-5-534-04520-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/470010.
2. Руссинович М. Соломон Д. Ионеску А. Внутреннее устройство Windows. Седьмое издание. – Санкт-Петербург, Издательство Питер 2019г. – 944 с. – ISBN 978-5-4461-0663-9.
3. Таненбаум Э. Бос. Х. Современные операционные системы. Санкт-Петербург, Издательство ПИТЕР, 2019 г. – 1120с ISBN: 978-5-4461-1155-8.
4. Щеглов А.Ю. Математические модели и методы формального проектирования систем защиты информационных систем : учебное пособие / Щеглов А.Ю., Щеглов К.А.. — Санкт-Петербург : Университет ИТМО, 2015. — 93 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/67260.html — Режим доступа: для авторизир. пользователей
5. Программно-аппаратные средства защиты информационных систем : учебное пособие / Ю.Ю. Громов [и др.].. — Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2017. — 193 с. — ISBN 978-5-8265-1737-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/85968.html — Режим доступа: для авторизир. пользователей
6. Пушкарев В.П. Защита информационных процессов в компьютерных системах : учебное пособие / Пушкарев В.П., Пушкарев В.В.. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2012. — 131 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/13929.html — Режим доступа: для авторизир. пользователей.
7. Кулябов Д.С. Основы администрирования операционных систем: лабораторные работы: учебное пособие / Кулябов Д.С., Королькова А.В. — Москва: Российский университет дружбы народов, 2018. — 123 с. — ISBN 978-5-209-09058-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: https://www.iprbookshop.ru/104234.html — Режим доступа: для авторизир. пользователей
8. Филиппов М.В. Операционные системы : учебно-методическое пособие / Филиппов М.В., Завьялов Д.В.. — Волгоград : Волгоградский институт бизнеса, 2014. — 163 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/56020.html — Режим доступа: для авторизир. пользователей
9. Глотина И.М. Средства безопасности операционной системы Windows Server 2008 : учебно-методическое пособие / Глотина И.М.. — Саратов : Вузовское образование, 2018. — 141 с. — ISBN 978-5-4487-0136-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/72538.html — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/72538
10. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. - М.: Книжный мир, 2009. - 352 с. - ISBN 978-5-8041-0378-2.
11. http://www.securitylab.ru – российский портал по компьютерной безопасности.
12. http://www.pgpru.com – русскоязычный сайт, посвященный криптографическому стандарту PGP.

13. http://www.docload.spb.ru/Basesdoc/45/45674/index.htm – основные термины и определения в области технической защиты информации (согласно Приказу Федерального агентства по техническому регулированию и метрологии от 6 апреля 2005 г. № 77-ст)

СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Защита информации в современных информационных системах.

Тема 1. Основные понятия и положения защиты информации в информационно вычислительных системах. Предмет защиты информации. Понятия информации и информационных ресурсов. Достоверность, ценность и своевременность информации. Предмет защиты информации. Объект защиты информации. Понятия информационной системы. Понятие информационной безопасности. Понятие политики информационной безопасности. Понятие системы защиты информации. Основные положения безопасности информационных систем. Трехэтапная разработка мер по обеспечению безопасности информационных систем. Стадия выработки требований. Стадия определения способов защиты. Стадия определения функций, процедур и средств безопасности, реализуемых в виде некоторых механизмов защиты. Основные принципы обеспечения информационной безопасности в автоматизированной системе (АС). Положения по защите АС. Принципы, позволяющие реализовать положения по защите АС. Принцип системности. Принцип комплексности. Принцип непрерывной защиты. Разумная достаточность. Гибкость системы защиты. Открытость алгоритмов и механизмов защиты. Принцип простоты применения средств зашиты.

Тема 2. Угрозы безопасности информации в информационно-вычислительных системах. Понятие угрозы. Понятие атаки. Понятие злоумышленника. Источники угроз. Окно опасности. Критерии классификации угроз. Базовые признаки угроз информационной безопасности. Классификация угроз по природе возникновения. Классификация угроз по степени преднамеренности проявления. Классификация угроз по непосредственному источнику угроз. Классификация угроз по положению источника угроз. Классификация угроз по степени зависимости от активности АС. Классификация угроз по степени воздействия на АС. Классификация угроз по этапам доступа пользователей или программ к ресурсам АС. Классификация угроз по способу доступа к ресурсам АС. Классификация угроз по текущему месту расположения информации, хранимой и обрабатываемой в АС. Доступность информации. Угроза доступности. Целостность информации. Угроза нарушения целостности. Конфиденциальность информации. Угроза нарушения конфиденциальности. Угроза раскрытия параметров АС. Методы обеспечения информационной безопасности. Структуризация методов обеспечения информационной безопасности. Уровни доступа к защищаемой информации. Основные направления и методы реализации угроз информационной безопасности. Классификация злоумышленников.

Тема 3. Программно-технический уровень обеспечения информационной безопасности и его организация. Подходы к обеспечению компьютерной безопасности. Сервис безопасности. Основные и вспомогательные сервисы безопасности. Понятие полного набора. Виды сервисов безопасности. Понятия идентификации, аутентификации и авторизации пользователей. Виды аутентификации. Проблема надежной аутентификации и пути ее решения. Средства и методы хранения эталонных копий аутентификационной информации. Протоколы передачи аутентификационной информации по каналам вычислительной сети. Криптографическое обеспечение аутентификации пользователей. Парольная аутентификация. Виды парольной аутентификации. Преимущества и недостатки парольной аутентификации. Повышение надежности парольной аутентификации. Средства и методы защиты от компрометации и подбора паролей. Биометрическая аутентификация.

Общая схема биометрической аутентификации. Преимущества и недостатки биометрической аутентификации. Достоинства и недостатки различных схем биометрической аутентификации. Требования к защите компьютерной информации. Общие положения. Характеристики подходов к защите компьютерной информации. Классификация требований к системам защиты. Формализованные требования к набору и параметрам механизмов защиты. Необходимые требования. Дополнительные требования. Формализованные требования к защите информации от несанкционированного доступа. Общие подходы к построению систем защиты компьютерной информации. Нормативные документы Гостехкомиссии РФ, регламентирующие защиту информации от несанкционированного доступа. Формализованные требования к защите компьютерной информации АС. Основные подсистемы и группы механизмов защиты АС. Требования к защите конфиденциальной информации. Требования к защите секретной информации. Различия требований и основополагающих механизмов защиты от несанкционированного доступа.

Раздел 2. Подсистема безопасности в ОС семейства Windows.

Тема 4. Анализ подсистемы безопасности в ОС семейства Windows.

Основные механизмы защиты в ОС семейства Windows. Принципиальные недостатки защитных механизмов ОС семейства Windows.

Тема 5. Идентификация, аутентификация и авторизация в ОС семейства Windows. Возможности подсистемы безопасности в ОС семейства Windows. Модель безопасности для подсистемы безопасности в ОС семейства Windows. Механизм идентификации пользователей. Идентификатор защиты SID пользователей. Идентификаторы полномочий. Возможные значения идентификатора полномочий. Относительный идентификатор. Маркер доступа и привилегии пользователя. Просмотр привилегий пользователя. Команда whoami и ее параметры. Ограничивающие маркеры доступа. Команда runas и ее параметры. API функции для создания маркеров доступа. Защита объектов системы. Дескриптор безопасности SD. Атрибуты дескриптора безопасности. Парольная аутентификация в ОС семейства Windows. Механизм аутентификации. Средства управления параметрами аутентификации. Учетные записи пользователей. Локальные учетные записи пользователей. База данных SAM. Возможности получения доступа к SAM. Организация защиты SAM от несанкционированного доступа. Авторизация в ОС семейства Windows. Недостатки в организации разграничения доступа к файлам в ОС семейства Windows. Механизм авторизации в ОС семейства Windows. Маркеры доступа. Дескриптор безопасности. Формат дескрипторов безопасности. Список контроля доступа ACL. Системный (SACL) и пользовательский (DACL) списки управления доступом. Структура списков управления доступом. Возможность управления правами доступа с помощью API. Пример проверки прав доступа пользователя к объекту. Изменение прав доступа к объекту. Смена владельца объекта. Команда cacls и ее параметры.

Тема 6. Аудит в ОС семейства Windows. Подсистема аудита в ОС семейства Windows. Категории аудита. Оснастка gpedit.msc. Настройка списка SACL. API функции для работы с SACL. Просмотр событий аудита. Утилита Event Viewer. Оснастка eventvwr.msc. Журналы аудита. Типы регистрируемых событий в журналах аудита. Настройка журналов аудита. Типы записей в журналах событий. Определение набора подлежащих аудиту событий.

Тема 7. Возможности шифрования файлов в ОС семейства Windows. Шифрующая файловая система EFS. Возможности шифрующей файловой системы EFS. Принципы работы EFS. Используемые в EFS алгоритмы шифрования. Случайный ключ для шифрования файла FEK. Шифрование ключа FEK. Команда cipher и ее параметры. Понятие агента восстановления. Добавление агентов восстановления. Сертификаты агентов восстановления. Поле восстановления данных DRF. API функции для работы с EFS. Система шифрования дисков BitLocker. Основные возможности BitLocker. Поддерживаемые алгоритмы шифрования. Принцип работы. Механизмы проверки

подлинности и расшифровки. Уязвимости BitLocker. Настройка BitLocker. Шифрование и дешифрование дисков при помощи BitLocker.

Тема 8. Прочие возможности подсистемы безопасности в ОС семейства Windows.

Интерфейс CryptoAPI. Возможности CryptoAPI. Работа с поставщиками службы шифрования CSP. Типы CSP в ОС семейства Windows. Контроль учетных записей пользователей UAC. Предпосылки к появлению UAC. Принцип работы UAC. События, приводящие к срабатыванию UAC. Настройка UAC. Недостатки UAC. Шаблоны безопасности в ОС семейства Windows. Возможности шаблонов безопасности. Настройки шаблонов безопасности.

Тема 9. Усиление подсистемы безопасности в ОС семейства Windows.

Использование систем криптографической защиты информации. Наиболее известные системы криптографической защиты информации и особенности их работы. Противодействие вирусным атакам в системе. Выбор антивируса. Организация антивирусной защиты.

Раздел 3. Подсистема безопасности в ОС семейства UNIX

Тема 10. Анализ подсистемы безопасности в ОС семейства UNIX.

Основные механизмы защиты в ОС семейства UNIX. Особенности организации файловой системы в UNIX. Принципиальные недостатки защитных механизмов ОС семейства UNIX.

Тема 11. Идентификация, аутентификация и авторизация в ОС семейства UNIX.

Особенности подсистемы безопасности в ОС семейства UNIX. Единая модель безопасности для ОС семейства UNIX. Парольная аутентификация в UNIX. Зарегистрированные пользователи системы. Учетный файл зарегистрированных пользователей /etc/passwd. Содержимое файла /etc/passwd. Подключаемые модули аутентификации PAM. Основы PAM. Настройка PAM. Механизм идентификации пользователей. Идентификаторы пользователей UID, RUID, EUID. Учетный файл зарегистрированных групп /etc/group. Идентификаторы групп пользователей GID, RGID, EGID. Суперпользователи и привилегированные группы. Возможности суперпользователей и привилегированных групп. Хранение паролей в других файлах в ОС семейства UNIX. Командные интерпретаторы в ОС семейства UNIX. Авторизация в ОС семейства UNIX. Особенности доступа к файлам в ОС семейства UNIX. Классы доступа к файлу. Список прав доступа к файлу. Различие возможных значений прав доступа для разных типов файлов. Изменение прав доступа к файлу утилитой chmod. Формат команд для утилиты chmod. Проверка прав доступа при обращении к файлам в ОС UNIX. Дополнительные права SUID, SGID, Sticky-бит. Применение дополнительных прав. Работа из-под root. Особенности работы из-под root. Выполнение операций от имени root. Команда su и утилита sudo. Файл sudoers. Редактирование файла sudoers с помощью утилиты visudo.

Тема 12. Аудит в ОС семейства UNIX.

Подсистема аудита в UNIX. Централизованная система регистрации системных сообщений Syslog. Возможности системы Syslog. Компоненты Syslog. Работа системы Syslog. Файл конфигурации Syslog syslog.conf. Селекторы Syslog. Средства и уровни Syslog. Действия с сообщениями Syslog. Утилита newsyslog. Работа утилиты newsyslog. Файл конфигурации newsyslog.conf. Тема 13. Возможности шифрования файлов в ОС семейства UNIX с использованием PGP. Шифование файлов при помощи PGP. Особенности PGP. Защищенность PGP. Ключи, генерируемые PGP и их типы. Поддержка PGP возможности цифровой подписи и сжатия данных. Установка и настройка PGP.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ И ЗАДАНИЯ К ЛАБОРАТОРНЫМ РАБОТАМ

Цель. Лабораторный практикум по дисциплине направлен на изучение студентами всех современных подходов для обеспечения информационной безопасности современных операционных систем. Охватывает клиентские операционные системе (на базе Microsoft Windows 10 и Alt Linux), а также серверные операционное системы (на базе Microsoft Server

2026R2 и Alt Linux Server). В соответствии с руководящими документами обучение происходит на сертифицированные версиях операционных систем.
Методология основывается на самостоятельном обучении студентов решению стандартных задач на основе технической документации, теоретического материала. Все работы обладают дифференцированной линейно растущей сложностью выполнению и созданы на основе стандартных практических задач современного предприятия. Поиск технической информации, а также подбор необходимого решения производиться самостоятельно студентами в открытых источниках и контролируется в ходе лабораторных занятий и процессе демонстрации полученного решения.
Результат. Полученные решения демонстрируются студентом для каждого из типа операционных систем. При необходимости демонстрируется ход выполнения работы.
Требования к оборудованию. Для выполнения работ студенты используют несколько виртуальных машин с различными версиями операционных систем. Возможно самостоятельное выполнение лабораторных работ вне лаборатории. Компьютер с жестким диском – 100 Gb, ОЗУ: 8 Gb, Windows 10 Pro, BaseAlt (Альт Рабочая станция, Альт сервер), Kali Linux, Oracle Virtual Box, Putty, PGP, Apache, nginx, Statistica, Origin. По желанию студента все виртуальные машины могут быть развернуты на выделенном сервере виртуальных машин в лаборатории.

Лабораторная работа №1. Пользователи и группы

Цель. Изучение системы администрирования пользователей и групп в операционных системах. Изучение системы защиты информации файловых систем NTFS (MS Windows) и ext4fs (BaseAlt (Альт Рабочая станция, Альт сервер)). Реализация системы разграничение прав доступа к каталогам файловой системы и файлам. Разграничение прав доступа к файловой системе по сети.
Задача. Все задачи необходимо выполнить на ОС MS Windows 10 и BaseAlt (Альт Рабочая станция, Альт сервер).

- Разработать политику именования сотрудников организации.
- Необходимо создать пользователей в ОС в соответствии с разработанной политикой:
    - Корейко Александр Иванович
    - Балаганов Шура
    - Mr. Panikovskii Mikhail Samuelivich
    - Остап Бендер
- Необходимо создать группы пользователей в ОС: Руководство, Планово-финансовый отдел, Департамент инженерных решений.
- Включить каждого пользователя в свою группу: Бендер -> Руководство, Балаганов -> Департамент инженерных решений, Panikovskii -> Планово-финансовый отдел.
- Создать каталог ООО Рога и Копыта, в нем каталоги Общие документы, Финансовые отчеты, Поставщики.
- Назначить права для данных каталогов в соответствии с матрицей доступа

	Руководство	Планово-финансовый отдел	Департамент инженерных решений	Корейко
Общие документы	Ч,З	Ч,З	Ч,З	-
Финансовые отчеты	Ч	Ч,З	-	-
Поставщики	Ч	-	Ч,З	-

- В каталоге «Поставщики» создать файл Особой важности.txt предоставить доступ только к этому файлу для чтения членам «Планово-финансового отдел»

- Предоставить общий доступ к папке Общие документы через сеть.
- Предоставить доступ к папке Общие документы для Корейко, только для чтения.
- Запретить пользователям Планово-финансового отдела хранить больше 1Мб информации в папке Общие документы.

Лабораторная работа №2. Массовая регистрация пользователей

Цель. Изучение системы администрирования пользователей при помощи стандартного API операционной системы. Изучение методов назначения прав доступа к объектам файловой системы из скриптовых языков.

Задача. Все задачи необходимо выполнить на ОС MS Windows 10 и BaseAlt (Альт Рабочая станция, Альт сервер).

В файле в формате csv создан список более 100 пользователей, содержащий ФИО сотрудников, которым необходимо предоставить доступ к компьютеру:

Васисуалий Лоханкин, v.lohankin@roga-kopita.ru

Зося Синицкая, z.sinickaya@roga-kopita.ru

В соответствии с разработанной политикой именования сотрудников создать всех пользователей при помощи скрипта.

Создать в каталоге ООО Рога и Копыта каталог Пользовательские данные

Создать каталоги для каждого пользователя и назначить пользователей владельцем своего каталога.

Запретить всем другим пользователям доступ к данному каталогу.

Разрешить группе Руководство доступ к каталогу для чтения и записи.

Лабораторная работа №3. Политика безопасности

Цель. Изучение возможности управления групповой политики операционных систем семейства Microsoft Windows.

Задание №1. Выполняется только под ОС Microsoft Windows 10 и Microsoft Windows Server.

1. Определите следующую политику паролей:
   1.1. Установите количество запоминаемых паролей равное 10.
   1.2. Установите срок действия паролей равным 10 дням.
   1.3. Установите минимальный срок действия пароля равным 5 дням.
   1.4. Потребуйте установку пароля, отвечающего требованиям сложности.
   1.5. Установите длину пароля не менее 5 символов.
   1.6. Отключите использование обратного шифрования при хранении паролей.
2. Задайте политику блокировки учетных записей:
   2.1. Определите блокировку учетной записи через 3 неудачных попытки входа в систему.
   2.2. Определите блокировку учетной записи после неудачных попыток входа на 10 мин.
   2.3. Определите время в течение, которого подсчитываются неудачные попытки входа равным 15 мин.
3. Сделайте регистрацию следующих событий:
   3.1. Вход в систему (успех).
   3.2. Доступ к объектам (успех).
   3.3. Доступ к службе каталогов (успех).
   3.4. Изменение политики (успех).
   3.5. Использование привилегий (успех).
   3.6. Отслеживание процессов (успех).
   3.7. Системные события (успех).
   3.8. События входа в систему (успех).

3.9. Управление учетными записями (успех).

Задание №2.
Осуществите три неудачные попытки входа в систему. Продемонстрируйте работу системных журналов регистрации событий входа.

Лабораторная работа №4. Ограниченное использование программ

Цель. Изучение возможности изменения уровней безопасности операционной системы путем блокирования определённых приложений.
Задача. Выполнять только для ОС Microsoft Windows 10 и Microsoft Server.

1. Задайте политику безопасности по «белому списку».
2. Добавьте к исполняемым файлам, файлы с расширением «.isp».
3. Разрешите всем пользователям проверять сертификаты.
4. Запретите по хеш-значению запуск программы «Калькулятор».
5. Запретите установку программ, загруженных из Интернета.

Лабораторная работа №5. Взлом паролей пользователей

Взлом паролей Microsoft Windows 10.

1. Установить на виртуальную машину Windows 10.
2. Создать трех пользователей с именами ФИО-Низкий, ФИО-Средний, ФИО-Высокий, где ФИО-ваша фамилия имя отчество. Например:
3. КАЕ-Низкий, КАЕ-Средний, КАЕ-Высокий.
4. Установить для каждого пользователя свой пароль.
5. Для Низкий - 6 букв и цифр латинского алфавита.
6. Для Средний - 12 букв и цифр латинского алфавита.
7. Для Высокий - 15 символов включая заглавные и прописные буквы, цифры, спец. символы.
8. Сохранить все файлы в файл Lab3\pass.txt
9. Найти bootkey ОС Windows.
10. Выгрузить базу паролей SAM.
11. Взломать пароли используя любую утилиту Kali Linux. Например john.

Лабораторная работа №6. Прозрачное шифрование файловой системы.

Цель. Изучение возможностей применения «прозрачного» шифрования данных в файловых системах.

Задача. Организация защиты исполняемого кода. Выполняется для ОС Windows Server и для BaseAlt (Альт Рабочая станция, Альт сервер). Возможно использование LUKS или LVM.

- Установить WEB сервер apache или ngnix. Создать каталог www для хранения данных сайта в каталоге ООО Рога и Копыта.
- Настроить отображение тестовой страницы index.html для данного сайта.
- Создать пользователя web-www с правами только чтения и записи данных в каталог www.
- Настроить шифрование файлов для каталога www и установить ключи шифрования для пользователя Остап Бендер и для web-www.
- Все остальные пользователи не должны иметь доступ каталогу.

- Проверить чтение файла index.html под другим пользователем.

Лабораторная работа №7. Шифрование и хеширование

Цель. Изучение методов контроля целостности и шифрования данных.
Задание №1. Выполняется для ОС Microsoft Windows 10 и BaseAlt (Альт Рабочая станция, Альт сервер).

- В каталоге ООО Рога и Копыта\Финансовые отчеты создайте 1000 файлов отчетов с именами в следующем формате: yyyymmdd-report.txt, где yyyy-год, mm-месяц в виде числа, dd – день. Создание файлов реализовать скриптом начиная с текущей даты и назад в прошлое на 1000 дней. В файл записать текущее время в формате yyyymmddhhMMss.
- Создать файл с контрольными суммами (hash) для всех файлов каталога.
- Сгенерировать ключ шифрования данных для gpg.
- Зашифровать все файлы отчетов каждый отдельно.
- Заархивировать все зашифрованные файлы и файл с хеш суммами и передать его на другую ОС (с MS Windows 10 на BaseAlt (Альт Рабочая станция, Альт сервер) и наоборот).
- Распаковать файлы и расшифровать их. Проверить все хеш суммы файлов.
- Изменить один из файлов и продемонстрировать, что хеш суммы у файлов не совпадают.

Задание №2. Выполняется для ОС Microsoft Windows 10 и BaseAlt (Альт Рабочая станция, Альт сервер).

- Установить на виртуальные машины КриптоАРМ ГОСТ. Внимание! Программа будет работать только 14 дней. Используйте копии виртуальных машин.
- Сформируйте тестовый квалифицированный сертификат электронной подписи в тестовом удостоверяющем центре КриптоПро.
- Сформируйте квалифицированную электронную подпись для архива отчетов.
- Зашифруйте архив и передайте его на другую ОС.
- Расшифруйте архив при помощи сертификата и проверьте электронную подпись документов.

- *Дополнительное задание.* Сохраните закрытый ключ и сертификат ключа на отчуждаемом носителе (RuToken, Jacarta и т.д.). и выполните полностью задание №2.

Лабораторная работа №8. Отказоустойчивость. RAID массивы

Цель. Изучение возможностей программный средств создания отказоустойчивых хранилищ данных для обеспечения целостности и доступности информации.
Задание. Выполняется для ОС Microsoft Windows Server и BaseAlt (Альт Рабочая станция, Альт сервер).

- Создать программный отказоустойчивый RAID0 массив в ОС состоящий из двух и более жестких дисков (флеш кард, независимых дисков).
- Сформировать 100 файлов по 100 мегабайт данных.
- Разработать скрипт, копирующий данные на RAID массив и засекающий время копирования информации.

- Считать данные с RAID массива и зафиксировать время чтения данных.
- Повторить эксперимент не менее 25 раз.
- Провести графический статистический анализ результатов быстродействия RAID массива.

Повторить все шаги для RAID массивов уровня 1 и 5. Подготовить сравнительный анализ быстродействия каждого из типов RAID массивов в различных ОС.

- *Дополнительное задание.* Провести тестирование аппаратных RAID контроллеров, встроенных в сервера лаборатории или ваши персональные компьютеры при наличии не менее двух независимых жестких дисков.

Лабораторная работа №9. Домены

Цель. Изучение возможностей создания контура безопасности предприятия на основе доменной структуры. Применение групповых политик безопасности к пользователям и компьютерам предприятия.

Задание. Выполняется для ОС Microsoft Windows Server и BaseAlt (Альт Рабочая станция, Альт сервер).

- Установить роль «Контролера домена» в ОС Microsoft Windows Server.
- Включить в домен одну рабочую станцию на ОС Microsoft Windows 10.
- Включить в домен одну рабочую станцию на ОС BaseAlt (Альт Рабочая станция, Альт сервер).
- Выполнить Лабораторную работу №1 Пользователи и Группы для домена.
- Продемонстрировать доступ к общим папкам со всех рабочих станций.

Дополнительное задание. Настроить единое хранилище профилей пользователя на сетевом диске сервера. Продемонстрировать миграцию профилей пользователя.

Лабораторная работа №10. Аудит событий

Цель. Изучение механизмов регистрации различных событий в ОС. Ознакомление с методами анализа событий по различным критериям.

Задание. Выполняется для ОС Microsoft Windows Server и BaseAlt (Альт Рабочая станция, Альт сервер).

- Настроить политику регистрации событий входа в систему и ошибок входа в систему для домена.
- Распространить политику на все компьютеры домена.
- Написать скрипт на powershell получающий все журналы событий с компьютеров домена.
- Провести анализ журналов событий с указанием всех отказов входа в систему для пользователя «Корейко».
- Провести локальный анализ журналов событий для ОС BaseAlt (Альт Рабочая станция, Альт сервер). Выделить все отказы входа в систему.

Дополнительное задание. Выполняется для ОС Microsoft Windows Server и BaseAlt (Альт Рабочая станция, Альт сервер).

- Создать каталог с файлами журналов удовлетворяющих маске: yyyymmddhhss.txt не менее 100 файлов.
- Написать скрипт реализующий резервную копию данных файлов:
- 1. Все файлы за прошлый месяц отправляются в архив yyyymm.zip
- 2. Все файлы за прошлую неделю отправляются в архив yyyymmKW.zip KW - номер недели в году.

- 3. Все файлы не старше 7 дней остаются в каталоге.

ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Основные понятия и положения защиты информации в информационно вычислительных системах.
2. Угрозы безопасности информации в информационно-вычислительных системах и их классификацию.
3. Основные понятия программно-технического уровня обеспечения информационной безопасности.
4. Основные сервисы безопасности и их особенности.
5. Требования к защите компьютерной информации с учетом различных нормативных документов.
6. Принципиальные недостатки защитных механизмов ОС семейства Windows.
7. Механизм идентификации пользователей в ОС семейства Windows.
8. Механизм аутентификации пользователей в ОС семейства Windows.
9. Механизмы разграничения доступа к файлам в ОС семейства Windows.
10. Файловая система EFS в ОС семейства Windows.
11. Шифрования дисков BitLocker в ОС семейства Windows.
12. Возможности CryptoAPI в ОС семейства Windows.
13. Служба UAC в ОС семейства Windows.
14. Шаблоны безопасности в ОС семейства Windows.
15. Подсистема защиты в ОС семейства Windows.
16. Выявление и устранение уязвимости в подсистеме защиты в ОС семейства Windows.
17. Возможности усиления подсистемы безопасности в ОС семейства Windows.
18. Принципиальные недостатки защитных механизмов ОС семейства UNIX.
19. Механизм идентификации пользователей в ОС семейства UNIX.
20. Механизм аутентификации пользователей в ОС семейства UNIX.
21. Подключаемые модули аутентификации PAM и работе с ними в ОС семейства UNIX.
22. Механизм разграничения доступа к файлам в ОС семейства UNIX.
23. Система шифрования файлов PGP в ОС семейства UNIX.
24. Конфигурация подсистемы защиты в ОС семейства UNIX.
25. Выявление и устранение уязвимости в подсистеме защиты в ОС семейства UNIX.
26. Bash-скрипты и работа с ними в ОС семейства UNIX.
27. Возможности усиления подсистемы безопасности в ОС семейства UNIX.
28. Ведение и анализ журналов безопасности в ОС.