МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению лабораторных работ
по дисциплине «МОДЕЛИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ»
для студентов специальности 10.05.01 Компьютерная безопасность
специализация «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Ставрополь
2026

Содержание

Лабораторная работа № 1. Работа с учётными записями пользователей и группами

Цель работы: изучить особенности и освоить навыки администрирования локальных учётных записей пользователей и групп в операционных системах специального назначения (ОССН) с использованием командной строки и графического интерфейса.

Общие положения

ОССН Astra Linux – многопользовательская ОС, потому учётная запись пользователя – ключевой элемент всей системы управлении доступом. Для идентификации учётных записей пользователей и групп в ОССН, как во всех ОС семейства Linux, используются *uid* и *gid* соответственно. Каждый пользователь должен принадлежать как минимум к одной группе – первичной группе. При создании учётной записи польэователя командой *adduser* или с использованием графической утилиты *fly-admin-smc* создаётся группа, имя которой совпадает с системным именем учётной записи пользователи. Данная группа применяется как первичная группа и будет задана идентификатором в учётной записи пользователя, расположенной в файле */etc/passwd*. Учётная запись пользователя может входить более чем в одну группу.

Для администрирования параметров учётных записей пользователей используются следующие команды и утилиты:

– *useradd* и *adduser* – команды добавления учётной записи пользователя;

– *passwd* – команда смены пароли учётной записи пользователя;

– *usermod* – команда модификации параметров уже существующей учётной записи;

– *userdel* – команда удаления учётной записи пользователя;

– *gpasswd* – команда управления группами;

– *addgroup* – команда создания группы;

– *delgroup* – команда удаления группы;

– *fly-admin-smc* – графическая утилита, позволяющая решать комплекс задач по администрированию учётных записей пользователей и групп, в том числе администрировать параметры мандатного управления доступом и мандатного контроля целостности.

Порядок выполнения работы

1 Начать работу со входа в ОССН в графическом режиме с учётной записью пользователя *user* (уровень доступа – 0, неиерархические категории – нет, уровень целостности – «Низкий»).

2 Запустить терминал *Fly*.

3 Определить текущую учётную запись пользователя с использованием команды *whoami*.

4 Проверить наличие права доступа на чтение к файлу */etc/passwd* и получить следующие данные, выполнив команды *cat /etc/*passwd или *less /etc/passwd*:

– количество параметров учётных записей пользователей;

– количество параметров, совпадающих у всех учётных записей пользователей;

– текущее число учётных записей пользователей;

– количество различных используемых командных интерпретаторов.

5 Вывести строку, соответствующую текущей учётной записи пользователя, из файла *etc/pass*wd с использованием команды *cat /etc/passwd | grep "^$(whoami)"*, при этом получить следующие данные:

– наличие пароля или свёртки пароля (вывести эти данные командой *cat /etc/passwd | grep "^$(whoami)" | cut -d : -f2*;

– группа и идентификатор текущей учётной записи пользователя.

6 Добавить две учётные записи пользователей *user1* и *user2* (с соответствующими домашними каталогами) с использованием команд *sudo adduser user1* и *sudo adduscr user2*.

7 Осуществить последовательные попытки входа в ОССН с учётными записями созданных пользователей *user1* и *user2*. При этом осуществить следующие действия:

– проанализировать причины неудачного входа в ОССН с учётной записью пользователя *user1*, сравнив отличия в командах, использованных при модификации параметров учётных записей пользователей *user1* и *user2*;

– вернуть домашний каталог учётной записи пользователя *user1* командой *usermod -u -d /home/user1 user1*, рассмотреть результат её выполнения, проверить запись о домашнем каталоге в файле *etc/passwd*;

– повторно установить домашний каталог пользователя *user1* командой *usermod -ID -d /home/userone user1*, проверить результат;

– проверить *возможность* входа в ОССН с учётной записью пользователя *user1*, выйти из ОССН.

8 Выполнить удаление учётных записей пользователей:

– удалить учётную запись пользователя *user1* с использованием графической утилиты «Управление политикой безопасности»:

– удалить учётную запись пользователя *user2* командой *sudo deluser user2*;

– удалить учётную запись пользователя *user1* командой *sudo userdel user1*:

– проверить наличие домашних каталогов учётных записей пользователей *userl* и *user2,* после чего с использованием справочной информации по

команде *userdel* определить её параметры, позволяющие удалить содержимое домашнего каталога учётной записи пользователя;

– удалить домашние каталоги учётных записей пользователей *user1* и *user2* непосредственно командами *rm -s / home/userone* и *rm -s /lunne/usertw*o, осуществив попытки удаления без использования и с использованием команды *sudo*;

– проверить наличие домашних каталогов учётных записей пользователей *user1, user2* в каталоге *home/.pdp*.

Контрольные вопросы

1. Какие имеются особенности создания учётных записей пользователей с использованием команд adduser; useradd и графической утилиты «Управление политикой безопасности» (fly-admin-smc), в том числе:

- какой группе должна принадлежать учётная запись пользователя, чтобы была возможность выполнения команды adduser?

- какими командами создаётся учётная запись пользователя, и какие дополнительные параметры при этом вводятся?

- какие ограничения накладываются на пароль учётной записи пользователя при его создании?

- в какие группы автоматически добавляется учётная запись пользователя?

2. Как выполнять привилегированные команды?

3. Создаются ли домашние каталоги учётных записей пользователей при добавлении их с использованием графической утилиты «Управление политикой безопасности»?

4. Создаются ли домашние каталоги учётных записей пользователей при их добавлении с использованием команд adduser и useradd?

5. Какие минимальный и максимальный уровни доступа задаются по умолчанию для учётных записей пользователей, создаваемых командами adduser и useradd?

6. Какими способами можно добавить или удалить учётную запись пользователя из группы?

7. Каким образом организовано хранение сущностей файловой системы ОССН, созданных процессами, обладающими различными уровнями доступа?

8. Где и в каком формате хранятся параметры мандатного управления доступом и мандатного контроля целостности, заданные в ОССН?

9. Где и в каком формате хранятся параметры мандатного управления доступом и мандатного контроля целостности для учётных записей пользователей?

10. Какой командой задаётся максимальный набор неиерархических категорий для текущей учётной записи пользователя?

11. Каким образом осуществляется переход от текущего сеанса к сеансу, функционирующему от имени другой учётной записи пользователя?

12. Позволяют ли команды useradd и adduser задавать параметры мандатного управления доступом и мандатного контроля целостности для создаваемых учётных записей пользователя?

Лабораторная работа № 2. Создание и настройка параметров мандатного управления доступом и мандатного контроля целостности

Цель работы: изучить и освоить администрирование основных параметров мандатного управления доступом в ОССН с применением графических утилит и консольных команд.

Общие положения

В ОССН, наряду с традиционной для ОС семейства Linux системой дискреционного управления доступом, реализована система мандатного управления доступом и мандатного контроля целостности. С этим связано наличие у сущностей ОССН мандатных меток конфиденциальности и целостности.

Параметрами мандатного управления доступом (мандатной меткой) являются следующие элементы:

– уровень доступа или конфиденциальности (соответствует уровню доступа субъект-сессий или конфиденциальности сущности);
– уровень целостности сущности и субъект-сессии;
– набор неиерархических категорий;
– специальные атрибуты (*CCNR*, *CCNRI*, *EHole*).

При установке ОССН (по умолчанию) задаются следующие параметры мандатного управления доступом и мандатного контроля целостности:

– два уровня целостности («Низкий» – значение 0, «Высокий» – 1);
– четыре уровня доступа/конфиденциальности («Уровень 0» – значение 0,

«Уровень 1» – 1, «Уровень 2» – 2, «Уровень 3» – 3); – неиерархические категории – нет.

Мандатное управление доступом процессов (субъект-сессий) к ресурсам (сущностям) основано на реализации соответствующего механизма в ядре ОС. При этом принятие решения о запрете или разрешении доступа субъект-сессии к сущности осуществляется в соответствии с правилами, описанными в рамках модели, и зависит от запрашиваемого вида доступа (чтение, запись, применение права доступа на выполнение) и мандатного контекста (используемых в запросе уровней конфиденциальности, доступа и целостности).

Практическое задание

1 Начать работу в графическом режиме с учётной записью пользователя *user* (уровень доступа – 0, неиерархические категории – нет, уровень целостности – «Низкий»).

2 Запустить графическую утилиту редактирования учетных записей пользователей «Управление политикой безопасности» через меню «Настройки» главного пользовательского меню.

3 Модифицировать параметры мандатного управления доступом, для этого осуществить следующие действия:

– открыть раздел «Уровни», выбрать «0: Уровень_0)» и переименовать данный уровень доступа: «Уровень 0»;

– осуществить попытку создания уровня доступа с именем «Уровень_4», установив значение, равное 4. Проанализировать результат;

– выполнить создание уровня доступа с именем «Уровень_4», задав значение, равное 1, после чего проверить наличие записи «Уровень_4» в списке «Уровни»;

– выполнить обратное переименование «Уровень 1» в «Уровень 0».

4 Создать учётную запись пользователя *user1*, установив максимальный уровень доступа «Уровень_4».

5 Выполнить удаление уровня доступа 1 из раздела «Уровни» путем выбора в контекстном меню пункта «Удалить».

6 Открыть учётную запись пользователя *user1* и в закладке «Дополнительные» в элементе «Максимальный уровень» проверить наличие записи «(4)», при этом в списке выбора уровня «Уровень 4» будет отсутствовать.

7 Вывести в терминал *Fly* параметры мандатного управления доступом для учётной записи пользователя *user1*. Для этого выполнить следующие действия:

– запустить терминал *Fly* и перейти в каталог */etc/parsec/macdb*;

– прочитать параметры учётной записи *nscil* командой *sudo grep "user1" **;

– определить максимальный уровень доступа учётной записи *user1* командой *sudo grep "user1" * | cat -d : -f 5*;

– определить минимальный уровень доступа учётной записи *user1* командой *sudo grep "user1" * | cat -d : -f* 3 и проверить его соответствие данным, отображаемым в графической утилите «Управление политикой безопасности».

8 Изменить мандатный уровень доступа с использованием графической утилиты «Управление политикой безопасности».

9 Вынести в терминал *Fly* параметры мандатного управления доступом и мандатного контроля целостности.

Контрольные вопросы

1 Какие уровни доступа и иерархические категории создаются при установке ОССН?

2 Как добавить новые уровни доступа и иерархические категории?

3 Каковы особенности удаления и модификации уровней доступа и иерархических категорий в ОССН?

4 Какие команды используются для создання, модификации и удаления уровней доступа и иерархических категорий в ОССН?

5 Какие команды используются для настройки привилегий учётных записей пользователей?

6 Как принудительно удалить привилегии для заданной учётной записи пользователя?

Лабораторная работа № 3. Мандатное управление доступом в файловой системе

Цель работы: получить навыки администрирования мандатного управления доступом и контроля целостности в файловых системах *Ext2* / *Ext3* / *Ext4* в ОССН и навыки использования для этого графической утилиты «Управление политикой безопасности», менеджера файлов, а также консольных команд.

Общие положения

В ОССН мандатное управление доступом интегрировано в файловую систему за счёт хранения в ней не только дискреционных прав доступа, но и мандатных меток файлов с дополнительными специальными атрибутами. Параметрами мандатного управления доступом (мандатной меткой) каждой сущности файловой системы являются: – уровень конфиденциальности; – уровень целостности:

– набор неиерархических категорий;

– специальные атрибуты.

Наличие у сущности файловой системы мандатных меток целостности позволяет дополнительно усилить защиту от несанкционированной модификации файлов, влияющих на безопасность ОССН. Это реализуется установкой уровня целостности «Высокий», что позволяет предотвратить изменение или удаление таких файлов процессами с низким уровнем целостности.

Практическое задание

1 Начать работу в графическом режиме с учётной записью пользователя *user* (уровень доступа – 0, неиерархические категории – нет, уровень целостности – «Низкий»).

2 Создать неиерархические категории с использованием графической утилиты «Управление политикой безопасности». Дня этого выполнить следующие действия: в разделе «Категории» создать следующие новые неиерархические категории: «Группа_1» со значением «Разряд», равным 0, «Группа_2» со значением «Разряд», равным 1, «Группа _3» со значением «Разряд», равным 2.

3 Создать новую группу с именем *office1* с использованием графической утилиты «Управление политикой безопасности».

4 Создать новые учётные записи пользователей *user1*, *user2*, *user3*.

5 Изучить особенности однопользовательской работы с сущностями файловой системы на различных мандатных уровнях доступа и с различными наборами неиерархических категорий с использованием графической утилиты *fly-fm*.

6 Выполнить вывод мандатных меток конфиденциальности и целостности файлов 01.txt, 11.txt, 21.txt с использованием графической утилиты *fly-fm*.

7 Изучить особенности многопользовательской работы с сущностями файловой системы на различных уровнях доступа и целостности и с различными наборами неиерархических категорий.

Контрольные вопросы

1. Какие команды используются для изменения или просмотра параметров мандатного управления доступом файлов?
2. Как организовано хранение файлов в домашних каталогах учётных записей пользователей при работе на различных уровнях доступа?
3. Какие параметры мандатного управления доступом устанавливаются по умолчанию при создании файлов и каталогов?
4. Каково назначение специальных атрибутов CCNR , CCNRI и Ehole?
5. Какие имеются особенности работы с сущностями файловой системы при функционировании процессов, имеющих различные уровни целостности?
6. Каковы особенности создания каталогов, предназначенных для хранения файлов с различными параметрами мандатного управления доступом?

Лабораторная работа № 4. Аутентификация пользователей в системе. Работа с модулями PAM

Цель работы: получить практический опыт настройки системы аутентификации (в том числе двухфакторной) в ОССН с использованием модулей PAM (Pluggable Authentication Modules).

Общие положения

Для подключённых модулей PAM их конфигурирование выполняется путем редактирования файлов в каталогах */etc/security* и */etc/pam.d*. При использовании аутентификации с использованием PAM формируется стек модулей обработки запроса на аутентификацию. Например, в ОССН имеется модуль *pam_limits.so* (с конфигурационным файлом */etc/security/limits.conf*), позволяющий задавать для учётных записей пользователей ограничения на параметры работы функцио- нирующих от их имени процессов, или модуль *pam.cracklib.so*, реализующий правила формирования новых паролей учётных записей пользователей, что позволяет ограничивать минимальную длину пароля, задавать сложность пароля и другие параметры.

В ОССН реализованы следующие типы модулей PAM:

– auth – модули аутентификации;
– account – модули управления учётными записями пользователей;
– session – модули управления сеансами;
– password – модули управления паролями учётных записей пользователей.

При реализации двухфакторной аутентификации электронный идентификатор (ЭИ) должен быть совместим с ОССН. Кроме того, для работы с ЭИ необходима установка дополнительных пакетов, содержащих драйверы или иные необходимые для функционирования ЭИ файлы.

При проверке корректности двухфакторной аутентификации с использованием ЭИ необходимо оставлять возможность штатной аутентификации. В противном случае, например, при неправильной настройке ЭИ, вход в систему с использованием штатной аутентификации будет невозможен и потребуется восстановление ОССН.

Для работы с модулями PAM и ЭИ используются следующие команды:

– *pam-auth-update* – команда управления активными профилями PAM;
– *passwd* – команда смены пароля учётной записи пользователя;
– *pkcs15-tool* – команда для работы с параметрами ЭИ;
– *pkcs15-init* – команда инициализации ЭИ;
– *openssl* – команда для работы с ключевой информацией и ЭИ.

Практическое задание

1 Начать работу в графическом режиме с учётной записью пользователя *user* (уровень доступа – 0, неиерархические категории – нет, уровень целостности – «Низкий») и запустить терминал *Fly* в привилегированном режиме командой *sudo fly-term*.

2 Определить модули PAM, установленные в ОССН, командой *find / -name "pam_*.so"* и выяснить их расположение в каталогах ОССН.

3 Проанализировать текущие настройки PAM в файле *etc/pam.conf* командой *less /etc/pam.con*f.

4 Перейти в каталог */etc/pam.con*f для настройки модулей PAM. Считать список файлов сценариев аутентификации командой *ls –l.*

5 Проанализировать общие настройки аутентификации по файлу */etc/pamd/common-auth*, выполнив команду *less common-auth*.

6 Проверить настройки паролей, для этого выполнить следующие действия:

– запустить графическую утилиту «Управление политикой безопасности» и открыть раздел «Глобальная политика»;

– сравнить значения параметров использования паролей, заданные во вкладке «Параметры изменения пароля» и в файле */etc/login.defs*, во вкладке «Параметры структуры поля» и в файлах *cracklib* и *common-password*.

7 Выполнить смену пароля учетной записи текущего пользователя командой *passwd* и ввести старый пароль, а затем проверить параметры паролей путём его смены и просмотра предупреждающих сообщений.

8 Проверить работу двухфакторной аутентификации на различных уровнях доступа.

Контрольные вопросы

1 Какие типы модулей PAM поддерживаются в ОССН?

2 Каким образом осуществляется обработка стека модулей PAM при аутентификации от имен и учетных записей пользователей в ОССН?

3 Какими командами создаются ключевые пары на ЭИ?

Лабораторная работа № 5. Настройка механизмов организации замкнутой программной среды

Цель работы: изучить принципы и технологии контроля целостности средств защиты (КСЗ), реализованных в ОССН; освоить умения, необходимые для решения задач контроля целостности и создания замкнутой программной среды.

Общие положения

Механизм замкнутой программной среды позволяет ограничить доступ пользователей к исполняемым файлам только теми программами, которые необходимы им для работы.

При использовании этого механизма действуют следующие правила:

– пользователь может запустить программу только из списка разрешенных для запуска программ (*UEL*-список, *User Executable List*). Этот список формируется индивидуально для каждого пользователя;

– замкнутая программная среда может быть включена выборочно для от-дельных пользователей;

– замкнутая программная среда может использоваться в одном из двух ре-жимов работы: «мягком» или «жестком».

При «мягком» режиме пользователю разрешается запускать любые программы, а не только входящие в UEL-список. При этом в журнале безопасности регистрируются соответствующие события несанкционированного доступа (НСД).

При «жестком» режиме запуск программы разрешается, если:

– разрешен запуск файла в *UEL*-списке;

– файл не доступен текущему пользователю на изменение;

– файл не находится на сменном носителе;

– владельцем файла является локальная группа администраторов (это дополнительное ограничение, которое может и не использоваться).

Механизм контроля целостности исполняемых файлов и разделяемых библиотек формата ELF при запуске программы на выполнение реализован в модуле ядра ОС *digsig_verif*, который является невыгружаемым модулем ядра ОССН и может функционировать в одном из следующих режимов:

– исполняемым файлам и разделяемым библиотекам с неверной электронной цифровой подписью (ЭЦП), а также без ЭЦП загрузка на исполнение запрещается (штатный режим функционирования);

– исполняемым файлам и разделяемым библиотекам с неверной ЭЦП, а также без ЭЦП загрузка на исполнение разрешается, при этом выдается сообщение об ошибке проверки ЭЦП (режим для проверки ЭЦП);

– ЭЦП при загрузке исполняемых файлов и разделяемых библиотек не про-веряется (отладочный режим для тестирования).

Механизм контроля целостности файлов при их открытии на основе ЭЦП в расширенных атрибутах файловой системы также реализован в модуле ядра ОС *digsig_verif* и может функционировать в одном из следующих режимов:

– запрещается открытие файлов, поставленных на контроль, с неверной ЭЦП или без ЭЦП;

– открытие файлов, поставленных на контроль, с неверной ЭЦП или без ЭЦП разрешается, при этом выдается сообщение об ошибке проверки ЭЦП

(режим для проверки ЭЦП в расширенных атрибутах файловой системы); – ЭЦП при открытии файлов не проверяется.

Практическое задание

1 Запустить терминал *Fly* в «привилегированном» режиме командой *sudo fly-term*.

2 Просмотреть загруженные модули ядра ОССН и вынести в терминал данные о невыгружаемом модуле *digsig_verif* конвейером команд *lsmod* | *grep digsig-verif*.

3 Выполнить импорт открытых ключей, используемых для проверки ЭП файлов. Для этого выполнить следующие действия:

– инициализировать каталог */roof/.gnupg* при просмотре текущих ключей командой *gpg --list-sigs*;

– импортировать открытый мастер-ключ «NPO RusBITech» командой *gpg --import /etc/digsig/primary_key.gpg*;

– импортировать открытый ключ «ССТ RusBITech», используемый для ЭП файлов, командой *gpg --import /etc/digsig/key_for_signing.gpg*.

4 Вывести текущие ключи командой *gpg --list-sigs*. Определить идентификатор мастер-ключа.

Контрольные вопросы

1 Каким вариантом модулей ядра ОССН является модуль *digsig.verif*?

2 Какой формат файлов ключей ЭП СПО использует модуль *digsig.verif*?

3 Какой файл сценария командного интерпретатора *bash* применяется для хранения ключей ЭП для модуля *digsig.verif*?

4 Связан ли модуль *digsig.verif* с другими загружаемыми (невыгружаемыми) модулями?

Лабораторная работа № 6. Настройка сетевого взаимодействия

Цель работы: изучить принципы и порядок конфигурирования сетевого взаимодействия узлов автоматизированной системы в защищенном исполнении (АСЗИ) на базе ОССН; освоить навыки решения задач управления сетевыми интерфейсами и протоколами, а также маршрутизацией пакетов.

Общие положения

Взаимодействие узлов АСЗИ между собой и с сетевым оборудованием в сетях с пакетной коммутацией на базе стека протоколов TCP/IP основано на сетевых службах, реализуемых соответствующими процессами в ОССН. Такие процессы на серверных узлах АСЗИ создают программные интерфейсы (сокеты), связанные с требуемыми сетевыми службами сетевыми портами. Процессы ОССН на клиентских узлах АСЗИ формируют запрос на открытие соответствующего сокета с указанием IP-адреса и сетевого порта серверных узлов АСЗИ. Результатом выполнения такого запроса является установление соединения между серверными и клиентскими узлами ОССН в рамках заданной сетевой службы.

Особенностью этого соединения в ОССН является поддержка передачи по нему данных мандатного контекста сущностей сетевой службы и субъектов доступа к ней. При этом монитором обращений выступает подсистема безопасности *PARSEC*. В случаях, когда сетевой сервис не обрабатывает данные мандатного контекста, однако осуществляет соединение с процессами ОССН, работающими в различных мандатных контекстах, применяется механизм *privsock*.

Конфигурация сетевых интерфейсов, настройка адресной информации и статической маршрутизации пакетов реализуются наборами команд *Net tools* (пакет *nettools*) и *Iproute2* (пакет *iproute*), графической утилитой *fly-admin-device-manager* и командой *cthtool*. Для статического конфигурирования параметров сетевых интерфейсов также используется конфигурационный файл */etc/network/interfaces*, а для управления запуском программ перед инициализацией и закрытием сетевых интерфейсов – наборы сценариев, расположенные в каталогах */etc/network/if-np.d*, */etc/network/if-down.d*, */etc/if-pre-up.d* и */etc./ifpost-down.d.*

Практическое задание

1 Начать работу со входа в ОССН *AstraClient1*, *AstraClient2* и *AstraRouter* в графическом режиме с учётной записью пользователя *user* (уровень доступа – 0, неиерархические категории – нет, уровень целостности – «Низкий»).

2 В ОССН *AstraClient1*, *AstraClient2* и *AstraRouter* запустить терминал *Fly* в привилегированном режиме командой *sudo fly-term* и вывести информацию о доступных сетевых интерфейсах командой *ip link list*.

3 Настроить ОССН *AstraClient1*.

4 Выполнить настройки сетевого интерфейса ОССН *AstraClient2*.

5 В ОССН *AstraRouter* выполнить настройку статических сетевых адресов и маршрутизации.

6 Проверить функционирование маршрутизации между подсетями.

7 Выполнить настройки сетевых интерфейсов в ОССН *AstraClient1* с использованием графической утилиты «Сетевые соединения».

8 Проверить совместную работу программ конфигурирования сетевых интерфейсов в ОССН *AstraClient1*.

9 Настроить DNS-сервер в ОССН *AstraRouter* для работы с использованием механизма */network*.

10 Проверить работу ОССН *AstraClient1* с DNS-сервером в сессии, функционирующей от имени учётной записи пользователя *user* с мандатным уровнем доступа, равным 2.

Контрольные вопросы

1 Укажите назначение пакета *inroute*.
2 Какие основные команды входят в пакет *inroute*?
3 Каковы отличительные особенности пакетов *inroute* и *net-toole*?

Лабораторная работа № 7. Конфигурирование службы AstraLinuxDirectory

Цель работы: получить практический опыт установки и настройки параметров службы Astra Linux Directory (ALD) в ОССН.

Общие положения

В компьютерных сетях, построенных на основе ОССН, имеется возможность организовать централизованное хранение учётных записей пользователей в домене *ALD* (далее – домене), а также развёртывать централизованный защищенный файловый сервер, содержащий сетевые домашние каталоги данных учётных записей пользователей. Таким образом, у учётных записей пользователей *ALD* появляется возможность регистрации и доступа к своим сетевым объектам с любого компьютера, входящего в домен. Это особенно актуально в случае территориальной удалённости между контроллером *ALD* и компьютерами, входящими в состав домена.

Администратор домена выполняет следующие функции по управлению доменом:

– централизованное управление учётными записями пользователей домена с использованием команды *ald-admin* и графической утилиты «Управления политикой безопасности»;

– настройка СЗИ, управляющих их доступом к файловым сущностям защищенного файлового сервера.

Служба *ALD* обладает расширяемой архитектурой, состоящей из ядра, отвечающего за основной функционал системы, ряда интерфейсов (*LDAP*, *Kerberos*) и модулей расширения, команд и графических утилит настройки служб и подсистем *ALD*, что позволяет расширять функциональность *ALD*, устанавливая дополнительные пакеты.

На компьютере, осуществляющем функции контроллера *ALD*, операции по администрированию *ALD* выполняются от имени учётных записей пользователей, обладающих соответствующими административными полномочиями. В зависимости от назначенных привилегий администраторов *ALD* можно разделить на следующие группы по полномочиям:

– корневой администратор (имя *admin/admin*, администратор *ALD*) обладает всеми полномочиями по управлению доменом;

– администраторы (пользователи с привилегией *admin*) обладают полномочиями по управлению конфигурацией домена и учётными записями пользователей;

– ограниченные администраторы (учётные записи пользователей с привиле-гиями *hosts-add* или *all-hosts-add*) обладают полномочиями по добавлению компьютеров в домен;

– пользователи утилит администрирования (пользователи с привилегией *adm-user*) обладают полномочиями по запуску утилит администрирования; – обычные пользователи.

Для администрирования домена используются команды *ald-admin* и графическая утилита «Управление политикой безопасности».

Практическое задание

1 Для настройки сетевого соединения на контроллере и клиентах *ALD* начать работу со входа в ОССН *AstraClient1*, *AstraClient2* и *AstraServer* в графическом режиме с учётной записью пользователя *user* (уровень доступа – 0, неиерархические категории – нет, уровень целостности – «Низкий»).

2 В ОССН *AstraClient1, AstraClient2* и *AstraServer* выполнить настройку статических сетевых адресов.

3 Выполнить проверку корректности настроек командой *ping*. При этом проверить доступность *AstraClient1*, *AstraClient2* с *AstraServer* по сети командами *ping 10.0.0.1* и *ping 10.0.0.2*. Затем проверить доступность *AstraClientl* с *AstraClient2* командой *ping 10.0.0.1*. В каждом случае количество полученных «*recieved*»-пакетов должно соответствовать количеству отосланных «*transmitted*».

4 Выполнить установку, конфигурирование, запуск клиентов *ALD*.

5 Осуществить проверку функционирования и настройку контроллера и клиентов *ALD*.

6 Создать новую учётную запись пользователя *ALD* и осуществить вход с неё в ОССН *AstraClient1*.

Контрольные вопросы

1 Каково назначение служб контроллера *ALD*?

2 Какие службы устанавливаются на контроллер *ALD*?

3 Каковы особенности настройки имен компьютеров, входящих в домен?

Лабораторная работа № 8. Управление программными пакетами. Настройка системных служб

Цель работы: освоить администрирование пакетов ОССН, в том числе используемых для этого команд и графических утилит, а также администрирование и настройку системных служб.

Общие положения

Система управления пакетами ОССН включает несколько команд и утилит, которые могут работать в режиме командной строки, в псевдографическом и графическом режимах. При этом порядок действий при их использовании для изменения состава установленных в ОССН пакетов принципиально не отличается, за исключением, возможно, установки взаимосвязанных пакетов.

Для управления пакетами применяются утилиты *aptitude*, «Менеджер пакетов *Synaptic*», команды системы управления пакетами *APT* и команда *dpkg*.

Для управления запуском системных служб используется команда *service имя_службы <команда>*. В качестве параметров команды применяются *start*, *stop*, *restart*, *status* для запуска, останова, перезапуска или определения статуса системной службы соответственно. Просмотр уровней запуска системных служб может быть осуществлён с использованием команд *service --status-all* или более наглядной *chkcontig -list*. Для включения/отключения системной службы на конкретном уровне может быть использована команда *chkconfig имя-службы <on|off>*. Аналогичные функции реализует графическая утилита *fly-admin-runlevel*.

Практическое задание

1 Начать работу в ОССН в графическом режиме учётной записью пользователя *user* (уровень доступа – 0, неиерархические категории – нет, уровень целостности – «Низкий»).

2 Запустить терминал *Fly* и перейти в каталог */etc/apt*.

3 Вывести дискреционные права доступа к файлу *sources.list* командой *ls-l sources.list*. Определить возможность изменения файла при работе от имени данной учётной записи пользователя.

4 Запустить второй терминал *Fly* командой *sudo fly-term* и в нём выполнить команду *aptitude*.

5 В первом терминале выполнить попытку удаления пакета *ed* командой *aptget remove ed*, проанализировать выводимые ошибки.

6 Завершить *aptitude* во втором терминале. В первом терминале повторить удаление пакета *ed* командой *apt-get remove ed*. Проанализировать отображаемые в терминале сообщения и определить количество удаленных пакетов.

7 Выполнить проверку статуса установленных пакетов, для чего осуществить следующие действия:

– в привилегированном режиме терминала *Fly* запустить утилиту *aptitude* и проанализировать предупреждения;

– нажать клавишу «c» для просмотра первого решения об установке пакета *vim-common*;

– выполнить просмотр следующего решения и выйти из утилиты *aptitude*.

8 Выполнить настройку пакетов в графической утилите *Synaptic*, для чего осуществить следующие действия:

– запустить графическую утилиту *Synaptic*, при этом ввести пароль текущей учётной записи пользователя для возможности работы в привилегированном режиме;

– открыть меню «Настройки/Репозитории» и проверить наличие неактивного репозптория, который был ранее закомментирован в файле *sources.li*st; – удалить неактивный и активный репозитории.

9 Для управления системными службами выполнить следующие действия:

– в привилегированном режиме терминала *Fly* получить текущие статусы запускаемых системных служб командой *service_status-all*;

– определить статус системной службы *nfs-kernel-server* командой *service nfs-kernel-server status*;

– выполнить попытку определения статуса системной службы *console setup* командой *service console-setup status* и проанализировать результат;

– для анализа порядка вызова команды *service* вывести на экран содержимое файла *console-setup* командой *cat /etc/init.d console-setup*;

– аналогично по содержимому файла *console-setup* найти реализацию вызова команды *status*.

Контрольные вопросы

1 Каковы особенности одновременной работы нескольких утилит управления пакетами?

2 Какие команды позволяют работать с зависимыми пакетами в автоматическом режиме?

3 Как определить статус запуска системной службы?

Лабораторная работа № 9. Контроль целостности комплекса средств зашиты

Цель работы: изучить принципы и технологии контроля целостности комплекса средств защиты (КСЗ), реализованных в ОССН.

Общие положения

АСЗИ на базе ОССН должны обеспечивать функции как аудита доступа к сущностям файловой системы, так и контроля целостности (*integrity*) данных и содержимого исполняемых файлов.

Подобный контроль позволяет с достаточной уверенностью констатировать факт отсутствия в данных, обрабатываемых системными процессами ОССН, недекларируемых для АСЗИ возможностей.

Для решения задачи контроля целостности в состав КСЗ ОССН включены средства, реализующие частные функции управления целостностью данных:

– вычисления и проверки контрольных сумм файлов и оптических дисков: – контроля соответствия дистрибутиву; – регламентного контроля целостности.

Контрольная сумма – значение, рассчитанное по набору данных путём применения определённого алгоритма и используемое для проверки целостности данных при их передаче или хранении. Она используется для быстрого сравнения двух наборов данных на эквивалентность: с большой вероятностью отличающиеся наборы данных будут иметь разные контрольные суммы.

Проверка соответствия модулей установленной ОССН модулям, входящим в состав её дистрибутива, является вариантом статического контроля целостности и обеспечивает контроль целостности файловых сущностей, копируемых в корневой раздел ОССН на этапе установки, что позволяет убедиться в отсутствии изменений в файловых сущностях модулей, произошедших на этапе их эксплуатации.

Практическое задание

1 Начать работу со входа в ОССН в графическом режиме с учетной записью пользователя *user* (уровень доступа – 0, неиерархические категории – нет, уровень целостности – «Низкий») и запустить терминал *Fly* в привилегированном режиме командой *sudo fly-term*.

2 В домашнем каталоге создать подкаталог *checksum* и скопировать в него все файлы (исключая вложенные каталоги) из каталога */etc*.

3 Используя алгоритм *MD5* вычислить контрольные суммы всех файлов в каталоге */home/user/checksum* и перенаправить результат их вычисления в файл */home/user/md5check*, а поток «перечень ошибок» – в файл */home/user/error.md5*.

4 Используя алгоритм *SHA-512/256*, вычислить контрольные суммы всех файлов в каталоге */home/user/checksum*.

5 Изменить содержимое файла /*etc/fstab*, удалив в нем две первые строки.

6 Запустить графическую утилиту «Контроль целостности файлов» (*aficktk*) управления системой *AFICK* из меню «Системные» главного пользовательского меню и выполнить принудительную проверку целостности, выбрав действие – сравнение с базой.

7 После завершения контроля целостности в меню утилиты *afick-tk* «Файлистория» определить дату и время последнего принудительного контроля целостности.

8 Проанализировать найденную запись о нарушении целостности п определить параметры, соответствующие действиям (*action*) нарушения целостности, и их текущие значения.

Контрольные вопросы

1 В каких средствах контроля целостности используется библиотека *libgost*?

2 Как инициализировать базу данных системы регламентного контроля *AFICK* после внесения изменений в её конфигурационный файл?

3 Каким образом реализована взаимосвязь системы регламентного контроля целостности *AFICK* и сервиса *cron*?

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по проведению практических занятий
по дисциплине «МОДЕЛИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ»
для студентов специальности 10.05.01 Компьютерная безопасность
специализация «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Ставрополь
2026

Содержание

Практическое занятие 1. Оценка рисков информационной безопасности

Оценка рисков информационной безопасности – это процесс систематического анализа и оценки потенциальных угроз, уязвимостей и возможных последствий для информационных активов организации. Она выполняется с целью идентификации и оценки потенциальных угроз безопасности информации, выявления уязвимостей, анализа возможных последствий и разработки соответствующих мер по снижению рисков.

Оценка рисков информационной безопасности имеет несколько целей и применений:

1. Идентификация потенциальных угроз: Оценка рисков позволяет идентифицировать и анализировать различные угрозы, которые могут нанести вред информационным активам организации. Это может быть несанкционированный доступ к данным, вредоносные программы, физические кражи или потери информации и другие виды атак. Идентификация угроз позволяет организации более точно определить, какие меры безопасности нужно предпринять для защиты своей информации.

2. Анализ уязвимостей: Оценка рисков также включает анализ уязвимостей, которые могут быть использованы злоумышленниками для атаки на информационные активы. Уязвимости могут быть связаны с программным обеспечением, сетевой инфраструктурой, аутентификацией и другими аспектами информационной системы. Последствиями уязвимостей могут быть несанкционированный доступ, потеря данных, нарушение конфиденциальности и целостности информации. Анализ уязвимостей позволяет организации выявить слабые места в своей информационной системе и принять соответствующие меры по защите.

3. Оценка возможных последствий: Оценка рисков информационной безопасности помогает оценить потенциальные последствия нарушения безопасности информации. Это может включать финансовые потери, ущерб репутации организации, правовые и юридические последствия, а также нарушение доверия клиентов и потерю бизнеса. Оценка последствий помогает организации понять важность и воздействие безопасности информации на ее деятельность и принять соответствующие меры по снижению рисков.

4. Принятие решений по снижению рисков: Оценка рисков информационной безопасности предоставляет организации информацию,

необходимую для принятия обоснованных решений по повышению безопасности информации. На основе результатов оценки, организация может определить наиболее критичные угрозы и уязвимости, определить приоритеты в области безопасности, а также разработать и реализовать соответствующие меры защиты. Это может включать технические, организационные и юридические меры, такие как использование современных методов шифрования, установка брандмауэров, обучение персонала и установление политик безопасности.

5. Соответствие требованиям нормативных актов: Оценка рисков информационной безопасности также позволяет организации установить соответствие требованиям нормативно-правовых актов в области защиты информации. Многие отраслевые стандарты и законодательные акты требуют проведения систематической оценки рисков и принятия соответствующих мер для обеспечения безопасности информации. Оценка рисков помогает организации определить, в какой степени она соответствует требованиям законодательства и нормативов и принять меры по их выполнению.

В конечном итоге, оценка рисков информационной безопасности играет важную роль в понимании угроз, уязвимостей и возможных последствий для информационных активов. Она помогает организации определить приоритеты в области безопасности, разработать соответствующие меры по снижению рисков и обеспечить соответствие нормативам и требованиям в области защиты информации.

Основные методы оценки рисков информационной безопасности:

1: При использовании метода экспертных оценок для оценки рисков информационной безопасности, специалисты и эксперты в данной области анализируют и оценивают потенциальные угрозы и уязвимости, основываясь на своем опыте и экспертном мнении. Они могут применять различные методики, такие как опросы, интервью, фокус-группы и т.д., чтобы собрать информацию о возможных рисках. После этого эксперты оценивают вероятность возникновения угрозы и возможные последствия, присваивая им определенные значения или категории. Затем производится агрегация оценок, чтобы определить общую оценку риска информационной безопасности.

2: При использовании методов экономики для оценки рисков информационной безопасности, основное внимание уделяется экономическим аспектам. В этом случае, риски оцениваются с точки зрения финансовых потерь, которые могут возникнуть в результате нарушения информационной безопасности. Методы, такие как квантификация рисков, стоимостной анализ, оценка затрат на восстановление и перспективный анализ, могут быть

использованы для определения экономической ценности информации и принятия решений о мерах по снижению рисков.

3: Оценка рисков информационной безопасности на основе права подразумевает анализ соответствия мероприятий по обеспечению информационной безопасности нормативно-правовым требованиям. Здесь используются законодательные акты, нормы и стандарты для определения требований к безопасности информации. Риски оцениваются путем анализа наличия и эффективности принятых правовых и организационных мер, а также определения возможных юридических последствий нарушений информационной безопасности.

4: Оценка рисков информационной безопасности в соответствии со степенями секретности предполагает классификацию информации по степени ее значимости и конфиденциальности. В данном случае, риски оцениваются на основе возможности несанкционированного доступа, утечки или компрометации информации разных уровней секретности. Разработанные протоколы, классификационные системы и критерии определения степени секретности помогают в оценке рисков и принятии соответствующих мер по защите информации.

5: Вероятностные методы оценки рисков информационной безопасности основываются на анализе вероятности возникновения различных угроз и их воздействия на информацию и системы. Здесь используются статистические данные, историческая информация, экспертные оценки и другие факторы, чтобы определить вероятность возникновения рисков и их влияние на информационные активы. Методы, такие как статистический анализ, моделирование и симуляция, могут применяться для количественной оценки вероятностей и последствий рисков.

6: Методы теории графов применяются для оценки рисков информационной безопасности путем анализа связей и взаимодействий между информационными активами, уязвимостями и потенциальными угрозами. Графическое представление информационных систем и их компонентов позволяет идентифицировать уязвимости, потенциальные пути атаки и цепочки последствий. Это помогает оценить риски и принять меры по улучшению информационной безопасности.

7: Оценка рисков информационной безопасности с использованием логических методов основывается на анализе логических отношений и причинно-следственных связей между угрозами, уязвимостями и возможными последствиями. Здесь применяются методы логического вывода, моделирования и дедукции для анализа рисков и принятия решений по их снижению. Объективная логическая оценка позволяет выявить потенциальные проблемы и разработать соответствующие стратегии по обеспечению безопасности информации.

Задание: Описать оценку рисков информационной безопасности (по вариантам).

Вариант 1	Методом экспертных оценок.
Вариант 2	Методами экономики.
Вариант 3	На основе права.
Вариант 4	В соответствии со степенями секретности.
Вариант 5	Вероятностными методами.
Вариант 6	Методами теории графов.
Вариант 7	Логическими методами.

Контрольные вопросы

1. Какие основные шаги необходимо выполнить при проведении оценки рисков информационной безопасности?
2. Какие факторы необходимо учитывать при оценке рисков информационной безопасности?
3. Какие методы и инструменты могут быть использованы для оценки рисков информационной безопасности?
4. Как идентифицировать потенциальные угрозы безопасности информации в организации?
5. Какие преимущества имеют качественные и количественные методы оценки рисков информационной безопасности?
6. Какие документы и информацию требуется собрать для проведения оценки рисков информационной безопасности?
7. Каким образом определить уязвимости в информационной системе и их ранг по степени угрозы?
8. Какие факторы могут повлиять на возникновение и воздействие угроз информационной безопасности?
9. Как определить вероятность возникновения и последствий угроз для информационных активов организации?
10. Каким образом оценить финансовые, репутационные и операционные риски в области информационной безопасности?
11. Какие критерии использовать при приоритизации рисков информационной безопасности?
12. Какие меры безопасности могут быть приняты для снижения рисков информационной безопасности и предотвращения угроз?

13. Какие изменения в нормативных актах и требованиях по безопасности информации необходимы для обеспечения эффективной оценки рисков?

14. Как оценить эффективность принятых мер по снижению рисков информационной безопасности?

15. Какие роли и ответственность играют сотрудники организации в оценке и управлении рисками информационной безопасности?

Практическое занятие 2. Оценка эффективности организации информационной безопасности

Оценка эффективности организации информационной безопасности - это процесс анализа и измерения результатов и эффективности принятых мер для обеспечения безопасности информации в организации. Она позволяет определить, насколько эффективно функционируют механизмы защиты информации и какие улучшения могут быть внедрены для повышения уровня безопасности.

Основная цель оценки эффективности организации информационной безопасности заключается в обеспечении достаточного уровня защиты информации от различных угроз, таких как несанкционированный доступ, внутренние и внешние атаки, утечки данных и другие нарушения безопасности. Кроме того, оценка эффективности позволяет:

1. Идентифицировать слабые места и уязвимости в системе безопасности: Оценка эффективности помогает выявить существующие проблемы и уязвимые места в инфраструктуре информационной безопасности организации. Это может быть связано с недостаточной защитой сети, недостаточными политиками безопасности, устаревшими системами или недостаточно подготовленным персоналом. Идентификация таких проблем помогает принять меры по их устранению.

2. Измерить эффективность принятых мер безопасности: Оценка эффективности позволяет измерить эффективность принятых мер безопасности. Она помогает определить, насколько эффективно действуют механизмы защиты и контроля, такие как брандмауэры, системы обнаружения вторжений, контроль доступа и шифрование данных. Это помогает оценить, насколько система безопасности может устоять перед потенциальными атаками и на сколько успешно она предотвращает потенциальные инциденты безопасности.

3. Повысить осведомленность и подготовку персонала: Оценка эффективности позволяет оценить подготовку и осведомленность персонала об информационной безопасности. Персонал является одним из основных звеньев в системе безопасности. Подготовленный и осведомленный персонал способен эффективно реагировать на потенциальные угрозы и предотвращать инциденты безопасности. Оценка эффективности помогает выявить необходимые области улучшения и обеспечить обучение персонала в соответствии с современными требованиями безопасности.

4. Предоставить информацию для стратегического планирования: Оценка эффективности информационной безопасности обеспечивает ценную информацию для стратегического планирования. Результаты оценки могут помочь выявить приоритеты и определить направления развития системы безопасности. На основе этих данных можно разработать и реализовать целенаправленные меры по улучшению безопасности информации, оптимизации инфраструктуры и использованию ресурсов.

5. Соответствие нормативным требованиям и стандартам безопасности: Оценка эффективности помогает установить, насколько система безопасности соответствует нормативным требованиям и стандартам безопасности. Многие отраслевые регуляторы и стандарты, такие как GDPR, ISO 27001 и др., определяют специфические требования в области информационной безопасности. Оценка эффективности позволяет оценить степень соответствия организации таким требованиям и принять меры по их выполнению.

В целом, оценка эффективности организации информационной безопасности помогает собрать объективные данные, выявить проблемные области, определить приоритеты и принять меры по обеспечению безопасности информации. Она служит инструментом для постоянного улучшения и совершенствования системы безопасности организации и обеспечивает защиту информации от разнообразных угроз.

Задание: Описать оценку эффективности организации информационной безопасности (по вариантам).

Вариант 1	Логическими методами.
Вариант 2	Методами теории графов.
Вариант 3	Вероятностными методами.
Вариант 4	Методами экономики.
Вариант 5	Методом экспертных оценок.
Вариант 6	В соответствии со степенями секретности.
Вариант 7	На основе права.

Контрольные вопросы

1. Какие основные компоненты оценки эффективности информационной безопасности включает в себя?
2. Какими методами можно оценить уровень защищенности информации в организации?
3. Какие факторы и угрозы следует учитывать при оценке эффективности информационной безопасности?
4. Какие показатели и метрики могут быть использованы для измерения эффективности организации информационной безопасности?
5. Какие шаги необходимо предпринять, чтобы провести успешную оценку эффективности информационной безопасности?
6. Какие рекомендации можно дать для улучшения эффективности организации информационной безопасности на основе результатов оценки?
7. Как влияют политики безопасности на эффективность информационной безопасности организации?
8. Какую роль играет обучение и осведомленность персонала в оценке эффективности информационной безопасности?
9. Как оценить уровень соответствия организации нормативным требованиям и стандартам в области информационной безопасности?
10. Какие типичные уязвимости информационной безопасности могут быть выявлены при оценке эффективности организации?
11. Как определить частоту и масштаб возможных инцидентов безопасности при оценке эффективности информационной безопасности?
12. Каким образом оценка эффективности информационной безопасности может способствовать выявлению улучшений в инфраструктуре и системах безопасности?
13. Как оценить риск и потенциальный ущерб, связанный с нарушением безопасности информации в организации?
14. Как влияют внутренние и внешние аудиты на оценку эффективности информационной безопасности?
15. Какие новые тенденции и технологии могут повлиять на оценку эффективности информационной безопасности в будущем

Практическое занятие 3. Реализация модели информационной безопасности

Цель работы. Целью работы является изучение структуры, характеристик, сильных и слабых различных политик информационной безопасности.

Модель информационной безопасности представляет собой концептуальный фреймворк, разработанный для организации и управления мерами по обеспечению безопасности информации в организации. Она определяет структуру, характеристики, политики и процедуры, необходимые для создания и поддержки безопасной информационной среды.

Цель модели информационной безопасности заключается в обеспечении конфиденциальности, целостности и доступности информации, а также защите от угроз и рисков, связанных с некорректным использованием, доступом или разглашением информации. Она помогает организации определить свои цели и требования в области безопасности информации, а также спланировать и реализовать соответствующие политики и меры.

Существует несколько способов реализации модели информационной безопасности, которые могут быть выбраны в зависимости от размера и типа организации, ее потребностей и ресурсов. Некоторые из распространенных способов включают:

1. Процессный подход: Этот подход основан на определении и документировании процессов и процедур, связанных с безопасностью информации. В рамках этого подхода организация разрабатывает и внедряет политики и процедуры по обеспечению конфиденциальности, целостности и доступности информации.

2. Стандартный подход: Организация может руководствоваться набором стандартов безопасности, таких как ISO 27001. Этот стандарт устанавливает системный подход к управлению информационной безопасностью и предлагает набор рекомендаций и контролей, необходимых для эффективной защиты информации.

3. Комплексный подход: В этом случае организация комбинирует несколько подходов и методологий для создания комплексной модели информационной безопасности. Например, она может использовать стандарты безопасности в сочетании с процессами и технологическими мерами.

Структура модели информационной безопасности часто состоит из следующих компонентов:

1. Политики безопасности: Это документированные декларации и руководства, определяющие требования и правила, которые должны соблюдаться для обеспечения безопасности информации. Они могут включать политики по управлению доступом, шифрованию, резервному копированию и другим аспектам безопасности.

2. Организационные структуры и роли: Модель информационной безопасности определяет ответственности и роли внутри организации, связанные с обеспечением безопасности информации. Это может включать назначение информационного безопасного офицера (CISO) и других ключевых лиц, а также определение команд и отделов, отвечающих за безопасность.

3. Технические меры: В модели информационной безопасности определяются технологические меры, необходимые для защиты информации. Это может включать настройку брандмауэров, систем антивирусной защиты, шифрования данных, контроля доступа и аудита систем.

4. Обучение и осведомленность персонала: Модель информационной безопасности также предусматривает обучение и повышение осведомленности персонала о правилах и процедурах безопасности информации. Это помогает улучшить соблюдение политик и защиту от основных уязвимостей, связанных с некорректным поведением персонала.

5. Аудит и управление рисками: Модель информационной безопасности включает процессы аудита и управления рисками для выявления и устранения уязвимостей и потенциальных угроз. Аудит проводится для проверки соответствия политикам безопасности, анализа инцидентов и идентификации областей, требующих улучшений.

Сильные и слабые стороны различных политик информационной безопасности зависят от их конкретной реализации и соответствия целям организации. Однако, некоторые общие примеры могут включать:

Сильные стороны:

- Четкое определение целей и требований безопасности информации.
- Адекватная классификация и защита конфиденциальных данных.
- Регулярное обновление политик и процедур безопасности.
- Проактивное обучение персонала и повышение осведомленности о безопасности.
- Систематический аудит и мониторинг безопасности информации.

Слабые стороны:

- Недостаточное финансирование и ресурсы для реализации политик безопасности информации.
- Неполное понимание угроз и рисков информационной безопасности.
- Недостаточная актуализация политик и процедур в соответствии с меняющейся угрозовой ситуацией.
- Неэффективность обучения персонала и низкая осведомленность о правилах безопасности.
- Недостаточная координация между отделами и стейкхолдерами по вопросам безопасности информации.

В целом, модель информационной безопасности и политики, определенные в ее рамках, играют важную роль в обеспечении безопасности информации в организации. Они помогают снизить риски и уязвимости, создать защитные меры и регулярно анализировать и улучшать процессы безопасности для соответствия меняющимся требованиям и угрозам информационной среды.

Пример определения требований системы безопасности:

1. Мандатная политика безопасности: Эта политика определяет строгие правила доступа к информации на основе различных уровней секретности и санкционированных пользователей. Шаги для реализации этой модели могут быть следующими: ○ Определите уровни секретности и разрешенных пользователей. Например, можно определить уровни "Секретно", "Совершенно секретно" и "Строго секретно", а также список пользователей, которым разрешен доступ к каждому уровню. ○ Создайте систему управления доступом, которая будет проверять и авторизовывать пользователя перед предоставлением доступа к определенным уровням информации. ○ Реализуйте правила ограничения доступа, чтобы гарантировать, что пользователи могут получить доступ только к информации, соответствующей их уровню секретности. ○ Реализуйте аудиторию доступа, чтобы фиксировать попытки несанкционированного доступа и нарушения политики безопасности.
2. Дискреционная политика безопасности: Эта политика дает пользователю возможность управлять доступом к своей информации.

   Шаги для реализации этой модели могут быть следующими:

   ○ Создайте систему управления доступом, позволяющую каждому пользователю определить права доступа к своей информации. ○

Реализуйте механизмы контроля доступа, чтобы проверять разрешения пользователя перед предоставлением доступа к информации. ○ Реализуйте механизмы аутентификации и авторизации, чтобы обеспечить безопасность доступа и предотвратить несанкционированный доступ к информации других пользователей.

3. Модель матрицы доступов Харрисон-Руззо-Ульмана: Эта модель использует матрицы доступов для управления правами доступа к информации на основе матрицы разрешений. Шаги для реализации этой модели могут быть следующими: ○ Создайте матрицу разрешений, которая определяет, какие пользователи имеют доступ к каким ресурсам/объектам.

   ○ Создайте матрицу доступов, которая определяет текущие права доступа для каждого пользователя и ресурса/объекта. ○ Реализуйте механизмы для обновления матрицы доступов, включая проверку разрешений и внесение изменений по запросу пользователей или администраторов системы.

4. Модель распространения прав доступа "take-grant": Эта модель определяет правила и механизмы для передачи и получения прав доступа между субъектами и объектами в системе. Шаги для реализации этой модели могут быть следующими: ○ Определите субъекты и объекты в системе и установите их права доступа по умолчанию.

○ Реализуйте механизмы для передачи прав доступа между субъектами и объектами в соответствии с определенными правилами и политиками. ○ Убедитесь, что система контролирует и записывает все операции передачи прав доступа для обеспечения прозрачности и аудита. Другие модели информационной безопасности, такие как модель системы безопасности Белла-Лападула, модель low-water-mark и модели ролевого разграничения, также могут быть реализованы соответствующим образом, в зависимости от выбранного варианта.

Задание: Написать программу, реализующую модель информационной безопасности (по вариантам).

Вариант	Модель информационной безопасности
1	Мандатная политика безопасности
2	Дискреционная политика безопасности
3	Модель матрицы доступов Харрисон-Руззо-Ульмана

4	Модель распространения прав доступа *таке-grant*
5	Модель системы безопасности белла-лападула
6	Модель *low-water-mark*
7	Модели ролевого разграничения

Каждая модель безопасности имеет свои уникальные аспекты и реализация будет зависеть от выбранной модели. Вот общий подход к реализации моделей безопасности программно:

1. Определите требования: Перед началом реализации модели безопасности определите требования и цели вашей системы безопасности. Это поможет вам определить, какая модель наиболее подходит для вашего случая.

2. Проектирование структуры данных: Реализация модели безопасности часто требует использования структур данных для хранения прав доступа, ролей, пользователей и другой информации.

3. Реализуйте механизм аутентификации и авторизации: Любая модель безопасности требует механизмов аутентификации и авторизации для проверки легитимности пользователей и их прав доступа. Реализуйте подходящие механизмы для вашей модели.

4. Создайте систему управления доступом: Реализуйте механизмы и логику, которая будет контролировать доступ пользователей к ресурсам и объектам в вашей системе. Это может включать проверку прав доступа, управление ролями и разрешениями, аудиторию доступа и другие схожие фунции.

5. Тестирование и отладка: После реализации вашей модели безопасности проведите тестирование и отладку, чтобы убедиться, что она работает должным образом и соответствует вашим требованиям.

6. Обновления и обслуживание: Поддержка безопасности является непрерывным процессом. Обновляйте и настраивайте вашу модель по мере необходимости, чтобы удовлетворять новым требованиям и угрозам безопасности.

Контрольные вопросы

1. Каковы основные шаги при реализации модели информационной безопасности в организации?
2. Какие факторы необходимо учесть при выборе подхода к реализации модели информационной безопасности?
3. Какие преимущества можно получить, используя стандартные подходы к реализации модели информационной безопасности?
4. Какую роль играют политики безопасности в успешной реализации модели информационной безопасности?
5. Какие технические меры могут быть приняты в рамках модели информационной безопасности?
6. Каким образом обучение персонала и повышение осведомленности способствуют реализации модели информационной безопасности?
7. Как организационные структуры и роли связаны с реализацией модели информационной безопасности?
8. Какие компоненты модели информационной безопасности требуют аудита и управления рисками?
9. Какие инструменты и технологии можно использовать для реализации модели информационной безопасности?
10. Каковы главные вызовы или проблемы, с которыми можно столкнуться при реализации модели информационной безопасности?
11. Какая роль управления изменениями в успешной реализации модели информационной безопасности?
12. Какие требования должны быть учтены в политиках безопасности информации для реализации конфиденциальности данных?
13. Как эффективно вовлекать и согласовывать разные заинтересованные стороны при реализации модели информационной безопасности?
14. Какие рекомендации по документированию и обновлению политик и процедур безопасности информации можно предложить?
15. Каким образом можно оценить эффективность реализации модели информационной безопасности в организации?

Практическое занятие 4. Изучение парольных систем защиты

Парольные системы защиты служат для обеспечения безопасности и ограничения доступа к различным системам и ресурсам, таким как операционные системы, веб-серверы, электронная почта, FTP, архиваторы и записи на дисках. Ниже приведено более подробное описание роли парольных систем защиты в каждом из указанных случаев:

1. Операционные системы Windows: Парольная система защиты в ОС Windows используется для ограничения доступа к пользовательским учетным записям и защиты системных ресурсов. Пользователям предоставляются уникальные идентификаторы (логины) и соответствующие им пароли, которые необходимо вводить для аутентификации и получения доступа к системе.
2. Операционные системы семейства Unix: Парольная система защиты в операционных системах Unix основана на использовании файлов паролей, которые хранят хешированные значения паролей пользователей. При входе в систему пользователю требуется ввести свой пароль, пароль затем сравнивается с хешем, сохраненным в файле паролей для проверки подлинности.
3. Веб-серверы: Для обеспечения безопасности веб-серверов требуется парольная система защиты, чтобы ограничить доступ к вебстраницам, файлам и другим ресурсам. Веб-серверы обычно используют файлы паролей или базы данных для хранения учетных записей пользователей и их паролей.
4. Электронная почта: Парольная система защиты в электронной почте позволяет пользователям защитить свои ящики от несанкционированного доступа. При настройке почтового клиента или вебинтерфейса пользователь должен указать свой логин и пароль для аутентификации на сервере электронной почты.
5. FTP: Парольная система защиты в FTP используется для ограничения доступа к файловому хранилищу на FTP-сервере. При подключении к FTP-серверу пользователю необходимо указать свой логин и пароль для аутентификации и получения доступа к файлам и папкам.
6. Архиваторы: В парольных системах защиты архиваторов парольное шифрование используется для защиты содержимого архивов от несанкционированного доступа. Пользователю при открытии зашифрованного архива необходимо ввести пароль для расшифровки и получения доступа к файлам внутри архива.

7. Записи на дисках: Парольные системы защиты для записей на дисках используются для шифрования и защиты конфиденциальных данных, хранящихся на переносных носителях, таких как USB-флешки или внешние жесткие диски. Пользователь должен ввести пароль для доступа и расшифровки защищенных данных. Это обеспечивает конфиденциальность и предотвращает несанкционированный доступ к информации на диске.

Общий принцип парольных систем защиты заключается в том, чтобы требовать от пользователя ввода уникальной комбинации логина и пароля для проверки подлинности и предоставления доступа к защищенным системам или ресурсам.

Задание: Описать парольную систему защиты (по вариантам).

Вариант 1	ОС Windows.
Вариант 2	ОС семейства Unix.
Вариант 3	Web-сервера.
Вариант 4	Электронной почты.
Вариант 5	FTP.
Вариант 6	Архиваторов.
Вариант 7	Записи на дисках.

Контрольные вопросы

1. Какие основные принципы лежат в основе парольных систем защиты?
2. Какие проблемы возникают при использовании слабых паролей?
3. Какие методы аутентификации используются в парольных системах защиты?
4. Что такое хеширование паролей и почему оно важно?
5. Какие меры безопасности рекомендуется применять при хранении паролей?
6. Что такое "политика паролей" и какие принципы она должна включать?
7. Какие средства доступны для обнаружения и предотвращения атак на парольные системы?
8. Какие методы можно использовать для создания сильных паролей?

9. Какие рекомендации по безопасности паролей при общем использовании компьютера?

10. Как можно защититься от перехвата паролей при использовании открытых Wi-Fi сетей?

11. Что такое двухфакторная аутентификация и как она повышает безопасность парольных систем?

12. Как часто следует изменять пароли и почему это важно?

13. Какие меры можно предпринять для защиты паролей от взлома методом подбора?

14. Что такое "слив" паролей и как можно защититься от этого?

15. Какие инструменты и методы используются для управления и хранения больших количеств паролей?

Практическое занятие 5. Изучение характеристик защищенности паролей

Изучение характеристик защищенности паролей - это важный аспект в области информационной безопасности. Пароли являются одним из основных способов аутентификации пользователей и защиты конфиденциальной информации. Однако, слабые пароли могут стать уязвимостью, которую злоумышленник может использовать для несанкционированного доступа к системе или к учетным записям пользователей. Поэтому, исследование и понимание характеристик защищенности паролей является критическим для разработки механизмов парольной защиты, которые будут эффективными против различных атак.

Одна из основных характеристик защищенности паролей - это их сложность. Сложность пароля определяется его длиной и использованием различных типов символов, таких как буквы верхнего и нижнего регистра, цифры и специальные символы. Более сложные пароли, состоящие из большого количества символов, обычно являются более надежными, так как для их подбора требуется больше времени и ресурсов. Однако, сложные пароли также могут быть труднее для запоминания для пользователей, поэтому существует баланс между сложностью и удобством использования пароля.

Другой важной характеристикой защищенности паролей является их уникальность. Использование одного и того же пароля для нескольких учетных записей или систем может представлять риск, так как компрометация одного пароля может привести к компрометации всех учетных записей или систем. Поэтому, рекомендуется использовать уникальные пароли для каждой учетной записи или системы.

Одной из стратегий, широко используемых для повышения уровня безопасности паролей, является требование срока действия пароля и его периодического изменения. Это помогает предотвратить использование старых, возможно скомпрометированных паролей, а также способствует повышению осведомленности пользователей о вопросах безопасности паролей.

Дополнительным средством защиты паролей является использование механизма хэширования. Хэширование пароля преобразует его в непредсказуемую строку символов, которая сохраняется в системе вместо самого пароля. При аутентификации пользователя система сравнивает хеш пароля, введенного пользователем, с сохраненным хэшем в базе данных. Это улучшает защиту паролей, так как даже если база данных системы подвергается взлому, злоумышленнику будет трудно восстановить фактический пароль из хэша.

Однако, даже при использовании сильных паролей и современных механизмов хранения паролей, существуют методы атаки, которые могут позволить злоумышленнику получить доступ к паролю. Некоторые из таких

атак включают перебор паролей, внедрение аппаратного и программного обеспечения для перехвата паролей или использование словарей с популярными паролями. Поэтому, помимо требований к сложности и уникальности паролей, важно также обеспечить механизмы обнаружения и предотвращения таких атак.

Исследование характеристик защищенности паролей также включает анализ стандартов и рекомендаций в области безопасности паролей, разработку метрик оценки сложности и уникальности паролей, а также проведение экспериментов для определения эффективности различных методов защиты паролей.

Задание 1: Определить минимальную длину пароля, алфавит которого состоит из A символов, время перебора которого было бы не меньше T лет. Скорость перебора V паролей в секунду.

Вариант	A	T	V
1	33	100	100
2	26	120	13
3	52	60	30
4	66	70	20
5	59	50	200
6	118	90	50
7	128	100	500

Ход выполнения задания:

1. Уточнение данных:
   - Значение A: определить длину алфавита пароля (например, A = 26, если используются только английские буквы в нижнем регистре). ○ Значение T: определить желаемое время в годах, для которого пароль должен быть защищен. ○ Значение V: определить скорость перебора паролей в секундах, например, V = 10000 паролей в секунду.
2. Расчет количества возможных вариантов пароля:
   - Количество вариантов пароля вычисляется по формуле:

     Варианты = A^N, где N - длина пароля. ○ Рассчитаем длину пароля N: N = log(A, Варианты).
3. Расчет времени перебора пароля:

- Время перебора пароля можно определить, поделив количество возможных вариантов пароля на скорость перебора: Время = Варианты / V. ○ Переведем время в годы: Время_лет = Время / (60 * 60 * 24 * 365), где 60 * 60 * 24 * 365 - количество секунд в году.

4. Сравнение времени перебора с желаемым временем:
   - Если Время_лет >= T, значит, пароль соответствует требованиям и минимальная длина пароля найдена. ○ Если Время_лет < T, увеличиваем длину пароля и повторяем расчеты с шага 2.
5. Вывод результата:
   - Выводим найденную минимальную длину пароля, алфавит которого состоит из A символов, время перебора которого составляет не меньше T лет.

Задание 2: Освоить программу «ViPNet Генератор паролей». Оценить стойкость паролей, сгенерированных данной программой.

Ход выполнения работы:

1. Ознакомление с программой "ViPNet Генератор паролей":
   - Изучите документацию и функциональность программы "ViPNet Генератор паролей". ○ Убедитесь, что программа предлагает создавать пароли с высокой стойкостью.
2. Генерация паролей:
   - Используйте программу "ViPNet Генератор паролей" для создания нескольких паролей.
   - Укажите необходимую длину и сложность пароля в соответствии с требованиями безопасности.
3. Оценка стойкости паролей:
   - Рассмотрите каждый сгенерированный пароль и проанализируйте его стойкость. Проанализируйте каждый сгенерированный пароль, примените эти критерии и оцените стойкость каждого пароля в соответствии с ними. Чем больше критериев удовлетворяет пароль, тем он считается стойким.

     Сравните полученную стойкость с общепринятыми стандартами обеспечения безопасности паролей, чтобы определить,

соответствуют ли сгенерированные пароли требованиям безопасности.

- Учитывайте следующие факторы:
  - Длина пароля: чем длиннее пароль, тем сложнее его подобрать методом перебора. Общепринятая рекомендация - использовать пароли длиной не менее 8-10 символов. Пароли, состоящие из более 12 символов, считаются более стойким
  - Разнообразие символов: пароли, состоящие из смешанных символов (цифры, буквы разного регистра, специальные символы), являются более стойкими.
  - Отсутствие легко угадываемых шаблонов: пароли, не содержащие простые слова, имеют высокую степень стойкости. Широко известные или персональные информации (например, даты рождения, имена) тоже следует избегать.
  - Непредсказуемость: пароли, генерируемые случайным образом, сложнее угадать, чем пароли, основанные на паттернах или персональной информации.

4. Сравнение со стандартными требованиями:
   - Сопоставьте стойкость сгенерированных паролей с общепринятыми стандартами безопасности паролей.
   - Убедитесь, что сгенерированные пароли соответствуют минимальным требованиям к длине, сложности и обновлению паролей.
5. Вывод результата:
   - Сделайте вывод о стойкости паролей, сгенерированных с помощью программы "ViPNet Генератор паролей". ○ Опишите преимущества и недостатки программы в контексте создания безопасных паролей.

Контрольные вопросы

1. Каковы основные критерии стойкости паролей?
2. Какова рекомендуемая минимальная длина пароля для обеспечения безопасности?
3. Какие типы символов следует использовать в паролях для повышения их стойкости?

4. Почему важно избегать использования обычных слов и фраз в паролях?

5. Какие риски связаны с использованием персональной информации (например, даты рождения или имен) в паролях?

6. Какой роль длины пароля в защите от метода перебора?

7. Почему генерация паролей случайным образом способствует их стойкости?

8. Какие типы алгоритмов можно использовать для генерации непредсказуемых паролей?

9. Какие шаблоны паролей следует избегать?

10. Какой инструмент можно использовать для оценки стойкости сгенерированных паролей?

11. Какие шаги можно предпринять для обеспечения безопасности паролей в онлайн-сервисах?

12. Почему рекомендуется использовать уникальные пароли для каждого сервиса или аккаунта?

13. Какой метод защиты паролей является наиболее надежным: хэширование или шифрование?

14. Каковы основные методы взлома паролей и как защититься от них?

15. Какие меры предпринимаются для обеспечения безопасности хранилища паролей на сервере?

Практическое занятие 6. Целостность данных. Модель Кларка-Вилсона.

Цель работы. Целью работы является закрепление полученного теоретического материала по моделям целостности и применение на практике положений модели целостности Кларка-Вилсона к вычислительным системам.

Основные положения модели целостности Кларка-Вилсона

Модель Кларка-Вилсона появилась в результате проведенного авторами анализа реально применяемых методов обеспечения целостности документооборота в коммерческих компаниях. В отличие от моделей Биба и Белла-ЛаПадулы, она изначально ориентирована на нужды коммерческих заказчиков, и, по мнению авторов, более адекватна их требованиям, чем предложенная ранее коммерческая интерпретация модели целостности на основе решеток. Основные понятия рассматриваемой модели — это корректность транзакций и разграничение функциональных обязанностей.

Модель задает правила функционирования компьютерной системы и определяет две категории объектов данных и два класса операций над ними. Все содержащиеся в системе данные подразделяются на контролируемые и неконтролируемые элементы данных (constrained data items - CDI и unconstrained data items – UDI соответственно). Целостность первых обеспечивается моделью Кларка-Вилсона. Последние содержат информацию, целостность которой в рамках данной модели не контролируется (этим и объясняется выбор терминологии). Далее, модель вводит два класса операций над элементами данных: процедуры контроля целостности (integrity verification procedures - IVP) и процедуры преобразования (transformation procedures - TP).

Первые из них обеспечивают проверку целостности контролируемых элементов данных (CDI), вторые изменяют состав множества всех CDI (например, преобразуя элементы UDI в CDI). Так же модель содержит девять правил, определяющих взаимоотношения элементов данных и процедур в процессе функционирования системы.

Правило C1. Множество всех процедур контроля целостности (IVP) должно содержать процедуры контроля целостности любого элемента данных из множества всех CDI.

Правило C2. Все процедуры преобразования (TP) должны быть реализованы корректно в том смысле, что не должны нарушать целостность обрабатываемых ими CDI. Кроме того, с каждой процедурой преобразования должен быть связан список элементов CDI, которые допустимо обрабатывать данной процедурой. Такая связь устанавливается администратором безопасности.

Правило E1. Система должна контролировать допустимость применения TP к элементам CDI в соответствии со списками, указанными в правиле C2.

Правило E2. Система должна поддерживать список разрешенных конкретным пользователям процедур преобразования с указанием допустимого для каждой TP и данного пользователя набора обрабатываемых элементов CDI.

Правило C3. Список, определенный правилом C2, должен отвечать требованию разграничения функциональных обязанностей.

Правило E3. Система должна аутентифицировать всех пользователей, пытающихся выполнить какую-либо процедуру преобразования.

Правило C4. Каждая TP должна записывать в журнал регистрации информацию, достаточную для восстановления полной картины каждого применения этой TP. Журнал регистрации — это специальный элемент CDI, предназначенный только для добавления в него информации.

Правило C5. Любая TP, которая обрабатывает элемент UDI, должна выполнять только корректные преобразования этого элемента, в результате которых UDI превращается в CDI.

Правило E4. Только специально уполномоченное лицо может изменять списки, определенные в правилах C2 и E2. Это лицо не имеет права выполнять какие-либо действия, если оно уполномочено изменять регламентирующие эти действия списки.

Публикация описания модели Кларка-Вилсона вызвала широкий отклик среди исследователей, занимающихся проблемой контроля целостности. В ряде научных статей рассматриваются практические аспекты применения модели, предложены некоторые ее расширения и способы интеграции с другими моделями безопасности.

Роль каждого из девяти правил модели Кларка-Вилсона в обеспечении целостности информации можно пояснить, показав, каким из теоретических принципов политики контроля целостности отвечает данное правило:

1. корректность транзакций;
2. аутентификация пользователей;
3. минимизация привилегий;
4. разграничение функциональных обязанностей; 5. аудит произошедших событий;
6. объективный контроль.

Соответствие правил модели Кларка-Вилсона перечисленным принципам показано в таблице. Как видно из таблицы, принципы 1 (корректность транзакций) и 4 (разграничение функциональных обязанностей) реализуются большинством правил, что соответствует основной идее модели.

Правило модели КларкаВилсона	Принципы политики контроля целостности, реализуемые правилом

C1	1,6
C2	1
E1	3,4
E2	1,2,3,4
C3	4
E3	2
C4	5
C5	1
E4	4

Пример применения модели

В качестве примера рассмотрим систему форумовFORUM.TOMSK.RU 🎬

CDI – контролируемые элементы данных: логин и пароль.

- UDI – неконтролируемые элементы данных: вводимые данные через интерфейс пользователя.
- IVP – процедуры контроля целостности проверяют соответствие введенных пользователем логина и пароля с зарегистрированным логином и паролем (которые хранятся в базе данных системы). Процедуры проверки корректности данных ввода и хранимой информации.
- TP – процедуры преобразования: процедуры преобразования изменяют состав множества всех контролируемых элементов данных путем редактирования, создания, ввода, удаления и т.п. В частности – редактирование писем и их распределение по папкам.

C1: все процедуры преобразования данных соответствуют определенному пользователю, что в свою очередь обеспечивает конфиденциальность хранимой пользователем информации.

C2: все процедуры преобразования реализованы таким образом, чтобы не изменять системные файлы и папки. Для процедуры преобразования «удаление» установлен список тех данных, на которые эта процедура не сможет воздействовать и сможет влиять только в рамках тех прав, которые были установлены для пользователя с конкретными логином и паролем (пользователь не может удалить информацию о другом сеансе).

E1: должна обеспечиваться на уровне программного средства, должен быть установлен контроль доступа в соответствии со списками, которые были установлены в правиле C2, о применении процедур преобразования к соответствующим CDI.

E2: соответствие логина и пароля с доступом к определенной информации, отождествление пользователей с предназначенным для них списком прав. Четкое разграничение функциональных возможностей и обязанностей для каждого пользователя системы.

C3: администратор имеет право изменять логин и пароль, а также права доступа к информации, но не может менять данные в базе.

E3: при попытке пользователя совершить какую-либо операцию, каждый раз производиться аутентификация пользователя (более того, аутентификация пользователя происходит каждые 10 мин).

C4: Каждая операция, совершаемая пользователем, записывается в журнал историй.

C5: Сначала производиться поиск логина , далее соответствующего пароля в базе, а затем определяются права доступа к информации.

E4: должно быть определено уполномоченное лицо – администратор системы. Он определяет права и контролирует работу системы.

Задание к работе

Необходимо для заданной информационной системы определить:

- CDI – контролируемые элементы данных.
- UDI – неконтролируемые элементы данных.
- IVP – процедуры контроля целостности.
- TP – процедуры преобразования.

Выделить объект(ы), в которых хранятся списки, определенные в правилах C2 и E2, а также хранится журнал регистрации событий. Указать кто может изменять списки, определенные с правилах C2 и E2.

Создать правила, которые соответствовали ли бы девяти правилам, определяющим взаимоотношения элементов данных и процедур в процессе функционирования системы. Провести проверку целостности системы с использованием теоретических принципов политики контроля целостности.

Вариант 1	www-сервер
Вариант 2	ftp-сервер
Вариант 3	Почтовая база данных

Вариант 4	База данных Microsoft Access
Вариант 5	Операционная система
Вариант 6	Жесткий диск
Вариант 7	Мобильный телефон

Контрольные вопросы

1. Что такое целостность данных и почему она является важным аспектом информационной безопасности?
2. Какая роль у модели Кларка-Вилсона в обеспечении целостности данных?
3. Какие основные принципы лежат в основе модели Кларка-Вилсона?
4. Каковы основные компоненты модели Кларка-Вилсона?
5. Что означает понятие "целостность данных в широком смысле" в контексте модели Кларка-Вилсона?
6. Как модель Кларка-Вилсона помогает в предотвращении несанкционированного доступа к данным?
7. Как организации могут выполнять аутентификацию данных с использованием модели Кларка-Вилсона?
8. Какие виды угроз могут негативно повлиять на целостность данных?
9. Какая роль у криптографических хэш-функций в обеспечении целостности данных по модели Кларка-Вилсона?
10. Какие техники используются для обнаружения и восстановления поврежденных данных согласно модели Кларка-Вилсона?
11. Каким образом модель Кларка-Вилсона связана с резервным копированием данных?
12. Как модель Кларка-Вилсона помогает в предотвращении внутренних и маловероятных ошибок в данных?
13. Какие методы обеспечения целостности данных используются на уровне операционной системы?
14. Что такое проверка целостности в режиме реального времени и как она работает в рамках модели Кларка-Вилсона?
15. Какие лучшие практики могут быть применены для обеспечения целостности данных в соответствии с моделью Кларка-Вилсона?

СПИСОК ЛИТЕРАТУРЫ

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. – URL: https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 22.05.2023). - Режим доступа: по подписке. – Текст: электронный. 2. Основы администрирования информационных систем: учебное пособие / Д. О. Бобынцев, А. Л. Марухленко, Л. О. Марухленко [и др.]. – Москва; Берлин : Директ-Медиа, 2021. – 201 с. – URL: https://biblioclub.ru/index.php?page=book&id=598955. – Режим доступа: по подписке. – Текст: электронный.

3. Марухленко, А. Л. Разработка защищённых интерфейсов Webприложений : учебное пособие / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов. – Москва; Берлин: Директ-Медиа, 2021. – 175 с. – URL: https://biblioclub.ru/index.php?page=book&id=599050. – Режим доступа: по подписке. – Текст: электронный.

4. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю. Н. Загинайлов. – Москва; Берлин: Директ-Медиа, 2015. – 255 с. – URL: https://biblioclub.ru/index.php?page=book&id=276557. – Режим доступа: по подписке. – Текст: электронный.

5. Системы защиты информации в ведущих зарубежных странах: учебное пособие / В. И. Аверченков, М. Ю. Рытов, Г. В. Кондрашин, М. В. Рудановский; науч. ред. В. И. Аверченков. – 5-е изд., стер. – Москва: ФЛИНТА, 2021. – 224 с. – URL: https://biblioclub.ru/index.php?page=book&id=93351. – Режим доступа: по подписке. – Текст: электронный.