Методические рекомендации к практическому занятию №4

С.А. Краснов

НАСТРОЙКА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД В ОС СН «ASTRA LINUX»

# МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К ПРАКТИЧЕСКОМУ ЗАНЯТИЮ № 4

**НАСТРОЙКА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ОС СН «ASTRA LINUX»**

***Цель работы.*** Получить практические навыки настройки СЗИ НСД в ОС СН «Astra Linux».

***Теоретические сведения.*** ОС СН предназначена для построения автоматизированных систем в защищенном исполнении, обрабатывающих информацию, содержащую сведения, составляющие государственную тайну с грифом не выше «совершенно секретно».

Основная задача, решаемая ОС в процессе своего функционирования – обеспечение интерфейса для доступа ПО к устройствам вычислительной системы посредством управления устройствами, вычислительными процессами, а также эффективное распределение вычислительных ресурсов между вычислительными процессами в соответствии с требованиями руководящих документов по обеспечению защиты информации, содержащей сведения, составляющие государственную тайну с грифом не выше «совершенно секретно».

Для решения основной задачи функционирования ОС она декомпозируется на следующие основные классы задач:

**Идентификация и аутентификация пользователей.** Решение задачи идентификации и аутентификации пользователей в ОС основывается на использовании механизма PAM, который представляет собой набор разделяемых библиотек (модулей), с помощью которых администратор может организовывать процедуру аутентификации (подтверждение подлинности) пользователей прикладными программами. Каждый модуль реализует собственный механизм аутентификации. Изменяя набор и порядок следования модулей, можно построить сценарий аутентификации. Подобный подход позволяет изменять процедуру аутентификации без изменения исходного кода и повторного компилирования PAM. Сценарии описываются в конфигурационных файлах.

В ОС реализована возможность хранения аутентификационной информации пользователей, полученной с использованием хэш-функции по ГОСТ Р 34.11-94 и по ГОСТ Р 34.11-2012.

**Дискреционное разграничение доступа.** В ОС механизм дискреционного разграничения доступа обеспечивает проверку дискреционных ПРД, формируемых в виде базовых ПРД ОС семейства Linux, формируемых в виде идентификаторов субъектов (идентификатор пользователя (UID) и идентификатор группы (GID), имеющих доступ к объекту (чтение, запись, исполнение). Кроме того, для формирования дискреционных ПРД в ОС используются списки контроля доступа (ACL) и механизм системных привилегий ОС семейства Linux.

**Мандатное разграничение доступа.** Решение задачи мандатного разграничения доступа процессов к ресурсам основан на реализации соответствующего механизма в ядре ОС. При этом, принятие решения о запрете или разрешении доступа субъекта к объекту принимается на основе типа операции (чтение, запись, исполнение), мандатного контекста безопасности, связанного с каждым субъектом, и мандатной метки, связанной с объектом.

Правила приятия решения могут быть записаны следующим образом. Пусть контекст безопасности субъекта содержит уровень L0 и категории C0, а мандатная метка объекта содержит уровень L1 и категории C1. В ОС определены следующие операции сравнения уровней и категорий:

- уровень L0 меньше уровня L1 (L0<L1), если численное значение L0 меньше численного значения L1;

- уровень L0 равен уровню L1 (L0=L1), если численные значения L0 и L1 совпадают;

- категории C0 меньше категорий C1 (C0<C1), если все биты набора C0 являются подмножеством набора бит C1;

- категории C0 равны категориям C1 (C0=C1), если значения C0 и C1 совпадают;

Таким образом, в механизме мандатного разграничения доступа действуют следующие правила:

- операция записи разрешена, если L0=L1 и C0=C1;

- операция чтения разрешена, если L0>=L1 и C0>=C1;

- операция исполнения разрешена, если L0>=L1 и C0>=C1.

В остальных случаях анализируются полномочия и тип мандатной метки. Тип метки может использоваться для того, чтобы изменять ее эффектные действия. Ненулевой тип метки может быть установлен только привилегированным процессом.

**Изоляция адресных пространств процессов.** Решение задачи изоляции адресных пространств процессов основано на архитектуре ядра ОС, которое обеспечивает для каждого процесса в системе собственное изолированное адресное пространство. Данный механизм изоляции основан на страничном механизме защиты памяти, а также механизме трансляции виртуального адреса в физический, поддерживаемый модулем управления памятью. Одни и те же виртуальные адреса (с которыми и работает процессор) преобразуются в разные физические для разных адресных пространств. Процесс не может несанкционированным образом получить доступ к пространству другого процесса, так как непривилегированный пользовательский процесс лишен возможности работать с физической памятью на прямую.

Механизм разделяемой памяти является санкционированным способом получить нескольким процессам доступ к одному и тому же участку памяти и находится под контролем дискреционных и мандатных ПРД.

Адресное пространство ядра защищено от прямого воздействия пользовательских процессов с использованием механизма страничной защиты. Страницы пространства ядра являются привилегированными и доступ к ним из непривилегированного кода вызывает исключение процессора, которое обрабатывается корректным образом ядром ОС. Единственным санкционированным способом доступа к ядру ОС из пользовательской программы является механизм системных вызовов, который гарантирует возможность выполнения пользователем только санкционированных действий.

**Регистрация событий.** В ОС реализована расширенная подсистема протоколирования, осуществляющая регистрацию событий в двоичные файлы с использованием сервиса parlogd.

В библиотеках подсистемы безопасности PARSEC реализован программный интерфейс для протоколирования событий с использованием расширенной подсистемы протоколирования.

**Очистка оперативной и внешней памяти.** Решение задачи очистки ОП основано на архитектуре ядра ОС, которое гарантирует, что обычный непривилегированный процесс не получит данные чужого процесса, если это явно не разрешено ПРД. Это означает, что средства взаимодействия между процессами контролируются с помощью ПРД, и процесс не может получить неочищенную память (как оперативную, так и дисковую).

Решение задачи очистки памяти на внешних носителях основано на реализации механизма, который очищает неиспользуемые блоки ФС непосредственно при их освобождении. Работа названного механизма снижает скорость выполнения операция удаления и усечения размера файла. Механизм является настраиваемым и позволяет обеспечить работу ФС ОС в одном из следующих режимов:

- данные любых удаляемых/урезаемых файлов пределах ФС предварительно очищаются маскирующей последовательностью;

- данные ФС освобождаются обычным образом (без предварительного маскирования).

Режим работы ФС может быть выбран администратором ОС и задан в виде параметра монтирования ФС.

**Контроль целостности.** Решение задач контроля целостности основано на использовании библиотеки libgost, в которой реализованы функции хэширования в соответствии с ГОСТ Р 34.11- 94, ГОСТ Р 34.11-2012 с длиной хэш-кода 256 бит и ГОСТ Р 34.11-2012 с длиной хэш-кода 512 бит. Данная библиотека используется в средствах контроля целостности дистрибутива и средствах контроля целостности ФС.

Контроль целостности дистрибутива обеспечивается методом расчета его контрольной суммы и сравнения полученного значения с эталонным значением контрольной суммы.

Контроль целостности ОС, прикладного ПО и СЗИ обеспечивается набором программных средств, который предоставляет возможность периодического (с использованием системного планировщика заданий cron) вычисления контрольных сумм файлов и соответствующих им атрибутов с последующим сравнением вычисленных значений с эталонными. В указанном наборе программных средств реализовано использование библиотеки libgost и контроль целостности связанных с файлами атрибутов расширенной подсистемы безопасности PARSEC (мандатных атрибутов и атрибутов расширенной подсистемы протоколирования).

**Создание замкнутой программной среды.** Средства создания замкнутой программной среды предоставляют возможность внедрения цифровой подписи в исполняемые файлы формата ELF, входящие в состав устанавливаемого СПО и в расширенные атрибуты файловой системы.

Механизм контроля целостности исполняемых файлов и разделяемых библиотек формата ELF при запуске программы на выполнение реализован в модуле ядра ОС digsig\_verif, который̆ является не выгружаемым модулем ядра Linux, и может функционировать в одном из следующих режимов:

1) исполняемым файлам и разделяемым библиотекам с неверной̆ ЭЦП, а также без ЭЦП загрузка на исполнение запрещается (штатный̆ режим функционирования);

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

3) ЭЦП при загрузке исполняемых файлов и разделяемых библиотек не проверяется (отладочный̆ режим для тестирования СПО).

Механизм контроля целостности файлов при их открытии на основе ЭЦП в расширенных атрибутах файловой̆ системы также реализован в модуле ядра ОС digsig\_verif и может функционировать в одном из следующих режимов:

1) запрещается открытие файлов, поставленных на контроль файлов, с неверной̆ ЭЦП или без ЭЦП;

2) открытие файлов, поставленных на контроль файлов, с неверной̆ ЭЦП или без ЭЦП разрешается, при этом выдается сообщение об ошибке проверки ЭЦП (режим для проверки ЭЦП в расширенных атрибутах файловой̆ системы);

3) ЭЦП при загрузке исполняемых файлов и разделяемых библиотек не проверяется.

***Постановка задачи.*** Выполнить все шаги работы, необходимые для осуществления настройки СЗИ НСД. Результаты зафиксировать в отчете.

***Последовательность действий.***

Шаг 1. Создать пользователей системы (субъект доступа).

Шаг 2. Выполнить настройки идентификации и аутентификации.

Шаг 3. Создать защищаемые каталоги (объект доступа).

Шаг 4. Установить объектам доступа права разграничения доступа по отношению к субъектам доступа.

Шаг 5. Выполнить настройку очистки остаточной информации.

Шаг 6. Выполнить настройку регистрации событий для объектов доступа.

Шаг 7. Выполнить настройку контроля целостности файловой системы и программно-аппаратной среды.

Шаг 8. Выполнить настройку внешних носителей информации.

Шаг 9. Всю информацию собрать в единый документ, являющийся отчетом о настройке СЗИ НСД.

Для решения задачи в приложение В представлен пример настройки СЗИ. Более конкретная информация представлена в источниках, указанных в списке рекомендуемой литературы [3, 5].

**ПРИЛОЖЕНИЕ В**

**Пример настройки ОС СН «Astra Linux»**

**Создание пользователя системы.** Необходимо выполнить следующие действия:

- открыть «Управление политикой безопасности»;

- перейти по вкладке «Пользователи» (рис. 24);

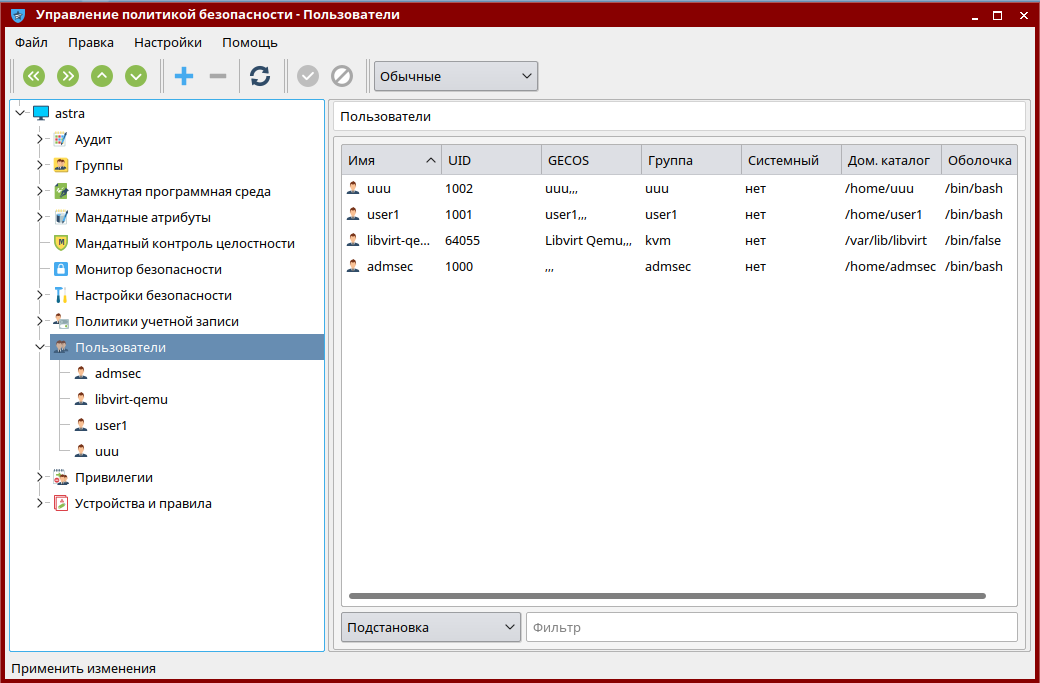


Рисунок 24. Окно учетных записей

- нажать кнопку «Создать новый элемент»;

- ввести имя пользователя;

- выбрать необходимые группы для пользователя (рис. 25);

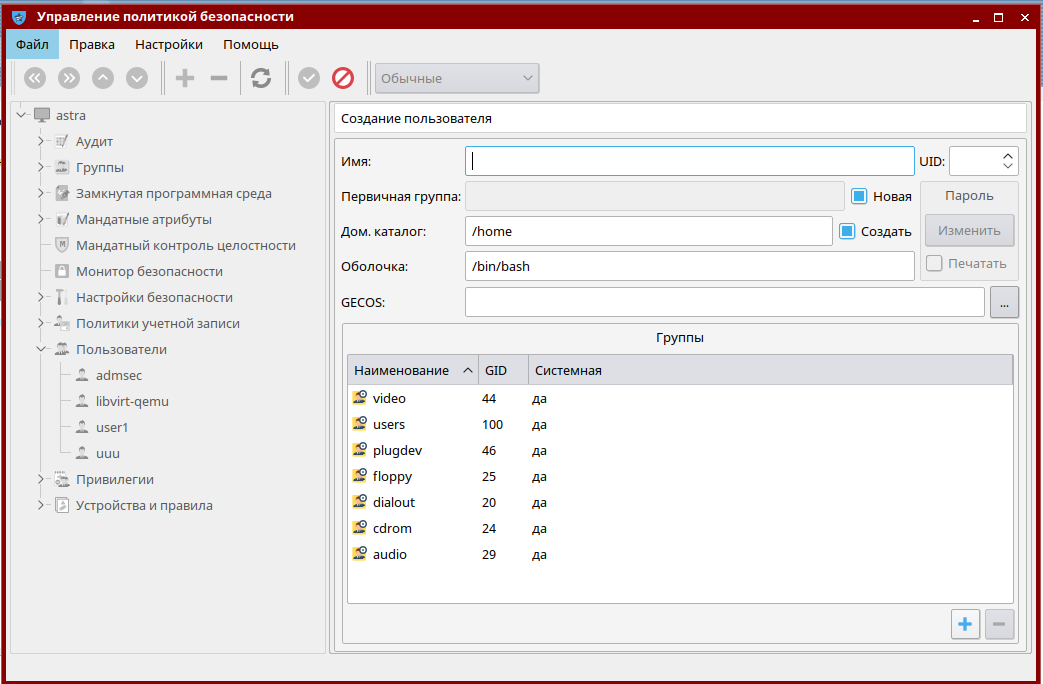


Рисунок 25. Окно создания учетной записи

- нажать кнопку «Применить изменения»;

- в форме «Пароль» нажать кнопку «Изменить» и добавить новый пароль для пользователя;

- выполнить необходимые настройки во вкладках «Блокировка», «Аудит», «МРД», «Срок действия» (рис. 26).

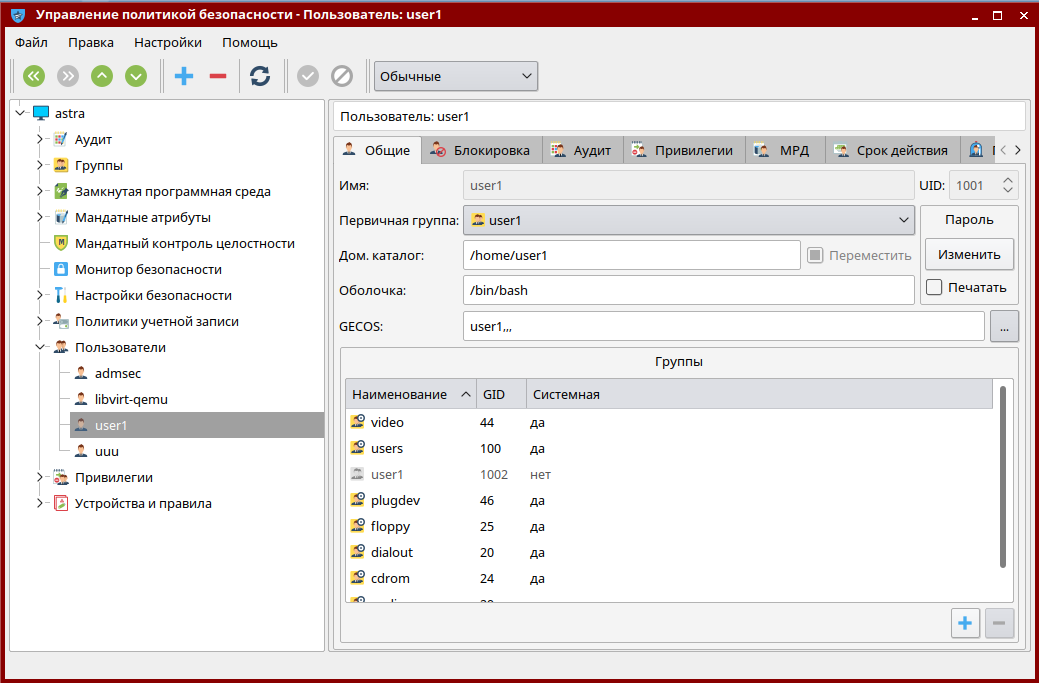


Рисунок 26. Окно настройки учетной записи

**Настройка идентификации и аутентификации.** Необходимо выполнить следующие действия:

- открыть «Управление политикой безопасности»;

- перейти по вкладке «Политики учетной записи» (рис. 27);

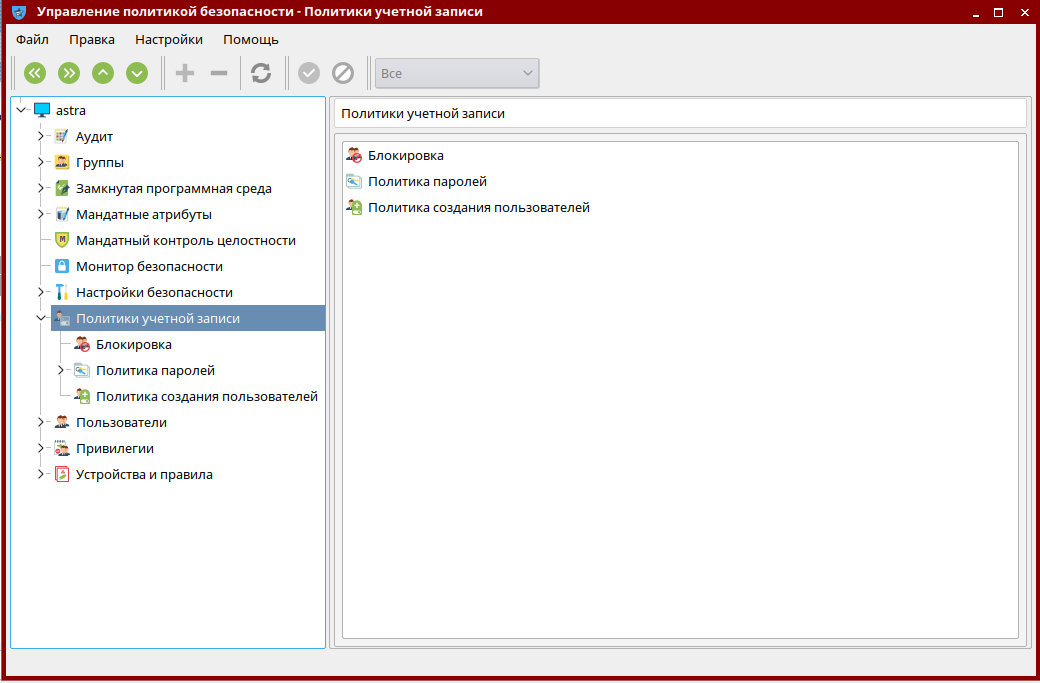
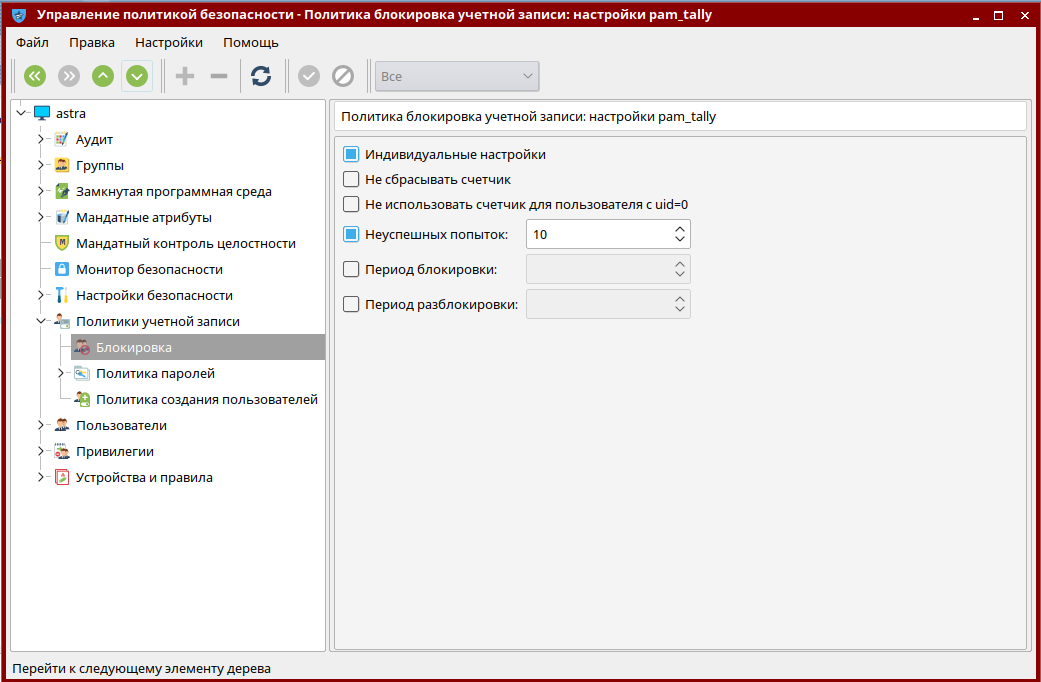


Рисунок 27. Окно настройки политик учетной записи

- выполнить необходимые настройки во вкладках «Блокировка», «Политика паролей» (рис. 28).



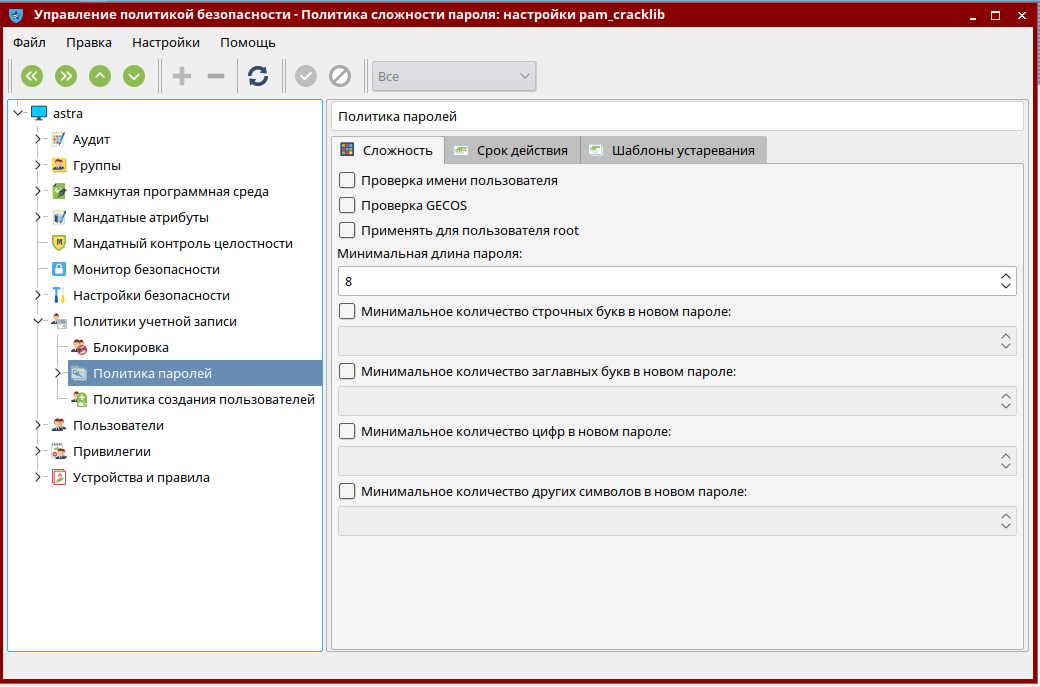


Рисунок 28. Окна настройки блокировки и политики паролей учетных записей

**Установка прав разграничения доступа.** Необходимо выполнить следующие действия:

- нажать сочетание клавиш «Win+R» и в появившемся окне ввести команду «sudo fly-fm» (рис. 29);

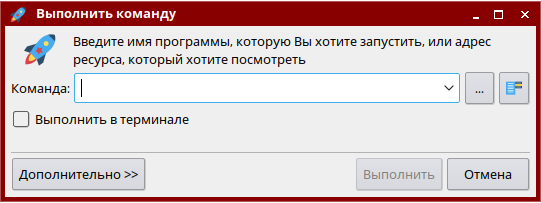


Рисунок 29. Окно выполнения команд

- откроется «Менеджер файлов» (рис. 30);

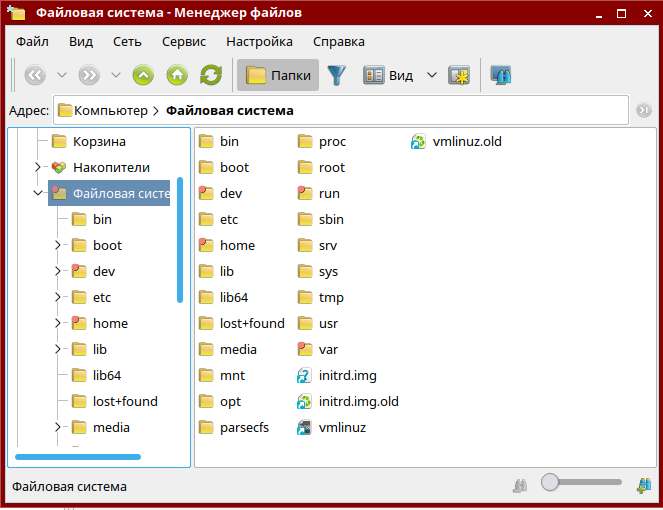


Рисунок 30. Окно менеджера файлов

- на выбранном объекте вызвать контекстное меню и нажать кнопку «Свойства»;

- открыть вкладку «Дискреционные атрибуты» (рис. 31);

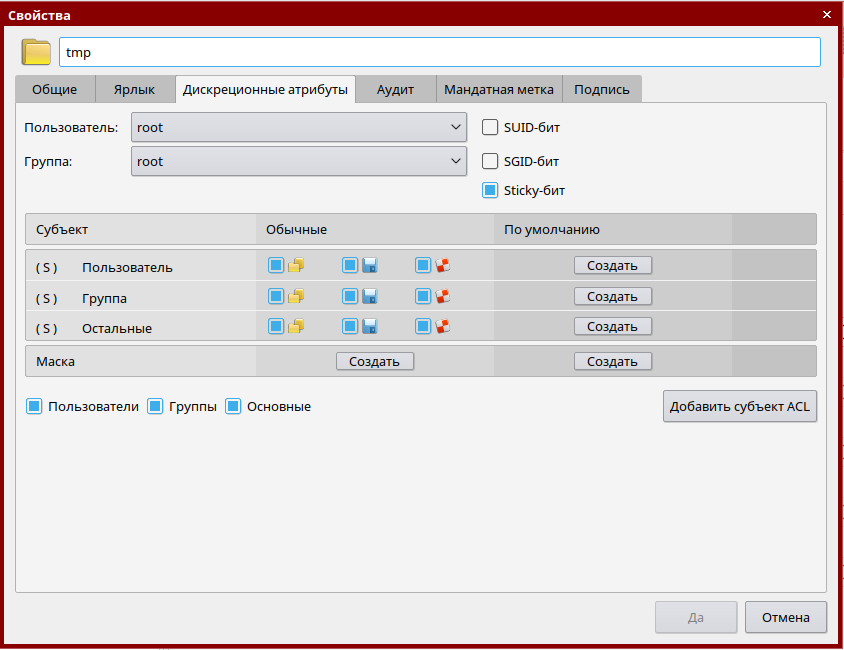


Рисунок 31. Окно настройки дискреционных прав разграничения доступа

- выполнить необходимые настройки разграничения доступа и нажать кнопку «Да».

**Настройка очистки остаточной информации.** Необходимо выполнить следующие действия:

- открыть «Управление политикой безопасности»;

- перейти по вкладке «Настройки безопасности», «Параметры очистки памяти» (рис. 32);

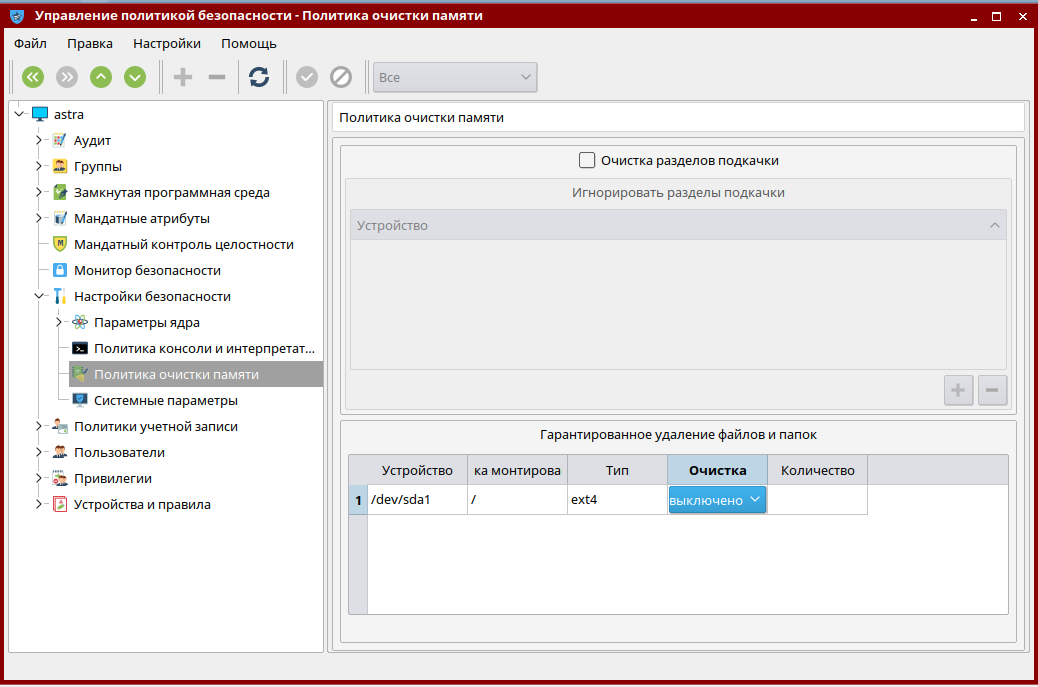


Рисунок 32. Окно настройки политики очистки памяти

- включить «Очистка разделов подкачки»;

- в форме «Гарантированное удаление файлов и папок» для нужного устройства выбрать необходимый тип очистки и количество затираний;

- нажать «Применить изменения».

**Настройка регистрации событий.** Необходимо выполнить следующие действия:

- настройка регистрации событий пользователя выполнялась при создании пользователей;

- для настройки регистрации событий по отношению к объектам доступа нажать сочетание клавиш «Win+R» и в появившемся окне ввести команду «sudo fly-fm» (рис. 33);

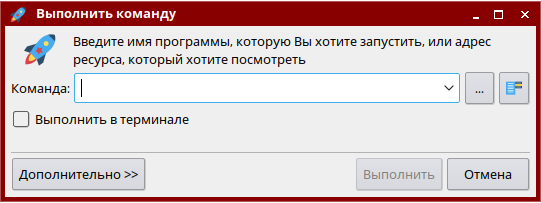


Рисунок 33. Окно выполнения команд

- откроется «Менеджер файлов» (рис. 34);

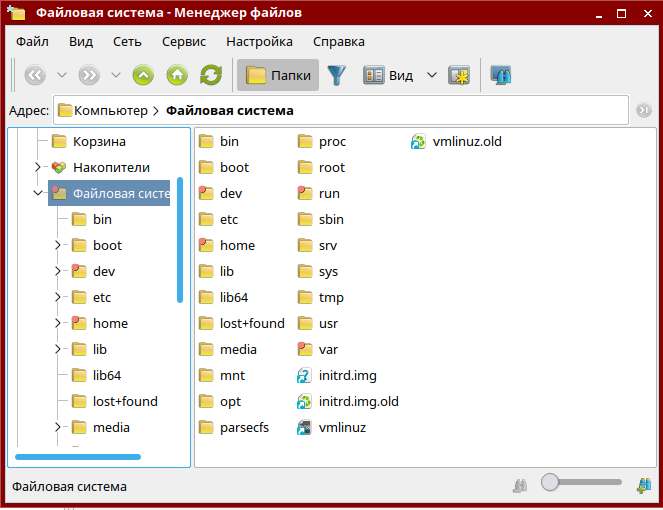


Рисунок 34. Окно менеджера файлов

- на выбранном объекте вызвать контекстное меню и нажать кнопку «Свойства»;

- открыть вкладку «Аудит» и нажать кнопку «Добавить элемент аудита» (рис. 35);

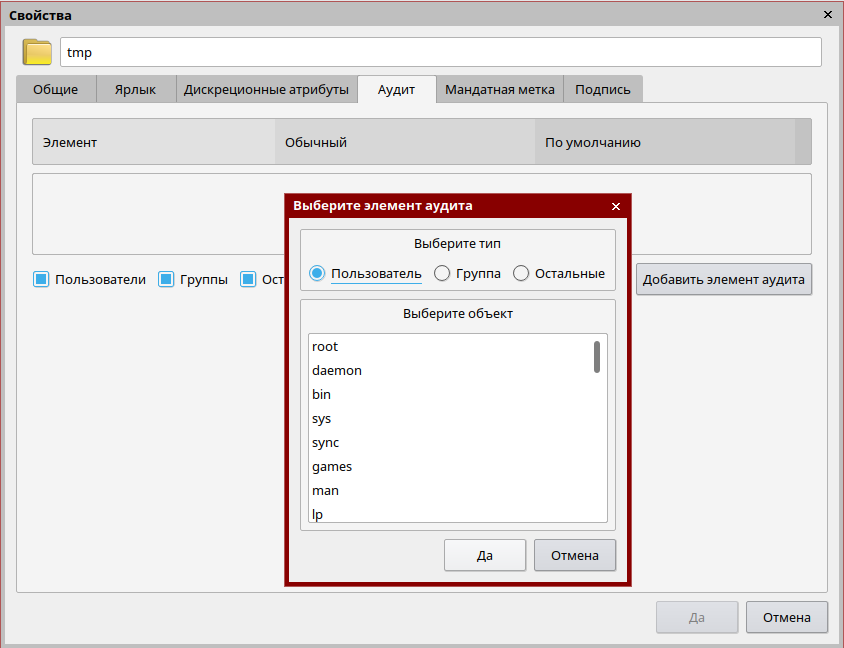


Рисунок 35. Окно выбора элемента аудита

- выбрать необходимых субъектов доступа, по отношению к которым настраивается аудит;

- добавить необходимые события аудита для выбранных субъектов доступа и нажать кнопку «Да» (рис. 36).

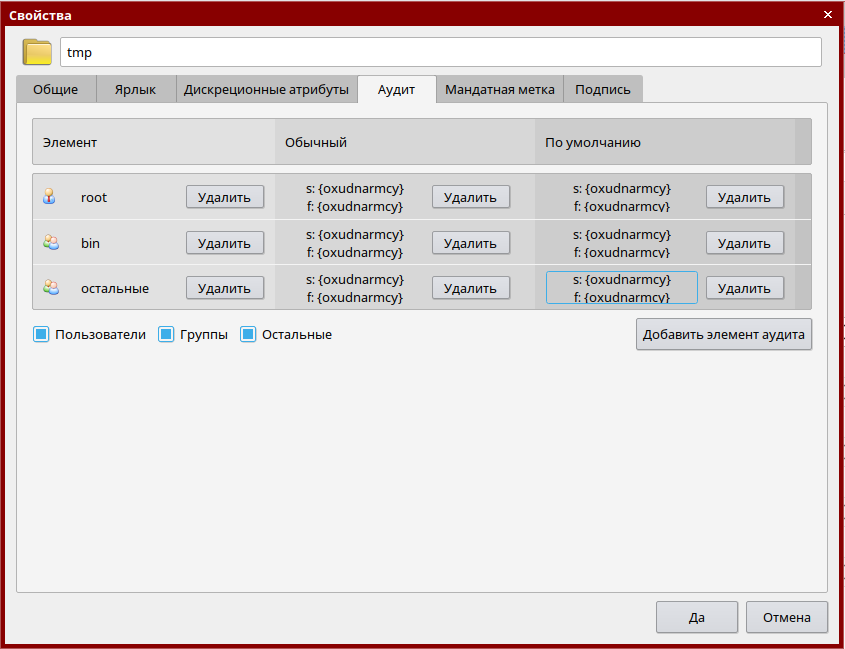


Рисунок 36. Окно настройки аудита

**Настройка контроля целостности файловой системы и программно-аппаратной среды.** Необходимо выполнить следующие действия:

- Изменить в файле «/etc/cron.daily/afick\_cron» параметры:

LOGFILE="/dev/null"

ERRORLOG="/dev/null"

nice -n $NICE $AFICK -c $CONFFILE -k > $LOGFILE 2>$ERRORLOG

- Изменить в файле «/etc/afick.conf» параметры:

history := /var/log/afick/afick.log

#archive := /var/lib/afick/archive

/boot md5

/lib/modules md5

/etc/security md5

/etc/pam.d md5

/lib/x86\_64-linux-gnu/security md5

/lib/security md5

/sbin md5

/etc/fstab md5

/usr/sbin md5

- в «Терминал Fly» выполнить следующие команды:

sudo touch /etc/init.d/afick.sh

sudo chmod 755 /etc/init.d/afick.sh

- в файл «/etc/init.d/afick.sh» необходимо вписать:

#!/bin/sh

### BEGIN INIT INFO

# Provides: afick

# Required-Start: $local\_fs

# Required-Stop: $local\_fs

# Default-Start: 2 3 4 5

# Default-Stop: 0 1 6

# Short-Description: Контроль целостности при старте системы

# Description: Контроль целостности при старте системы

### END INIT INFO

PATH=/sbin:/bin:/usr/sbin:/usr/bin

. /lib/lsb/init-functions

case $1 in

start)

log\_daemon\_msg "Starting integrity check" "afick"

log\_end\_msg 0

/usr/bin/afick -c /etc/afick.conf -k 2>&1 > /dev/null

status=$?

log\_daemon\_msg "Integrity check results" "afick"

log\_end\_msg $status

if [ $status -ne "0" ];

then

sleep 2

fi

;;

\*)

echo "Для использования данного скрипта необходимо запустить его с параметром start. Например: afick.sh start"

;;

esac

- в «Терминал Fly» выполнить следующие команды:

sudo afick -i

sudo update-rc.d afick.sh defaults

**Настройка прав разграничения доступа для внешних носителей информации.** Необходимо выполнить следующие действия:

- открыть «Управление политикой безопасности»;

- перейти по вкладке «Устройства и правила», «Устройства» (рис. 37);

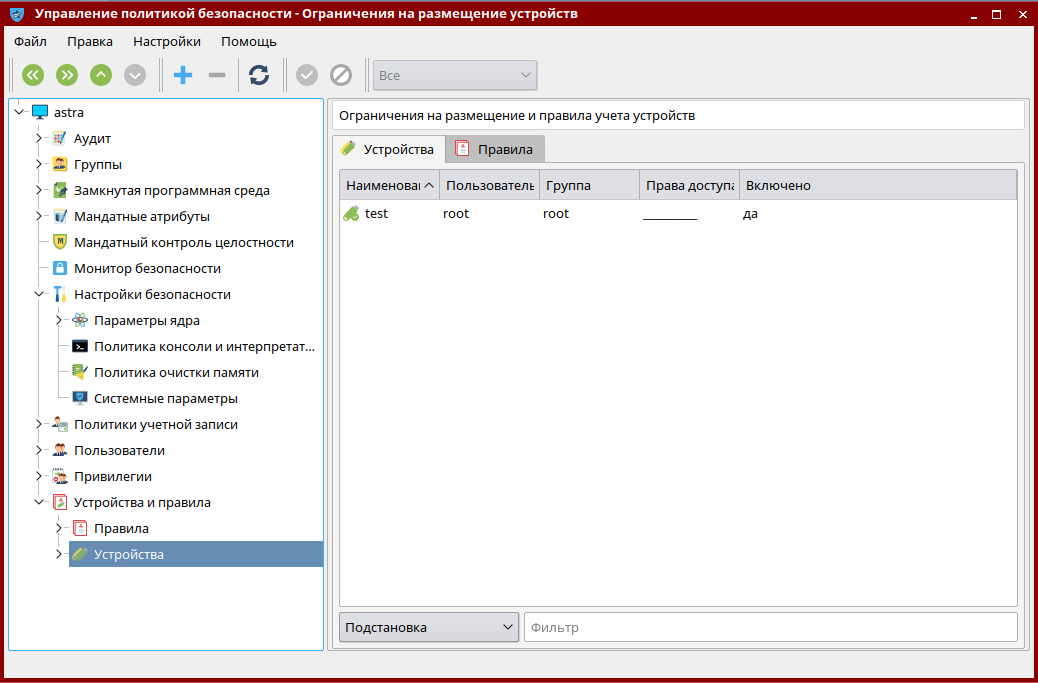


Рисунок 37. Окно зарегистрированных устройств

- вставить носитель информации;

- нажать «Создать новый элемент»;

- выбрать необходимый носитель;

- выполнить все необходимые настройки разграничения доступа к устройству и включить разграничение (рис. 38);

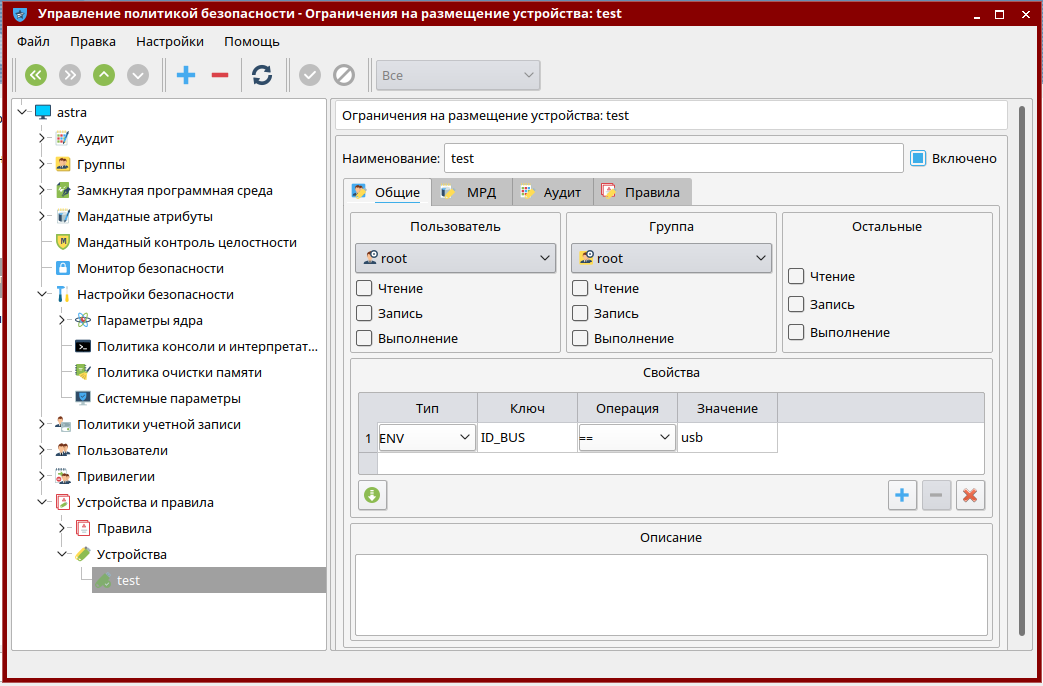


Рисунок 38. Окно настройки разграничения прав доступа к устройству

- нажать «Применить изменения».

**Контрольные вопросы**

1. Опишите механизмы подсистемы регистрации ОС Linux?
2. Состав подсистемы регистрации Auditd
3. Перечислите виды остаточных данных во внешней памяти
4. Какие задачи решает подсистема гарантированного уничтожения информации следующие?
5. Метка субъекта, называемая еще мандатом, задает:
6. Подсистема регистрации и учета предназначена для
7. Основные правила при принудительном разграничение доступа к компьютерным ресурсам
8. Принудительное разграничение доступа
9. Охарактеризуйте функцию резервирования и восстановления информации
10. Какая должна быть частота резервного копирования
11. Что относиться к угрозам несанкционированного использования компьютерных ресурсов
12. Какие отношения регулирует закон Российской Федерации «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 2006 г
13. Обладатель информации – это…
14. Основными функциями СРД являются:
15. Что понимается под политикой безопасности
16. Классификация методов аутентификации по используемым средствам:
17. Перечислите основные виды аппаратных электронных идентификаторов
18. Перечислите положительные стороны использования Смарт-карт:
19. Особенности использования электронных ключей Рутокен.

**Дополнительные материалы, информационные источники**

1. Справочный центр Astra Linux: сайт. ¬– URL: https://wiki.astralinux.ru (дата обращения: 09.09.2020). – Текст: электронный.

2. Макаренко С.И., Ковальский А.А., Краснов С.А. Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем: учеб. пособие. Часть 2: Сетевые операционные системы и принципы обеспечения информационной безопасности в сетях. - СПб.: Наукоемкие технологии, 2020. - 357 с.

3. Краснов, Сергей Александрович. Настройка средств защиты компьютерной информации [Текст]: учеб.­метод. пособие / С. А. Краснов, А. К. Племянников, Д. А. Решетняк, 2020. ­71 с.

**Методика текущего контроля**

Текущий контроль включает в себя контроль посещаемости (не менее 80 % занятий), сдача 4 коллоквиумов по тематике дисциплины (проверка знаний и умений по каждой теме) по результатам которого студент получает допуск на экзамен. На коллоквиумах проводится защиты работ, которые проводились на практических занятиях. В ходе проведения практических занятий целесообразно привлечение студентов к как можно более активному участию в дискуссиях, решении задач, обсуждениях и т. д. При этом активность студентов также может учитываться преподавателем, как один из способов текущего контроля на практических занятиях. самостоятельной работы студентов

Изучение дисциплины сопровождается самостоятельной работой студентов (СРС) с рекомендованными преподавателем литературными источниками и информационными ресурсами сети Интернет. Планирование времени для изучения дисциплины осуществляется на весь период обучения, предусматривая при этом регулярное повторение пройденного материала. Обучающимся, в рамках внеаудиторной самостоятельной работы, необходимо регулярно дополнять сведениями из литературных источников материал, законспектированный на лекциях. При этом на основе изучения рекомендованной литературы целесообразно составить конспект основных положений, терминов и определений, необходимых для освоения разделов учебной дисциплины. Особое место уделяется консультированию, как одной из форм обучения и контроля самостоятельной работы. Консультирование предполагает особым образом организованное взаимодействие между преподавателем и студентами, при этом предполагается, что консультант либо знает готовое решение, которое он может предписать консультируемому, либо он владеет способами деятельности, которые указывают путь решения проблемы.

**Текущая СРС по ПЗ № 4 состоит из:**

1. Работа с лекционным материалом, с учебной литературой – 1,5 ак.ч;

2. Опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях) 1 ак.ч.

3. Самостоятельное изучение разделов дисциплины - 1 ак.ч.

4. Подготовка к лабораторным работам, к практическим и семинарским занятиям – 1,5 ак.ч

5. Подготовка к контрольным работам, коллоквиумам – 1 ак.ч.

Контроль самостоятельной работы студентов осуществляется на лекционных и практических занятиях студентов по методике, описанной выше.

Доцент кафедры ИБ

Краснов С.А.