ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САМАРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА С.П. КОРОЛЕВА»
(САМАРСКИЙ УНИВЕРСИТЕТ)

Д.Б. ЖМУРОВ, С.В. ЖУКОВ

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

САМАРА 2022

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САМАРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА С.П. КОРОЛЕВА»
(САМАРСКИЙ УНИВЕРСИТЕТ)

Д.Б. ЖМУРОВ, С.В. ЖУКОВ

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Рекомендовано редакционно-издательским советом федерального государственного автономного образовательного учреждения высшего образования «Самарский национальный исследовательский университет имени академика С.П. Королева» в качестве учебного пособия для обучающихся по основной образовательной программе высшего образования по специальности 10.05.03 Информационная безопасность автоматизированных систем

Самара
Издательство Самарского университета
2022

УДК 004.056(075)
ББК 32.81я7
Ж774

Рецензенты: канд. техн. наук, доц. Н. Е. К а р п о в а,
канд. физ.-мат. наук, доц. М. Н. О с и п о в

Жмуров, Денис Борисович
Ж774 Программно-аппаратные средства защиты информации: учебное пособие / *Д.Б. Жмуров, С.В. Жуков*. – Самара: Издательство Самарского университета, 2022. – 80 с.: ил.

ISBN 978-5-7883-1799-1

В учебное пособие включены теоретические и практические материалы лабораторного практикума по курсу «Программно-аппаратные средства обеспечения информационной безопасности» для специальности «Информационная безопасность автоматизированных систем».

Учебное пособие может быть полезно студентам, преподавателям и аспирантам, осваивающим практические вопросы защиты информации. Работа включает в себя материал, посвящённый наиболее распространённым системам защиты информации, изучаемых на дисциплине «Программно-аппаратные средства защиты информации» в соответствии с учебным планом.

Подготовлено на кафедре геоинформатики и информационной безопасности.

УДК 004.056(075)
ББК 32.81я7

ISBN 978-5-7883-1799-1

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Обеспечение безопасности информации ограниченного доступа, обрабатываемой в автоматизированных системах, является важной и актуальной задачей. Важность этой задачи продиктована как интересами владельцев, так и требованиями государственных органов, осуществляющих надзор в области защиты информации.

Одним из основных способов обеспечения информационной безопасности локальных автоматизированных систем и вычислительных сетей является использование программно-аппаратных средств защиты. В настоящее время государственный реестр сертифицированных средств защиты информации включает в себя более 4000 наименований средств защиты информации различного назначения.

В настоящем учебном пособии рассмотрены вопросы конфигурирования защитных механизмов программно-аппаратных средств, которые наиболее часто используются для защиты государственной тайны, персональных данных и другой информации ограниченного доступа.

Материал пособия выстроен таким образом, чтобы обучающиеся имели возможность изучить назначение и принципы работы механизмов защиты информации, а также закрепить полученные знания при практической работе на учебном стенде «step–by–step».

Тематика практических работ по изучению СЗИ «Dallas Lock», «SecretNet Studio», «AstraLinux» имеет сходную структуру, благодаря чему обучающиеся имеют возможность проведения сравнительного анализа защитных механизмов реализованных в разных программных продуктах.

Практические знания и навыки, приобретенные в результате изучения представленного в данном пособии материала будут полезны в практической работе по подготовке к аттестации автоматизированных систем.

1 ЗАЩИТА АРМ СРЕДСТВАМИ СЗИ DALLAS LOCK 8.0

1.1 Общая характеристика СЗИ Dallas Lock 8.0

Dallas Lock 8.0 – сертифицированное СЗИ накладного типа для автономных и сетевых АРМ. Предназначено для защиты конфиденциальной информации (редакции «К» и «С»), в том числе содержащейся в АС до класса защищенности 1Г включительно, в ГИС до 1 класса защищенности включительно, в ИСПДн для обеспечения 1 уровня защищенности ПДн, а также для защиты информации, содержащей сведения, составляющие государственную тайну (редакция «С») до уровня «совершенно секретно» включительно.

Назначение системы:

– создание защищенных автоматизированных систем до класса защищенности 1Б включительно;

– обеспечение 1 уровня защищенности персональных данных;

– защита информации в ГИС 1 класса защищенности;

– создание защищенных информационных систем управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды до 1 класса защищенности включительно [1].

1.2 Основные и вспомогательные механизмы защиты

Подробное описание механизмов защиты, реализованных в СЗИ Dallas Lock 8.0, приводится в соответствующей технической документации [1] от производителя этого программного продукта. Далее приведено краткое описание защитных механизмов, изучение которых необходимо для выполнения практических заданий данного пособия.

Блокировка расширений

В системе защиты Dallas Lock 8.0 реализована функция блокировки доступа к файлам по их расширению. Эта функция может быть полезна, к примеру, для того чтобы запретить сотрудникам работу с файлами, не имеющими отношения к их профессиональным обязанностям (mp3, avi и т.д.).

Преобразованные файлы-контейнеры

Имеющиеся на защищенном ПК файлы или папки могут быть преобразованы в файл-контейнер с помощью системы защиты Dallas Lock 8.0 с использованием ключевой информации (пароля и (или) аппаратного идентификатора). Преобразованные файлы или папки могут быть обратно преобразованы в исходные данные, при условии верного ввода ключевой информации.

Таким образом, содержимое файлов-контейнеров становится недоступным на ПК, не защищенном СЗИ НСД Dallas Lock 8.0, и также недоступным на ПК, защищенном СЗИ НСД Dallas Lock 8.0, но в случае введения неверной ключевой информации при обратном преобразовании.

Преобразованные данные хранятся в файле-контейнере, который может быть безопасно передан по незащищенным сетевым каналам, электронной почте или с помощью сменного накопителя.

Для восстановления этих данных необходим пароль и аппаратный идентификатор, используемый при преобразовании.

Преобразованные файл-диски

Для безопасности хранения и обработки информации в Dallas Lock 8.0 реализован механизм создания таких контейнеров информации, при работе с размещенными на которых объектами ФС параллельно работе и не заметно для пользователя выполняется преобразование информации. Данные контейнеры называются преобразованные файл-диски.

Особенностью данного механизма является то, что данные файл-диски могут подключаться (монтироваться и демонтироваться) в ОС

Windows как логические диски и иметь свою букву диска и определенный объем. В то же время информация на таком диске будет преобразованной и подключение диска для работы с ним пользователем может быть произведено только на ПК, защищенном Dallas Lock 8.0, и только с указанием ключевой информации.

Зачистка остаточной информации

Большинство операционных систем при удалении файла не удаляют содержимое файла непосредственно, а всего лишь удаляют запись о файле из директории файловой системы. Так сделано для ускорения работы системы.

Реальное содержимое файла остается на запоминающем устройстве, и его можно достаточно легко просмотреть, по крайней мере, до тех пор, пока операционная система заново не использует это пространство для хранения новых данных. Данная остаточная информация может легко привести к непреднамеренному распространению конфиденциальной и секретной информации.

СЗИ НСД Dallas Lock 8.0 включает подсистему очистки остаточной информации, которая гарантирует предотвращение восстановления удаленных данных.

Добавление штампа на распечатываемые документы

Программный комплекс Dallas Lock позволяет добавлять штамп на распечатываемые документы. Они могут быть двух типов:

– произвольный штамп – пользователь может произвольно редактировать внешний вид штампа и его местоположение на листе;

– штамп по ГОСТ – не редактируемый предопределенный вид штампа.

Контроль целостности файлов и системной конфигурации

Система защиты информации Dallas Lock 8.0 включает в свой состав подсистему обеспечения целостности. Она позволяет контролировать целостность программно-аппаратной среды компьютера, целостность объектов файловой системы и реестра, а также

восстанавливать файлы и ветки реестры в случае обнаружения нарушенной целостности.

Основу механизмов контроля целостности представляет проверка соответствия контролируемого объекта эталонному образцу. Для этого используются контрольные суммы.

Процедура контроля целостности осуществляется следующим образом: после назначения дескриптора целостности при следующей проверке проверяется, было ли уже вычислено эталонное значение контрольной суммы параметра. Если оно еще не было вычислено, оно вычисляется и сохраняется. Если же оно уже было вычислено, то оно сравнивается с вычисляемым текущим значением контрольной суммы контролируемого параметра. Если хотя бы для одного из проверяемых параметров текущее значение параметра не совпало с эталонным значением, результат проверки считается отрицательным, а целостность контролируемых объектов – нарушенной.

1.3 Основные требования по информационной безопасности

В настоящем пособии рассматриваются практические вопросы настройки СЗИ для класса защищенности 2А. Требования безопасности информации приведены в руководящем документе ФСТЭК «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования к защите информации».

В соответствии с указанным документом, в системах класса 2А у пользователей равные полномочия в отношении всей информации. Сама же информация находится на носителях различного уровня конфиденциальности.

Для этого в обязательном порядке должны быть выполнены приведенные ниже требования ко всем подсистемам системы защиты информации.

Подсистема управления доступом

Должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

Подсистема регистрации и учёта

Должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС.

Криптографическая подсистема

Должно осуществляться шифрование всей конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, в каналах связи, а также на съемные носители данных (дискеты, микрокассеты и т.п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. При этом должны выполняться автоматическое освобождение и очистка областей внешней памяти, содержавших ранее незашифрованную информацию.

Подсистема обеспечения целостности

Должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды.

В дополнение к настройке подсистем обеспечим добавление штампа на распечатываемые документы для контроля документации.

1.4 Настройка прав доступа к файлам

Перед выполнением данного этапа необходимо ознакомиться с пунктом 5 руководства по эксплуатации [1].

1. Войти в систему под логином student с уровнем доступа «Сов.секретно» (пароль к этой учетной записи следует узнать у лаборанта).

Примечание. Пользователь *student* имеет права администратора в системе Dallas Lock. Поэтому создание новых пользователей и управление правами доступа следует выполнять из-под этой учетной записи.

Имя пользователя и уровень доступа отображаются в заголовке окна утилиты администратора Dallas Lock.

2. С помощью утилиты администратора Dallas Lock создать новых пользователей с параметрами, указанными в таблице 1.1.

Таблица 1.1. **Параметры учетных записей пользователей**

№	Логин	Полное имя	Уровень доступа
1	Secret_Ivanov	Иванов В.А.	Секретно
2	Secret_Petrov	Петров П.В.	Секретно
3	Open_Ivanov	Открытые данные	Открытые данные

Примечание. Вместо Ivanov, Petrov следует указывать фамилии студентов, выполняющих работу.

3. Убедиться, что учетные записи созданы в системе и для них подготовлены системные папки. Для этого нужно войти под учёткой каждого пользователя, указав уровень доступа «Открытые данные».

Примечание. Дальнейшая работа с настройкой прав пользователей будет проводиться в отношении пользовательских папок, находящихся в папке c:\Users\. Следует проверить наличие папок Secret_Ivanov, Secret_Petrov и Open_Ivanov.

4. Настроить доступ к папке Secret_Petrov следующим образом:

– пользователь Secret_Petrov имеет полный доступ ко всем вложенным папкам своей папки (которая также называется Secret_Petrov);

– пользователь Secret_Ivanov имеет полный доступ к папке «Мои документы» в Secret_Petrov;

– пользователь Secret_Ivanov имеет право просматривать файлы в папке «Мои видео» в Secret_Petrov, но не имеет право создавать новые файлы и изменять существующие.

Примечание. При задании прав доступа средствами Dallas Lock следует также задать соответствующие права доступа в системных настройках безопасности для соответствующих папок.

5. Включить полный аудит папок Secret_Ivanov и Secret_Petrov.

6. Настроить двухфакторную аутентификацию пользователя Secret_Ivanov по паролю и аппаратному идентификатору (токену).

Указание. Если данную работу одновременно выполняют две бригады и имеется только один аппаратный идентификатор, то этот пункт можно выполнить позже, по договоренности между бригадами.

1.5 Проверка прав доступа к файлам

Перед выполнением данного этапа необходимо ознакомиться с пунктом 5 руководства по эксплуатации [1].

1. Проверить полный доступ пользователя Secret_Petrov ко всем вложенным папкам своей папки (которая также называется Secret_Petrov).

Для этого следует зайти в систему под учёткой Secret_Petrov и создать любые файлы в папках «Мои документы», «Мои видео» и т.п.

2. Проверить полный доступ пользователя Secret_Ivanov к папке «Мои документы» впапке Secret_Petrov.

Для этого следует зайти в систему под учёткой Secret_Ivanov и создать любой файл в папке «Мои документы» в папке Secret_Petrov.

3. Проверить доступ пользователя Secret_Ivanov к папке «Мои видео» в Secret_Petrov с правами только чтения.

Для этого следует зайти в систему под учётной записью Secret_Ivanov и попытаться создать любой файл в папке «Мои видео» в папке Secret_Petrov. В этом действии должно быть отказано.

Выполнить попытку просмотра файла в папке «Мои видео». Это действие должно быть разрешено.

4. Проверить права доступа пользователя Open_Ivanov. Для этого следует зайти в систему под учёткой Open_Ivanov и попытаться открыть папки Secret_Ivanov и Secret_Petrov. В доступе должно быть отказано. Доступ к папке Open_Ivanov должен быть разрешен.

5. Проверить работу двухфакторной аутентификации. Для этого нужно попытаться войти в систему под учёткой Secret_Ivanov (к которой ранее был привязан аппаратный идентификатор). Во входе должно быть отказано.

6. Проверить правильность работы авторизации. Для этого нужно выполнить п.7, однако при входе в систему указать уровень доступа «Открытые данные». В доступе к файлам должно быть отказано.

7. Просмотреть журналы доступа и убедиться, что в них содержатся выполненные ранее действия по доступу к папкам Secret_Ivanov и Secret_Petrov.

8. Просмотреть журнал входов в систему и убедиться, что там содержится запись о неудачной попытке входа в систему пользователя Secret_Ivanov без аппаратного идентификатора (при выполнении п. 11).

1.6 Настройка управления отчуждаемыми носителями

Перед выполнением данного этапа необходимо ознакомиться с пунктом 13 руководства по эксплуатации [1].

1. Запретить использование всех USB-накопителей пользователю Secret_Ivanov.

Примечание. Для этого и последующих действий следует включать режим аудита доступа.

2. Вставить полученный USB-накопитель, зайти в систему под учетной записью Secret_Ivanov и проверить, запрещён ли доступ к нему.

3. Убедиться, что в журнале аудита появилась соответствующая запись о попытке доступа.

4. Разрешить пользователю Secret_Petrov использование имеющегося USB-накопителя. Доступ ко всем остальным должен быть запрещен.

5. Убедиться, что из учетной записи Secret_Petrov есть доступ только к одному, «разрешенному» USB-накопителю.

1.7 Блокировка работы с файлами по расширению

Перед выполнением данного этапа необходимо ознакомиться с пунктом 5 руководства по эксплуатации [1].

Дальнейшие задания следует выполнять под учетной записью Secret_Ivanov.

1. Создать на рабочем столе файлы с расширением .txt, .mp3, .avi, .pdf, .mp4.

2. Запустить Dallas Lock и на вкладке «Параметры безопасности» зайти в категорию «Блокируемые расширения». В окне программы появится поле со списком запрещенных расширений файлов и панель действий, содержащая инструменты по добавлению,

удалению или редактированию свойств необходимых блокируемых администратором расширений.

3. Нажать кнопку «Добавить», в результате чего выведется окно «Заблокированные расширения файлов».

В данном окне введите одно из расширений, указанных в первом пункте, и комментарий к нему, после чего нажмите кнопку «ОК». Повторите данную процедуру для оставшихся расширений.

4. Проверьте возможность доступа к ранее созданным файлам.

Следует учесть, что добавление в список блокируемых расширений, таких как exe, dll, sys – может привести к неработоспособности ОС!

1.8 Использование механизмов шифрования данных

СЗИ предоставляет возможность использования двух механизмов шифрования данных:

– преобразование данных в файл-контейнер;

– преобразование данных в файл-диск.

Указание. Перед выполнением данного этапа необходимо ознакомиться с пунктом 12 руководства по эксплуатации.

Чтобы выполнить преобразование данных в файл-контейнер следует выполнить перечисленные ниже действия.

1. Создать на рабочем столе файл test.txt.

2. Нажать на получившийся файл правой кнопкой мыши и в появившемся окне выбрать пункт «DL8.0: Преобразование данных».

3. В верхнем правом углу нажать на кнопку «Обзор» и в качестве пути сохранения файла выбрать рабочий стол. Алгоритм преобразования не изменять и оставить встроенный по умолчанию.

4. В нижней части окна ввести пароль и его подтверждение, после чего нажать на кнопку «Преобразование».

Убедиться, что на рабочем столе появился преобразованный файл и попытаться открыть его.

5. В появившемся окне аналогично пункту 3 выбрать в качестве папки назначения «Рабочий стол» и ввести ранее используемый пароль.

6. Проверить наличие не преобразованного файла.

Чтобы выполнить преобразование данных в файл-диск следует выполнить перечисленные ниже действия.

Перед дальнейшим выполнением работы необходимо ознакомиться с пунктом 12 руководства по эксплуатации.

7. На панели задач в меню значка блокировки ПК выбрать «Преобразованные файл диски» и затем «Создать преобразованный файл-диск».

8. В появившемся окне нажать на кнопку «обзор» и выбрать в качестве пути, по которому будет сохранен файл-диск – «Рабочий стол».

9. Размер диска указать 300мб и выбрать любую свободную букву диска.

10. Указать один из двух доступных алгоритмов преобразования и ввести пароль.

11. Убедиться в наличии ярлыка диска на рабочем столе и в «Проводнике».

12. Создать на файл-диске несколько файлов и отключить его. Для этого нажать на него правой кнопкой мыши и выбрать в появившемся меню пункт «отключить».

13. Убедиться в его отсутствии в «проводнике», после чего подключить его. Для этого на рабочем столе необходимо нажать на ярлык отключенного диска и ввести пароль, после чего проверить целостность файлов находящемся на подключенном диске.

1.9 Затирание остаточной информации

Перед выполнением данной работы необходимо ознакомиться с пунктом 8 руководства по эксплуатации [1].

1. Запустить Dallas Lock и на вкладке «Параметры безопасности» зайти в категорию «Очистка остаточной информации». В окне программы появится список параметров очистки остаточной информации.

2. Нажать на пункт «Проверять очистку остаточной информации» и в появившемся окне выбрать параметр «да», после чего нажать кнопку «ОК».

В качестве зачищаемого диска будет использоваться съемный носитель информации. Для этого необходимо подключить его к компьютеру.

3. В окне программы Dallas Lock перейти в основное меню, для этого нажать на значок программы в левом верхнем углу и выбрать пункт «зачистка диска».

4. В появившемся окне выбрать подключенный ранее съемный носитель и нажать кнопку «зачистить». (Появится предупреждающие о невозможности восстановления данных окно, в нем необходимо нажать на кнопку «Да»).

5. Убедиться, что в журнале ресурсов появилась соответствующая запись.

1.10 Маркировка распечатываемых документов

Указание. Перед выполнением данного этапа необходимо ознакомиться с пунктом 7 руководства по эксплуатации.

1. Запустить Dallas Lock и на вкладке «Параметры безопасности» зайти в категорию «Аудит». В окне программы выбрать пункт «Печать/редактировать штамп».

2. В новом окне нажать кнопку «да», а затем «редактировать» и в редакторе штампа создать свой штамп путем нажатия на кнопку «добавить элемент». Новый штамп должен содержать следующие параметры: дата и время, компьютер, имя пользователя и метку мандатного доступа. Редактирование содержания штампа происходит через элемент «Изменить текст».

3. Сохранить новый штамп на рабочий стол, нажав на кнопку программы в левом верхнем углу и последующим нажатием кнопки «сохранить как» и выбрать соответствующий путь. После этого выйти из редактора штампа. Если появится уведомление о том, что изменения не были применены – нажать на кнопку «Да».

4. Создать на рабочем столе новый документ формата .docx.

5. Перейти в параметр «Печать», в качестве принтера выбрать «Microsoft XPS Document Writer» и нажать кнопку «Да». В появившемся окне выбора пути сохранения файла указать «Рабочий стол».

6. Открыть созданный документ расширением .xps и убедиться, что штамп был успешно добавлен в документ.

1.11 Настройка подсистемы контроля целостности

Указание. Перед выполнением данного этапа необходимо ознакомиться с пунктом 9 руководства по эксплуатации [1].

1. Запустить программный комплекс Dallas Lock и на вкладке «Параметры безопасности» перейти в категорию «Контроль целостности», а затем в подкатегорию «Политики».

2. Выбрать пункт «Периодический контроль» и установить период контроля файловой системы равным 1 минуте.

3. Выбрать пункт «Контроль ФС по расписанию», выбрать для него все дни недели и установить время на 2 минуты позже текущего.

4. На вкладке «Журналы» перейти в категорию «Журнал управления политиками» и убедиться, что примененные настройки успешно добавлены в систему.

Контрольные вопросы по разделу 1

1. Какие учетные записи присутствуют в Dallas Lock по умолчанию?

2. Какие пользователи обладают правами для создания, удаления и изменения учетных записей пользователей?

3. Сколько уровней мандатного доступа предусмотрено в Dallas Lock? Какой уровень имеет наивысшие права?

4. Какие виды аудита папок имеются в Dallas Lock?

5. Какие параметры парольной политики доступны при создании/модификации учетной записи пользователя?

6. Для чего нужны преобразованные файлы?

2 ЗАЩИТА АРМ СРЕДСТВАМИ SECRET NET STUDIO

2.1 Архитектура и основные программные компоненты

Система Secret Net Studio (далее – SNS) состоит из следующих программных пакетов:

– «Secret Net Studio» (далее – клиент);

– «Secret Net Studio – Сервер безопасности» (далее – СБ);

– «Secret Net Studio – Центр управления» (далее – ЦУ).

Клиент предназначен для реализации защиты компьютера, на котором он установлен, путем применения защитных механизмов, расширяющих и дополняющих средства безопасности ОС Windows. Защитные механизмы – это совокупность настраиваемых программных средств, входящих в состав клиента и обеспечивающих безопасное использование ресурсов.

Сервер безопасности обеспечивает хранение данных централизованного управления, координацию работы других компонентов защиты в процессе централизованного управления системой, получение от клиентов и обработку информации о состоянии защищаемых компьютеров, управление пользователями и авторизацией сетевых соединений, а также централизованный сбор, хранение и архивирование журналов.

Программа управления обеспечивает управление параметрами объектов, отображение информации о состоянии защищаемых компьютеров и произошедших событиях тревоги, загрузку журналов событий, оперативное управление компьютерами и централизованное получение отчетов.

Клиент Secret Net Studio содержит следующие механизмы защиты:

– защита от входа в систему;

– функциональный контроль систем;

– регистрация событий;

– контроль целостности;

– замкнутая программная среда;

– механизм изоляции процессов;

– дискреционное управление доступом к ресурсам файловой системы;

– затирание удаляемой информации;

– контроль подключения и изменения устройств компьютера;

– разграничение доступа к устройствам;

– полномочное управление доступом;

– контроль печати;

– теневое копирование выводимых данных;

– защита информации на локальных дисках;

– шифрование данных в криптоконтейнерах;

– персональный межсетевой экран;

– авторизация сетевых соединений;

– обнаружение и предотвращение вторжений;

– антивирус;

– шифрование трафика с использованием VPN-клиента.

Далее рассмотрим некоторые механизмы защиты в SNS более подробно.

2.2 Механизмы защиты информации

Механизм контроля целостности

Механизм контроля целостности (КЦ) предназначен для слежения за неизменностью содержимого ресурсов компьютера, а его действие основано на сравнении текущих и эталонных значений контролируемых параметров проверяемых ресурсов. При обнаружении несоответствия система оповещает администратора о нарушении целостности ресурса и выполняет заданное при настройке

действие, например, блокирует компьютер, на котором это несоответствие обнаружено.

Замкнутая программная среда

Механизм замкнутой программной среды (ЗПС) предназначен для ограничения использования ПО на компьютере. Доступ разрешается только к тем программам, которые необходимы пользователям для работы. Для каждого пользователя определяется перечень ресурсов, в который входят разрешенные для запуска программы, библиотеки и сценарии. Попытки запуска других ресурсов блокируются, и в журнале регистрируются события тревоги. Настройка механизмов КЦ и ЗПС может осуществляться совместно в программе «Контроль программ и данных».

Контроль отчуждаемых носителей информации

Разграничение доступа пользователей к устройствам выполняется на основании списков устройств, которые формируются механизмом контроля подключения и изменения устройств. Для каждого устройства можно задать ряд ограничений на использование, категорию конфиденциальности или запретить пользоваться устройством вовсе. Также можно задать реакцию системы: например, при входе пользователя под своей учетной записью в момент, когда подключен «запрещенный» носитель информации, может быть отказано в доступе. Каждое действие с отчуждаемыми носителями информации регистрируется в журнале событий.

Дискреционное управление доступом

Механизм дискреционного управления доступом к ресурсам файловой системы обеспечивает:

– разграничение доступа пользователей к каталогам и файлам на локальных дисках на основе матрицы доступа субъектов к объектам доступа;

– контроль доступа к объектам при локальных или сетевых обращениях, включая обращения от имени системной учетной записи;

– невозможность доступа к объектам в обход установленных прав доступа (если используются стандартные средства ОС или прикладные программы без собственных драйверов для работы с файловой системой, поскольку в SNS диспетчер доступа к файлам и директориям работает над стандартным диспетчером Windows);

– независимость действия от встроенного механизма избирательного разграничения доступа ОС Windows: установленные в системе Secret Net Studio права доступа к файловым объектам не зависят от аналогичных прав доступа в ОС Windows и наоборот.

Полномочное управление доступом

Возможности механизма полномочного управления доступом:

– разграничение доступа пользователей к конфиденциальной информации;

– контроль подключения и использования устройств с назначенными категориями конфиденциальности;

– контроль потоков конфиденциальной информации в системе;

– контроль использования сетевых интерфейсов, для которых указаны допустимые уровни конфиденциальности сессий пользователей;

– контроль печати конфиденциальных документов, что позволяет ограничить использование принтеров для печати документов, которым присвоены определенные категории конфиденциальности. По умолчанию на всех принтерах разрешается печать документов с любой категорией конфиденциальности.

Количество категорий конфиденциальности можно увеличить с 3 (по умолчанию) до 16 и переименовать их.

Регистрация событий

По умолчанию в журнале Secret Net Studio регистрируются все возможные события, кроме некоторых событий категории «Контроль приложений», а также некоторых событий категорий «Кон-

троль целостности» и «Дискреционный доступ». Отдельные категории событий (например, события категории «Регистрация») регистрируются в обязательном порядке и их регистрацию отключить нельзя. Содержащиеся в журнале сведения содержат подробную информацию для анализа событий и позволяют контролировать работу механизмов защиты.

Теневое копирование выводимых данных

Механизм теневого копирования обеспечивает создание в системе дубликатов (копий) данных, выводимых на отчуждаемые носители информации. Эти копии сохраняются в специальном хранилище, доступ к которому имеют только уполномоченные пользователи. Действие механизма распространяется на те устройства, для которых включен режим сохранения копий при записи информации.

При включенном режиме сохранения копий вывод данных на внешнее устройство возможен только при условии создания копии этих данных в хранилище теневого копирования. Если по каким-либо причинам создать дубликат невозможно, операция вывода данных блокируется.

Теневое копирование поддерживается для устройств следующих видов:

– подключаемые сменные диски;

– дисководы гибких дисков;

– дисководы оптических дисков с функцией записи;

– принтеры.

Контроль печати и маркировка твёрдых копий

Механизм контроля печати позволяет предотвратить несанкционированный вывод конфиденциальных документов на локальные и сетевые принтеры и обеспечивает:

– разграничение доступа пользователей к принтерам;

– регистрацию событий вывода документов на печать в журнале Secret Net Studio;

– вывод на печать документов с определенной категорией конфиденциальности;

– автоматическое добавление грифа в распечатываемые документы;

– теневое копирование распечатываемых документов.

При включенном режиме маркировки в распечатываемые документы автоматически добавляются специальные маркеры (грифы), содержащие учетные сведения для печати. Маркер – это особая форма со сведениями о распечатанном документе (например, когда распечатан, кем, сколько страниц), который обычно располагается в колонтитулах или на полях страниц. Механизм маркировки позволяет:

– при печати документов для каждой категории конфиденциальности задать свой маркер или несколько маркеров;

– настроить маркировку в соответствии с действующими в организации требованиями оформления.

Характеристика работы

В данной работе будет произведена настройка локальной защиты АРМ пользователя, который может быть сотрудником предприятия. Для локальной защиты необходимо:

– обозначить его права по доступу к ресурсам, находящимся на АРМ;

– ограничить использование внешних носителей;

– настроить механизм замкнутой программной среды (список программ, возможных к запуску);

– настроить механизм теневого копирования и маркировки;

– обеспечить контроль целостности ресурсов, находящихся на АРМ.

2.3 Порядок работы с виртуальным учебным стендом

Выполнение практических заданий по изучению защитных механизмов SNS производится на специально подготовленных виртуальных стендах, которые для учебных целей предоставляет разработчик данного программного продукта – ООО «Код Безопасности».

Для выполнения работы следует использовать рабочие места, обозначенные как S11 и S12. Перед началом работы следует получить носитель информации у лаборанта.

На рабочем месте S12 установлен гипервизор с виртуальными машинами (далее – ВМ), используемыми для выполнения практических заданий. На рабочем месте S11 установлено клиентское ПО для доступа к ВМ гипервизора.

Перед началом работы рабочее место S12 должно быть выключено. При включении рабочего места следует войти в BIOS нажатием клавиши F2 или DEL. В появившимся UEFI-меню выбрать пункт «Boot», далее выбрать параметр «Boot Option #1». В опциях параметра «Boot Option #1» выбрать жесткий диск, на котором установлен гипервизор. После выполнения этих действий нужно выйти из меню UEFI сохранив изменения в конфигурации и дождаться загрузки гипервизора «VMwareESXi».

На рабочем месте S11 запустить ПО «VMware vSphere Client». В появившемся окне, в поле «IP address/Name» ввести IP-адрес гипервизора (в данном случае это 192.168.2.19) в поле «Username» ввести логин – **root**, в поле «Password» – **P@ssw0rd** и дождаться успешной авторизации.

После авторизации в левом верхнем углу окна, показанного на рисунке 2.1, будет отображаться IP-адрес гипервизора и список доступных на нём виртуальных машин.

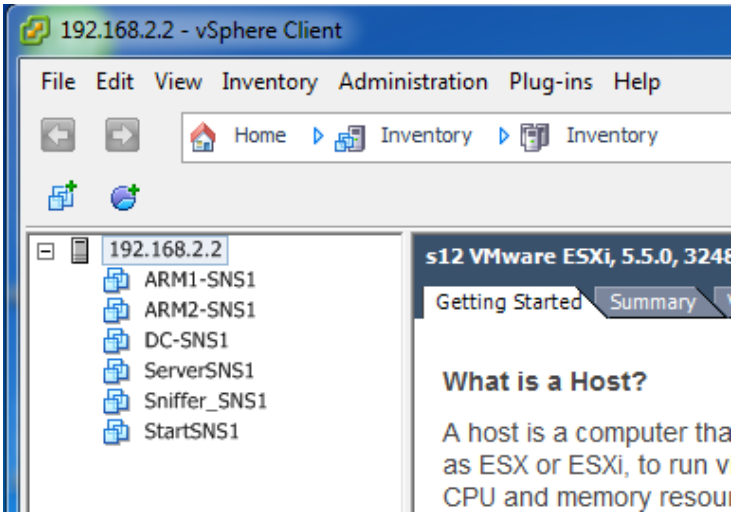

Рис. 2.1. Список доступных виртуальных машин гипервизора

ВМ StartSNS1 с гостевой ОС Microsoft Windows 7 x64 SP1 выполняет функции отдельного защищаемого компьютера.

Указанная ВМ содержит учетные записи, необходимые для выполнения практических заданий. Аутентификационные данные учетных записей представлены в таблице 1.

Таблица 2.1. **Аутентификационные данные учетных записей**

Учетная запись	**Пароль**	**Комментарии**
Администратор	P@ssw0rd	Встроенная УЗ локального администратора
adminsns	P@ssw0rd	Дополнительная УЗ с правами локального администратора
user1	P@ssw0rd	Пользовательская УЗ: Иванов Иван Иванович
user2	P@ssw0rd	Пользовательская УЗ: Иванова Мария Ивановна

2.4 Настройка механизма контроля целостности

Перед выполнением данной работы следует ознакомиться с главой 4 электронного документа «Руководство администратора. Настройка и эксплуатация. Локальная защита» разработанного в ООО «Код безопасности» [2].

Начальную настройку механизма контроля целостности и проверку его работоспособности покажем на примере работы с документом формата Microsoft Word. Для этого следует выполнить указанные ниже действия.

В окне ВМ StartSNS на диске «С:» создать папку «Контроль целостности». В этой папке создать файл «Документ Microsoft Word.docx» с произвольным содержанием, который будет контролируемым ресурсом в МД КЦ.

Запустить программу «Контроль программ и данных» в локальном режиме: «Пуск → Все программы → Код Безопасности → Secret Net Studio → Контроль программ и данных» и в открывшемся окне выбрать категорию «Ресурсы».

Подготовить описание контролируемого ресурса (созданного ранее файла) в модели данных КЦ. Для этого:

– в поле «Структура» вызвать контекстное меню папки «Ресурсы» и выбрать опцию «Создать ресурс(ы) / Одиночный»;

– в окне создания нового ресурса выбрать тип «Ресурс Windows» и нажать кнопку «ОК» – откроется следующее диалоговое окно создания ресурса.

– в поле «Тип» оставить установленный по умолчанию тип ресурса «Файл», через кнопку «Обзор» указать путь к созданному в п. 1 файлу «Документ Microsoft Word.docx» и нажать кнопку «ОК». Описание ресурса готово, вернитесь в окно «Контроль программ и данных».

В окне «Контроль программ и данных» в поле «Структура» развернуть ветку «Ресурсы / Файлы и каталоги / C:» и в папке «Контроль целостности» найти запись с описанием выбранного вами файла для контроля.

Согласно описанию модели данных контроля целостности, сформировать группу ресурсов и добавить в нее подготовленный ресурс. Для этого:

– в окне «Контроль программ и данных» выбрать категорию «Группы ресурсов»;

– в поле «Структура» вызвать контекстное меню папки «Группы ресурсов» и выбрать опцию «Создать группу / Вручную» – откроется диалоговое окно;

– в окне «Создание группы ресурсов» заполнить поля: «Имя» – ввести «Группа ресурсов для КЦ», «Описание» – произвольно. Нажать кнопку «ОК». В окне «Контроль программ и данных» появится запись с названием созданной группы. Обратить внимание, что группа пустая;

– в открывшемся диалоговом окне выделить запись подготовленного вами ранее файла ресурса «C:\Контроль целостности\Документ Microsoft Word.docx» и нажать кнопку «ОК» – в созданную группу добавлен файл ресурса.

В окне «Контроль программ и данных» создать новую задачу и добавить в нее подготовленную для контроля группу ресурсов. Для этого:

– выбрать категорию «Задачи», вызвать контекстное меню папки «Задачи» и выбрать опцию «Создать задачу / Вручную». Откроется диалоговое окно;

– ввести в поле «Имя» – имя задачи «КЦ в пособии», в поле «Описание» – произвольный текст;

– нажать кнопку «ОК». В структуре «Задачи» окна «Контроль программ и данных» появилась новая запись;

– в созданную задачу добавить группу ресурсов для КЦ. Для этого необходимо вызвать контекстное меню задачи «КЦ в пособии» и выбрать опцию «Добавить группы / Существующие». Откроется диалоговое окно;

– в окне «Добавление подчиненных объектов к выбранному», выбрать запись «Группа ресурсов для КЦ» и нажать кнопку «ОК» – задача создана и в нее добавлена группа.

В окне «Контроль программ и данных» создать новое задание. Для этого:

– открыть категорию «Задания» и в контекстном меню папки «Задания» выбрать опцию «Создать задание». Откроется диалоговое окно;

– обратить внимание, что опция «Контроль целостности (КЦ)» выбрана по умолчанию и нажать кнопку «ОК». Откроется диалоговое окно «Создание нового задания на КЦ»;

– в окне «Создание нового задания на КЦ, установить параметры: «Метод контроля ресурсов» – «Содержимое», «Алгоритм» – «Полное совпадение»;

– в группе «Реакция на отказ» для параметра «Действие» выбрать «Восстановить с блокировкой»;

– перейти на вкладку «Расписание», и в таблице «Календарный план» установить все отметки в верхней строке «Пн» – «Сб»;

– в поле «Временные параметры» установить флажок, в поле «Часы контроля» выбрать «Каждый час» и указать интервал «2 мин.». Проверка целостности ресурса будет проводиться в заданные дни каждый час с интервалом 2 минуты.

Нажать кнопку «ОК». В панели «Задания» сформируется новое задание «Новое задание на КЦ». Добавить в созданное задание задачу «КЦ в пособии». Для этого:

– в окне «Контроль программ и данных», для экземпляра задания «Новое задание на КЦ» вызвать контекстное меню и выбрать

опцию «Добавить задачи / группы / Существующие». Откроется диалоговое окно;

– выбрать задачу «КЦ в пособии» и нажать кнопку «ОК». После нажатия кнопки «ОК» откроется окно «Контроль программ и данных», в котором отобразится задача, добавленная в задание.

Указать субъект управления, на котором будет выполняться контроль целостности, т.е. выбрать компьютер и добить к нему сформированное задание – при установке связи заданий контроля целостности с субъектами «Компьютер» или «Группа» (компьютеров) включается действие механизма КЦ. Для этого:

– в окне «Контроль программ и данных» выбрать категорию «Субъекты управления» и для компьютера StartSNS из контекстного меню выбрать опцию «Добавить задания / Существующие». Откроется диалоговое окно добавления объектов;

– выбрать задание «Новое задание на КЦ» и нажать кнопку «ОК». Задание добавлено субъекту.

Провести расчет эталонов для входящих в задания контролируемых ресурсов. Для этого необходимо сделать следующее:

– в панели «Структура» развернуть структуру субъекта управления «StartSNS», найти и выделить задание «Новое задание на КЦ»;

– в главном меню выбрать опцию «Сервис / Эталоны / Расчет». Откроется диалоговое окно «Расчет эталонов»;

– в разделе «Реакция на ошибки» установить для всех пунктов значение «Выводить запрос»;

– нажать кнопку «ОК». В диалоговом окне подтверждения сохранения изменений нажать кнопку «Да» и дождаться окончания процесса расчета эталонов для ресурсов: после завершения расчета в окне информационного сообщения нажать кнопку «ОК». Вы вернетесь в окно программы «Контроль программ и данных».

Контроль целостности настроен. Далее следует проверить корректность работы механизма контроля целостности.

Для этого необходимо завершить работу программы «Контроль программ и данных», перезагрузить ВМ и авторизоваться под учетной записью «user1» (Иванов Иван Иванович).

Открыть файл «C:\Контроль целостности\Документ Microsoft Word.docx», внести произвольные изменения, а затем сохранить и закрыть документ.

Подождать указанное ранее в расписании контроля целостности время. Компьютер должен заблокироваться системой защиты Secret Net Studio.

Войти в систему под учетной записью «adminsns». В диалоговом окне ознакомиться с запросом на снятие блокировки.

Нажать кнопку «Да» в диалоговом окне, снять блокировку и дождаться окончания загрузки ОС.

Проверить целостность файла «C:\Контроль целостности\Документ Microsoft Word.docx». Для этого необходимо открыть данный файл и убедиться, что он восстановлен.

В программе «Локальный центр управления» открыть журнал событий Secret Net Studio. Найти и ознакомиться с записями категории «Контроль целостности» с уровнем угрозы «Повышенный».

2.5 Настройка полномочного управления доступом

Перед выполнением данной работы следует ознакомиться с главой 5 электронного документа «Руководство администратора. Настройка и эксплуатация. Локальная защита» разработанного в ООО «Код безопасности» [2].

1. Откройте консоль ВМ StartSNS и авторизуйтесь под учетной записью «adminsns». Запустите «Локальный центр управления» и раскройте в панель «Компьютер».

2. Для первоначальной настройки механизма полномочного управления доступом задайте следующие категории конфиденциальности: «Неконфиденциально», «ДСП» (для служебного пользования), «Секретно». Для этого в программе управления перейдите на вкладку «Настройки», в разделе «Политики» правой части окна раскройте группу «Защита локальных ресурсов / Полномочное управление доступом» и выполните следующие действия:

– используя кнопки, ознакомьтесь с информацией о настройках «Названия уровней конфиденциальности» и «Режим работы». Обратите внимание, что первые три уровня можно только переименовать;

– в поле «Названия уровней конфиденциальности» выберите значение «Конфиденциально» и с помощью клавиши [F2] переименуйте его в «ДСП» (для переименования можно также использовать двойной щелчок);

– аналогично переименуйте «Строго конфиденциально» в «Секретно»;

– убедитесь, что в поле «Режим работы» выбран переключатель «Контроль потоков отключен»;

– на вкладке «Настройки» нажмите кнопку «Применить» и просмотрите появившуюся запись в панели событий системы.

3. Назначьте уровни допуска и привилегии пользователей на компьютере StartSNS. Для этого перейдите в консоль его ВМ и убедитесь, что вы авторизованы под учетной записью «adminsns». Запустите программу «Управление пользователями»: «Пуск / Все программы / Код безопасности / Secret Net Studio / Управление пользователями» и выполните следующие действия:

– откройте окно свойств учетной записи администратора adminsns и в открывшемся окне перейдите на вкладку «Параметры безопасности»;

– на вкладке «Параметры безопасности» выберите категорию настроек «Доступ», установите для администратора «adminsns» самый высокий уровень допуска «Секретно», включите все привилегии и нажмите кнопку «ОК»;

– аналогично – для пользователей «user1» и «user2» на ВМ StartSNS назначьте уровни доступа согласно таблице 2.2 и установите все привилегии.

Таблица 2.2. **Уровни доступа**

Пользователь	**Полное имя**	**Пароль**	**Уровень допуска**
User1	Иван Иванович Иванов	P@ssw0rd	Секретно
User2	Мария Ивановна Иванова	P@ssw0rd	ДСП

4. Используя описание п. 3, выполните аналогичную настройку уровней доступа и привилегий в сетевом варианте программы «Управление пользователями» с рабочего места ARM2 под учетной записью «dadminsns1» согласно таблице 2.3.

Таблица 2.3. **Уровни доступа в сетевом варианте**

Пользователь	**Полное имя**	**Пароль**	**Уровень допуска**
dadminsns1	dadminsns1	P@ssw0rd	Секретно
User1	Иван Иванович Иванов	P@ssw0rd	Секретно
User2	Мария Ивановна Иванова	P@ssw0rd	ДСП

5. В консоли ВМ компьютера StartSNS переавторизуйтесь под учетной записью «adminsns», чтобы назначенный ранее уровень допуска и привилегии вступили в силу, и создайте на диске «C:» папки: «Секретно», «ДСП» и «Неконфиденциально». Выберите для каждой из них в соответствии с названием категорию конфиденциальности.

6. В папке «C:\Секретно» создайте документ формата Microsoft Word с произвольным содержанием: «тест.docx». Аналогично – в папке «C:\ДСП» создайте документ «тест1.docx».

7. Чтобы обеспечить функционирование механизма полномочного управления доступом при включенном режиме контроля потоков, проведите дополнительную настройку локально на компьютере. Подобная настройка должна выполняться перед включением режима контроля потоков, а также в процессе эксплуатации системы при добавлении новых пользователей, программ, принтеров для оптимизации функционирования механизма.

8. В окне ВМ StartSNS загрузите программу настройки подсистемы полномочного управления доступом – Пуск → Все программы → Код безопасности → Secret Net Studio → Программа настройки подсистемы полномочного управления доступом.

9. Запустите настройку для программ Microsoft Office. Для этого в разделе настроек выберите: Вручную → Программы → Microsoft Office и нажмите кнопку «Настроить».

Программа проведет настройку перенаправления файлов. Дождитесь завершения этого процесса. После создания правил перенаправления появится окно с информацией об успешном проведении настройки.

10. В окне «Настройка подсистемы полномочного управления доступом» нажмите кнопку «Закрыть». Перезагрузите ОС на ВМ StartSNS и авторизуйтесь под учетной записью «user2 – Иванова Мария Ивановна» с уровнем допуска «ДСП».

11. Сделайте попытку открытия любого файла из папки «C:\Секретно». Поскольку уровень допуска пользователя «user2» ниже, чем уровень конфиденциальности каталога «Секретно» и его содержимого, механизм полномочного управления доступом Secret Net Studio не позволит открыть документ, и система выдаст соответствующее сообщение.

12. Переавторизуйтесь на ВМ компьютера StartSNS под учетной записью пользователя «user1 – Иванов Иван Иванович», сделайте аналогичную попытку открытия любого файла из папки «C:\Секретно» и сравните результат.

2.6 Настройка дискреционного управления доступом

Перед выполнением данной работы следует ознакомиться с главой 6 электронного документа «Руководство администратора. Настройка и эксплуатация. Локальная защита» разработанного в ООО «Код безопасности» [2].

1. Переавторизуйтесь на ВМ StartSNS под учетной записью администратора adminsns.

2. На диске «C:» создайте следующие защищаемые ресурсы:

– папку «Иванов» и в ней файл произвольного содержания «Доклад.txt»;

– папку «Иванова» и в ней файл произвольного содержания «График.txt»;

– папку «Общие» и в ней файл произвольного содержания «План.txt».

3. Убедитесь, что администратору предоставлены привилегии для изменения прав доступа на любых ресурсах, а также настроена регистрация событий, связанных с доступом к ресурсам. Для этого:

– загрузите программу «Локальный центр управления», в панели «Компьютер» выберите вкладку «Настройки» и откройте раздел политик «Политики/ Защита локальных ресурсов / Дискреционное управление доступом»;

– убедитесь, что в параметре «Учетные записи с привилегией управления правами доступа» выбрана по умолчанию группа локальных администраторов, и с помощью кнопки  ознакомьтесь с описанием этой настройки. Обратите внимание, что при необходимости, используя кнопку «Добавить»  , можно установить привилегию управления правами доступа для ресурсов другому пользователю или группе пользователей;

– нажмите кнопку–ссылку «Аудит…» – вы перейдете в раздел настроек «Регистрация событий / Дискреционное управление доступом»;

– с помощью кнопки  ознакомьтесь с описанием событий.

Обратите внимание, что в целях минимизации размера журнала событий факт доступа к файлу или каталогу не регистрируется.

4. Установите права дискреционного доступа для пользователей «user1» и «user2» в соответствии с матрицей доступа, приведенной в таблице 2.4.

Таблица 2.4. **Матрица доступа**

Пользователи	**Документы**		
	C:\Иванов\ Доклад.txt	C:\Иванова\ График.txt	C:\Общие\ План.txt
User1	rx	–	Полный доступ
User2	–	rx	Полный доступ

В таблице 2.4 используются следующие условные обозначения: r – чтение, w – запись/изменение, d – удаление, x – выполнение.

5. Для установки прав дискреционного доступа сделайте следующее:

– откройте диалоговое окно «Свойства» для папки, например, «C:\Иванов», и перейдите на вкладку Secret Net Studio. В разделе «Дискреционное управление доступом» снимите галочку в поле «Наследовать…». Откроется диалоговое окно «Разрешения для группы…»;

– используя кнопку «Добавить», добавьте пользователей «user1» и «user2» и установите им права доступа;

– нажмите кнопку «Применить». Поскольку «user1» и «user2» являются членами группы пользователей компьютера, появится сообщение Windows, предупреждающее, что заданная политика запрета приоритетна. Нажмите кнопку «Да». Доступ для папки «C:\Иванов» задан.

6. Настройте аудит для папки «Иванов» таким образом, чтобы регистрировались только события отказов в доступе. Для этого в окне «Разрешения для группы …» нажмите кнопку «Дополнительно». В открывшемся окне «Дополнительные параметры безопасности…» перейдите на вкладку «Аудит» и сделайте следующее:

– удалите аудит успеха, выбрав в таблице «Элементы аудита» запись «Успех» и нажав кнопку «Удалить»;

– добавьте аудит отказа для группы «Пользователи». Для этого нажмите кнопку «Добавить», выберите группу «Пользователи» и нажмите кнопку «ОК». Откроется следующее диалоговое окно «Элементы аудита для…»;

– в колонке «Отказ» установите флажки для всех действий и нажмите кнопку «ОК». Вы вернулись в окно «Дополнительные параметры безопасности…»;

– аудит для папки «Иванов» настроен. Нажмите кнопку «ОК».

7. В окне «Разрешения для группы…» нажмите кнопку «ОК». В окне свойств папки также нажмите кнопку «ОК».

8. Таким образом, мы установили параметры доступа к папке «C:\Иванов» и аудит событий в соответствии с таблицей из п. 4. Откройте папку «C:\Иванов», вызовите окно свойств файла «Доклад.txt», перейдите на вкладку «Secret Net Studio» и убедитесь, что установлен параметр «Наследовать настройки доступа от родительского объекта».

9. Используя описание пп. 4–7, установите в соответствии с матрицей разграничения доступа права доступа и настройку аудита событий для папок «Иванова» и «Общие».

10. На компьютере StartSNS завершите работу локальной программы управления и переавторизуйтесь под учетной записью «user1». Убедитесь, что пользователю «user1», согласно таблице в п. 4, доступны следующие действия с ресурсами: «C:\Иванова\График.txt» – чтение, «C:\Иванов\Доклад.txt» – чтение и выполнение и «C:\Общие\План.txt» – полный доступ.

11. Переавторизуйтесь под учетной записью «user2». Убедитесь, что пользователю «user2», согласно таблице в п. 4, доступны следующие действия с ресурсами: «C:\Иванова\График.txt» – чтение, запись и выполнение; «C:\Иванов\Доклад.txt» – доступ запрещен и «C:\Общие\План.txt» – чтение.

12. Проверить наличие записей в журнале аудита.

2.7 Управление отчуждаемыми носителями

Перед выполнением данной работы следует ознакомиться с главой 1 электронного документа «Руководство администратора. Настройка и эксплуатация. Локальная защита» разработанного в ООО «Код безопасности» [2].

1. На ВМ StartSNS авторизуйтесь под учетной записью администратора «adminsns».

Подключите к ВМ StartSNS USB-флеш-накопитель, который будет использоваться в лабораторной работе в рамках иллюстрации работы подсистемы контроля устройств.

2. Загрузите список устройств, просмотрите сведения о подключенном USB-флеш-накопителе и настройте политики его контроля. Для этого:

– в программе «Локальный центр управления» на панели свойств компьютера выберите в разделе «Политики» группу «Контроль устройств» и прокрутите содержимое окна к таблице «Устройства»;

– просмотрите список устройств. Обратите внимание, что в него автоматически добавлены все обнаруженные устройства компьютера. Отключенные в данный момент устройства отображаются с зачеркнутыми именами;

– в таблице «Устройства» выберите «Устройства USB / Устройства хранения/ <подключенное устройство>» и раскройте поле «Параметры контроля». Убедитесь, что параметр «Подключение устройства разрешено» установлен, а «Наследовать настройки контроля от родительского объекта» – нет. Текущее состояние устройства означает, что включен режим контроля, при котором устройство разрешается подключать к компьютеру и отключать. В случае изменения состояния устройства в журнале регистрируются соответствующие события. Утверждение изменений аппаратной конфигурации при этом не требуется:

– закройте поле «Параметры контроля» и справа от него нажмите кнопку «Разрешения». Откроется диалоговое окно «Разрешения…», которое позволяет задавать параметры доступа к этому

устройству. Следует иметь в виду, что настройка разрешений и запретов предусмотрена только для портов, дисков и носителей данных (для системного диска управление разрешениями запрещено);

– в список «Группы или пользователи» добавьте пользователя «user2» и установите ему запрет на работу с подключенным в данный момент (с именно этим) USB-флеш-накопителем;

– проведите настройку аудита событий работы с устройством, установив только аудит отказов. Для этого в диалоговом окне «Разрешения…» нажмите кнопку «Дополнительно» и выполните действия, аналогичные описанным в п. 5 предыдущей лабораторной работы;

– политики контроля подключенного USB-флеш-накопителя настроены. Последовательно закройте диалоговые окна «Дополнительные параметры безопасности…» и «Разрешения…» и вернитесь в окно программы управления к перечню параметров «Контроль устройств».

3. Установите запрет всем пользователям на использование незарегистрированных USB-флеш-накопителей (всех, кроме подключенного в настоящий момент). Для этого:

– в таблице «Устройства» выберите: «Устройства USB / Устройства хранения» и раскройте поле «Параметры контроля»;

– удалите отметку из поля «Наследовать настройки контроля от родительского объекта» и установите флажок «Подключение устройства запрещено». Нажмите кнопку «Применить»;

– на вкладке «Настройки» нажмите кнопку «Применить». Таким образом, мы запретили всем пользователям использовать незарегистрированные USB-флеш-накопители.

4. Для отслеживания произошедших событий, связанных с работой механизма разграничения доступа к устройствам, следует выполнить настройку регистрации событий. Справа от заголовка группы параметров «Устройства» нажмите кнопку–ссылку

«Аудит…». Вы переключитесь в раздел настроек «Регистрация событий / Контроль устройств». Используя кнопку, ознакомьтесь с текущим вариантом настроек и измените их на свое усмотрение.

5. На ВМ StartSNS закройте программу управления, переавторизуйтесь под учетной записью пользователя «user2» и сделайте попытку доступа к подключенному в данный момент зарегистрированному USB-флеш-накопителю. Убедитесь, что в доступе отказано.

6. На ВМ StartSNS переавторизуйтесь под учетной записью пользователя «user1» и сделайте попытку доступа к подключенному в данный момент зарегистрированному USB-флеш-накопителю. Убедитесь, что доступ разрешен.

7. Протестируйте возможность разграничения доступа к устройству с помощью механизма полномочного управления доступом, присвоив требуемую категорию конфиденциальности. Для этого:

– на ВМ StartSNS в программе «Локальный центр управления» на панели свойств компьютера выберите в разделе «Политики» группу параметров «Контроль устройств/ Устройства»;

– в таблице «Устройства» выберите «Устройства USB / Устройства хранения / <подключенное устройство>» и справа от него нажмите кнопку «Разрешения». В открывшемся диалоговом окне «Разрешения…» в списке «Группы или пользователи» удалите запрет на работу с подключенным в данный момент флеш-накопителем для пользователя «user2»;

– раскройте поле «Параметры доступа». Текущее значение «Без учета категории» означает, что устройство должно функционировать независимо от уровня допуска пользователя;

– выберите параметр «Секретно» и нажмите кнопку «Применить» В поле «Теневое копирование» установите флажок. Ознакомьтесь с появившимся над таблицей «Устройства» текстом предупреждения;

– на вкладке «Настройки» нажмите кнопку «Применить». Закройте программу управления и переавторизуйтесь под учетной записью пользователя «user2». Убедитесь, что в авторизации отказано, поскольку подключено устройство (USB-флеш-накопитель), к которому у пользователя отсутствует доступ, поскольку категория конфиденциальности устройства выше, чем у пользователя;

– отключите от ВМ StartSNS зарегистрированный USB-флеш-накопитель.

8. Подключите к ВМ StartSNS другой – незарегистрированный – USB-флеш-накопитель и убедитесь, что подсистема контроля устройств Secret Net Studio не позволяет работать с ним всем пользователям.

9. На ВМ StartSNS переавторизуйтесь под учетной записью «adminsns». Откройте журнал Secret Net Studio, просмотрите записи категории «Разграничение доступа к устройствам» с типом «Аудит отказов» о событиях запрета подключения к незарегистрированному USB-флеш-накопителю.

10. На ВМ StartSNS отмените все заданные ограничения на использование USB-флеш-накопителей.

2.8 Настройка маркировки и теневого копирования

Перед выполнением данной работы следует ознакомиться с главами 2-3 электронного документа «Руководство администратора. Настройка и эксплуатация. Локальная защита» разработанного в ООО «Код безопасности» [2].

1. Откройте консоль ВМ StartSNS и в окне программы ЦУ выберете «Контроль печати».

2. Настройте список принтеров. Для этого выберите вкладку «Настройки» и раскройте раздел Политики → Контроль печати.

Включите политику для принтера «Настройки по умолчанию». Убедитесь, что в графе «Категории конфиденциальности» по умолчанию указано «Любой категории».

Обратите внимание, что при необходимости в ячейке колонки «Разрешения»  могут устанавливаться права пользователей для печати документов для конкретных принтеров или для элемента «Настройки по умолчанию». Нажмите кнопку «Применить».

3. Настройте для принтеров функцию теневого копирования. Для этого:

– в разделе политик «Политики → Контроль печати» найдите пункт «Теневое копирование» и с помощью кнопки  внимательно ознакомьтесь с ее описанием;

– измените установленное по умолчанию значение на «Определяется настройками принтера»;

– нажмите кнопку «Применить».

4. Настройте для принтеров функцию маркировки документов. Для этого:

– в разделе политик «Политики → Контроль печати» найдите пункт «Маркировка документов» и с помощью кнопки  внимательно ознакомьтесь с описанием ее параметров;

– измените установленное по умолчанию значение на «Стандартная обработка» – этот режим может использоваться во всех поддерживаемых приложениях. В данном режиме предпочтительнее печатать документы целиком. При печати фрагмента документа маркер будет содержать сведения только о распечатанных страницах без учета общего количества страниц документа (так как распечатанный фрагмент воспринимается как отдельный документ);

– используя кнопку «Редактировать»  , ознакомьтесь с возможностью редактирования заданных грифов маркировки. Выберите краткий гриф для шаблона «Гриф №1», затем откройте вкладку

«Категории конфиденциальности» и проверьте галочки для необходимых типов документов;

– обратите внимание, что если в политике «Маркировка документов» выбран параметр «Расширенная обработка», то с помощью кнопки-ссылки «Приложения, включенные в расширенную обработку» можно управлять перечнем приложений, которые будут поддерживать маркировку печатаемых документов;

– нажмите кнопку «Применить».

5. Проверьте работу механизмов теневого копирования и маркировки документов при печати. Для этого на ВМ компьютера StartSNS под учетной записью «adminsns» создайте любой из документов, добавьте произвольное содержимое.

6. Выполните печать документа на установленном по умолчанию виртуальном принтере. В промежуточном диалоговом окне «Атрибуты документа» системы Secret Net Studio введите произвольный учетный номер, а затем сохраните с любым именем файл печати .xps.

7. Проверьте результат.

2.9 Настройка механизма замкнутой программной среды

Перед выполнением данной работы следует ознакомиться с главой 4 электронного документа «Руководство администратора. Настройка и эксплуатация. Локальная защита» разработанного в ООО «Код безопасности».

В данной лабораторной работе рассматривается создание замкнутой программной среды для пользователей в автономном и сетевом вариантах использования Secret Net Studio на примере организации возможности запуска только ограниченного набора программ: Проводник, MS Wordpad, MS Word, MS Excel, Internet Explorer, Корзина.

Модель ЗПС будет создаваться на основе данных журнала Secret Net Studio. В этом случае, чтобы собрать нужные сведения, пользователям разрешается запускать любые приложения. На это отводится некоторый период времени, и запуск приложений регистрируется в журнале. На время сбора сведений необходимо включить регистрацию всех событий категории «Замкнутая программная среда» на тех компьютерах, на которых ЗПС будет использоваться.

По окончании сбора сведений осуществляется формирование задач ЗПС в модели данных на основе сведений о запускаемых программах из журнала Secret Net Studio. Экспорт сведений в модель данных может выполняться непосредственно из локального журнала Secret Net Studio или из файла, в который предварительно были сохранены записи журнала.

Примечание. Источником при добавлении задач ЗПС по журналу в централизованном режиме является evtx- или snlog-файл, в который предварительно были экспортированы сведения из журнала.

1. В окне консоли BM StartSNS убедитесь, что вы авторизованы под учетной записью *adminsns*. В окне программы управления выберите панель «Компьютер» и на вкладке «Настройки» раскройте группу Политики → Локальная защита → Замкнутая программная среда.

2. Обратите внимание, что в Secret Net Studio используется одна привилегия, связанная с работой ЗПС – она определяет пользователей, для которых не действуют правила замкнутой программной среды. По умолчанию эта привилегия предоставлена локальной группе Администраторы.

Добавьте с помощью кнопки «Добавить ⊕» администратора adminsns в группу привилегированных пользователей, а затем сохраните внесенные в политики изменения, используя кнопку «Применить».

3. Для настройки механизма ЗПС запустите программу Контроль программ и данных: Пуск → Все программы → Код Безопасности → Secret Net Studio → Контроль программ и данных.

4. Для формирования новой модели данных в главном меню выберите опцию Файл → Новая модель данных. В открывшемся диалоговом окне «Настройка контроля по умолчанию» установите опции так, как показано на рисунке.

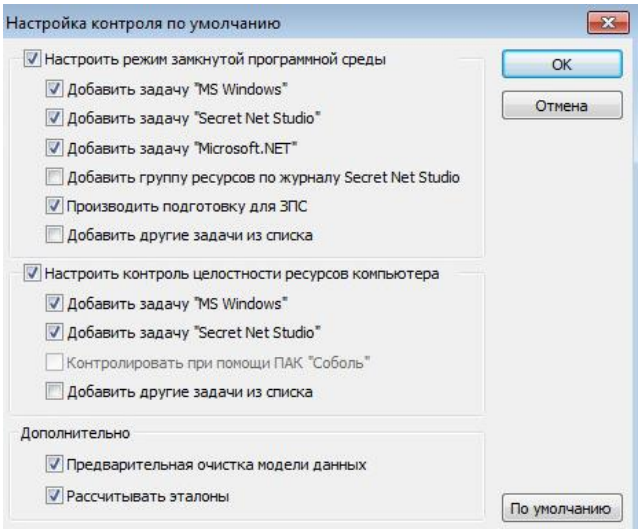

Рис. 2.2. Окно опция контроля по умолчанию

5. Нажмите кнопку «ОК». В диалоговом окне подтверждения нажмите кнопку «Да». Предыдущая модель данных будет удалена, и запустится процедура подготовки ресурсов для использования в ЗПС, по окончании которой автоматически запустится расчет эталонов для ресурсов. Дождитесь его завершения.

6. После успешного формирования модели данных в основном окне программы управления КЦ-ЗПС появится новая структура

объектов. Обратите внимание, что в ней уже содержится сформированное по умолчанию задание, включающее контроль ресурсов самой Secret Net Studio и ОС Windows. Создайте новое задание. Для этого в категории Субъекты управления вызовите контекстное меню вновь созданной структуры объектов BUILTIN → Пользователи и выберите опцию Добавить задание → Новое.

7. В открывшемся диалоговом окне введите название «ЗПС для пользователей» и нажмите кнопку ОК.

8. Убедитесь, что в окне Контроль программ и данных в структуре созданного ранее объекта появилась запись нового задания.

9. Для настройки механизма ЗПС на основе данных журнала Secret Net Studio включите мягкий режим работы ЗПС, в котором пользователю разрешается использовать любые программы. Если при этом запускаются программы, не входящие в перечень разрешенных, – в журнале Secret Net Studio регистрируются события аудита отказа. Это нужно для того, чтобы, не влияя на работу пользователей, в журнале накопить сведения о возможных ошибках, допущенных при настройке механизма ЗПС, и в последующем их устранить.

В жестком режиме разрешается запуск только тех программ, которые входят в список разрешенных, а запуск остальных блокируется, и в журнале Secret Net Studio регистрируются события тревоги.

Для включения мягкого режима выполните следующее:

– в окне «Контроль программ и данных» вызовите контекстное меню субъекта управления StartSNS и выберите опцию Свойства, в результате чего откроется диалоговое окно;

– переключитесь на вкладку «Режимы» и активируйте опции «Режим ЗПС включен» и «Мягкий режим»;

– нажмите кнопку «ОК», сохраните модель и перезагрузите ОС на ВМ StartSNS.

10. Авторизуйтесь на ВМ StartSNS под учетной записью adminsns и экспортируйте журнал Secret Net Studio во внешний файл, чтобы очистить его. Для этого:

– запустите программу управления в локальном режиме и в панели «Журналы» откройте журнал Secret Net Studio, вид которого представлен на рисунке 2.3;

– в правой части окна нажмите кнопку «Экспорт журнала» и выгрузите журнал Secret Net Studio в файл формата evtx с произвольным наименованием, установив параметр удаления записей при экспорте;

– убедитесь в том, что журнал очищен.

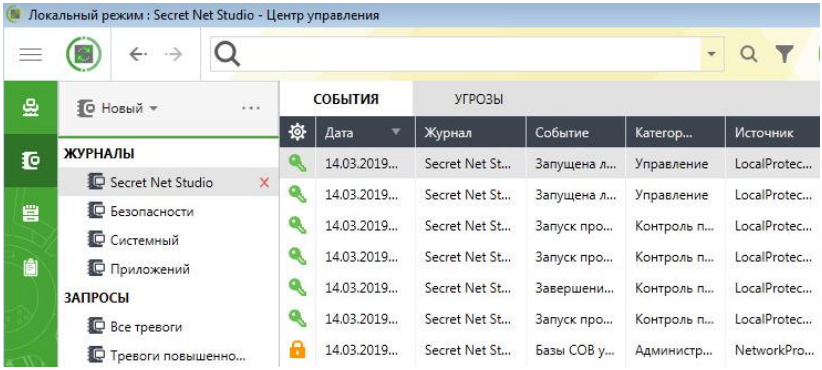

Рис. 2.3. Окно списка журналов

11. Перезагрузите ОС на ВМ StartSNS и авторизуйтесь под учетной записью user1 – Иванов Иван Иванович. Последовательно запустите все программы, которые будут разрешены в дальнейшем пользователям: Проводник, WordPad, MS Word, MS Excel, Internet Explorer, Корзина.

12. Переавторизуйтесь на ВМ StartSNS под учетной записью adminsns и откройте программу «Контроль программ и данных».

13. К созданному ранее заданию ЗПС добавьте задачи на основании данных из журнала Secret Net Studio. Для этого:

– выделите запись созданного вами ранее задания ЗПС для пользователей и в контекстном меню выберите опцию Добавить задачи/группы → Новую группу по журналу;

– в открывшемся диалоговом окне убедитесь в том, что выбран переключатель Загружаемые модули и нажмите кнопку «ОК».

14. В диалоговом окне Создание группы по журналу установите параметры:

– Способ: «Из журнала Secret Net Studio»;

– в поле «Пользователь» нажмите кнопку «Найти» и выберите user1;

– в поле «Отчетный период» укажите период запуска разрешенных программ для user1. Поскольку журнал Secret Net Studio был предварительно очищен, поле «Отчетный период» можно оставить без изменения (рис. 2.4).

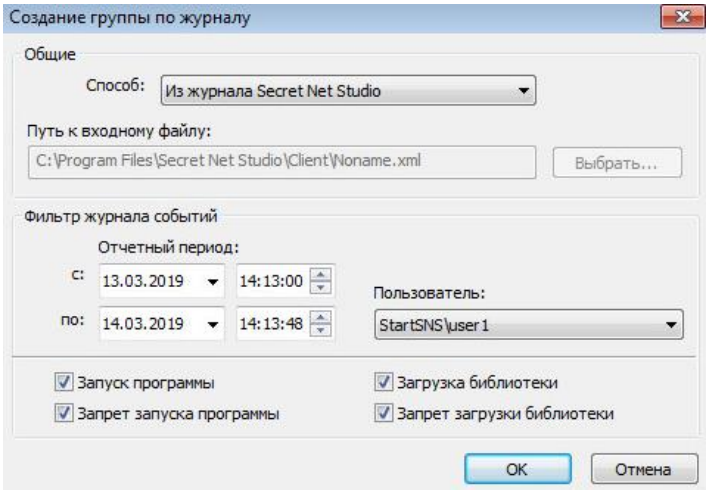

Рис. 2.4. Настройки создания группы на основе журналов

15. Нажмите кнопку «ОК» и сохраните сделанные изменения в модели данных.

16. Установите запрет обмена данными для приложения WordPad с другими процессами, настроив изоляцию процессов. Для этого:

– в окне «Контроль программ и данных» в категории «Субъекты управления» вызовите контекстное меню компьютера StartSNS и выберите опцию «Свойства», в результате чего откроется диалоговое окно;

– переключитесь на вкладку «Режимы» и активируйте пункт «Изоляция процессов включена». Обратите внимание, что механизм изоляции процессов может быть включен независимо от ЗПС;

– нажмите кнопку «ОК». Режим изоляции процессов начнет действовать для выбранного компьютера;

– включите изоляцию для ресурса WordPad. Для этого в окне «Контроль программ и данных» выберите категорию Ресурсы и раскройте ветку Файлы и каталоги / C: / Program files / Windows NT / Accessories. Вызовите контекстное меню файла wordpad.exe и выберите опцию «Свойства», в результате чего откроется диалоговое окно;

– в диалоговом окне «Свойства ресурса» нажмите кнопку «Дополнительно». В следующем открывшемся окне установите отметку в поле «Изолировать процесс»;

– в окнах «Дополнительные свойства приложения» и «Свойства ресурса» нажмите кнопку «ОК». Изоляция для ресурса WordPad включена, и теперь обмен данными между WordPad и другими процессами будет невозможен.

17. Включите жесткий режим для ЗПС. Для этого:

– в окне «Контроль программ и данных» вызовите контекстное меню субъекта управления StartSNS и выберите опцию «Свойства»;

– в открывшемся диалоговом окне переключитесь на вкладку «Режимы» и снимите отметку в поле «Мягкий режим»;

– нажмите кнопку ОК и сохраните модель данных.

18. Переавторизуйтесь на ВМ StartSNS под учетной записью *user1* и убедитесь, что пользователь может запускать только ограниченный набор программ: Проводник, WordPad, MS Word, MS Excel, Internet Explorer, Корзина. Попытки запуска других программ, например, Paint, блокируются.

19. Убедитесь, что для приложения WordPad работает механизм изоляции процессов и копирование любых данных из окна WordPad в другие приложения невозможно.

20. Переавторизуйтесь на ВМ StartSNS под учетной записью user2 и убедитесь, что ЗПС работает и для этого пользователя тоже.

21. Переавторизуйтесь на ВМ StartSNS под учетной записью adminsns, в программе управления откройте журнал Secret Net Studio и просмотрите записи категорий Замкнутая программная среда и Изоляция процессов с типом Аудит отказов.

22. Откройте программу Контроль программ и данных, отключите механизмы ЗПС и изоляции процессов, сохраните изменения и перезагрузите ВМ StartSNS.

Контрольные вопросы по разделу 2

1. Перечислите состав мер по обеспечению контроля целостности, представленные в данной лабораторной работе.

2. Что подразумевается под обеспечением целостности информации? Что представляет собой механизм контроля целостности?

3. Что представляет собой механизм полномочного управления доступом?

4. Что представляет собой механизм дискреционного управления доступом?

5. Для чего нужен механизм контроля устройств и от каких угроз он защищает?

3 ЗАЩИТА АРМ СРЕДСТВАМИ ОС ASTRA LINUX SE

3.1 Общая характеристика системы

Astra Linux Special Edition – операционная система, предназначенная для построения автоматизированных систем в защищенном исполнении, обрабатывающих информацию, содержащую сведения, составляющие государственную тайну с грифом не выше «совершенно секретно».

Система применяется в ряде государственных учреждений в сферах обороны, здравоохранения, науки и образования, финансов, промышленности и торговли, ЖКХ. В частности, на ней построена информационная система Национального центра управления обороной РФ.

Операционная система Astra Linux Special Edition основана на дистрибутиве Astra Linux Common Edition и включает в себя ряд принципиальных доработок для обеспечения соответствия требованиям руководящих документов по защите информации. Кроме того, в целях оптимизации, из дистрибутива Astra Linux Special Edition исключён ряд дублирующих друг друга компонент, решающих сходные целевые задачи.

Комплекс средств защиты (КСЗ) Astra Linux SE (подсистема безопасности PARSEC) предназначен для реализации функций ОС по защите информации от НСД и предоставления администратору безопасности информации средств управления функционированием КСЗ.

В состав КСЗ входят следующие основные подсистемы:

– модули подсистемы безопасности PARSEC, входящие в состав ядра ОС;

– библиотеки;

– утилиты безопасности;

– подсистема протоколирования (регистрации);

– модули аутентификации;

– графическая подсистема;

– консольный вход в систему;

– средства контроля целостности;

– средства восстановления;

– средства разграничения доступа к подключаемым устройствам.

3.2 Защитные функции

КСЗ обеспечивает реализацию следующих функций по защите информации от НСД:

1) идентификацию и аутентификацию;
2) дискреционное разграничение доступа;
3) мандатное разграничение доступа;
4) регламентный контроль целостности;
5) контроль целостности КСЗ;
6) блокировка макросов и других нежелательных системных функций.

1. Идентификация и аутентификация. Основывается на использовании механизма PAM (Pluggable Authentication Modules). PAM представляют собой набор «модулей» (разделяемых библиотек), с помощью которых системный администратор может организовать процедуру аутентификации (подтверждение подлинности) пользователей прикладными программами. Каждый модуль реализует собственный механизм аутентификации. Изменяя набор и порядок следования модулей, можно построить сценарий аутентификации. На рисунке 3.1 представлена общая схема работы PAM.

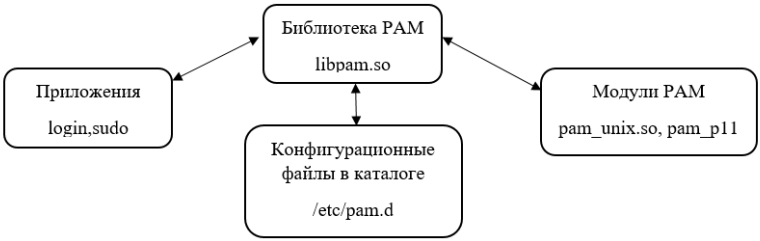

Рис. 3.1. Общая схема работы PAM

2. Дискреционное разграничение доступа. Отправной точкой реализации управления доступом в Astra Linux SE являлось унаследованное от ОС семейства Linux дискреционное управление доступом. Поэтому, несмотря на то, что в настоящее время в Astra Linux SE используются мандатные управление доступом и контроль целостности, а в перспективе ролевое управление доступом, целесообразно рассмотреть основные элементы дискреционного управления доступом, не утратившие своей актуальности в современных релизах Astra Linux SE.

Дискреционное управление доступом в ОС семейства Linux базируется на понятии владения (использовании права доступа владения) файлом, каталогом, процессом (сущностями и субъект-сессиями). Так в файловых системах семейства extfs, которые по умолчанию используются в Astra Linux SE, для каждого файла или каталога обязательно задана учётная запись пользователя – их владелец. Процесс, функционирующий от имени такой учётной записи-владельца сущности, имеет право изменять дискреционные права доступа к ней, например назначать их учётным записям других пользователей Astra Linux SE на основе стандарта POSIX ACL.

Access Control List или ACL – список контроля доступа, который определяет, кто или что может получать доступ к конкретному объекту, и какие именно операции разрешено или запрещено этому

субъекту проводить над объектом. Списки контроля доступа являются основой систем с избирательным управлением доступа.

Для оптимизации и облегчения администрирования дискреционного управления доступом в случаях, когда к одним и тем же файлам или каталогам требуется установить одинаковые права доступа более чем для одной учётной записи пользователя, в Astra Linux SE применяются группы учётных записей пользователей. В результате для файлов и каталогов владельцем (обладателем к ним правом доступа владения) может быть задана группа. При этом для них остаются владельцами и соответствующие учётные записи пользователей. В перспективе при реализации в Astra Linux SE ролевого управления доступом вместо учётных записей пользователей и групп владельцами будут задаваться роли или административные роли.

3. Мандатное разграничение доступа. Реализация мандатного управления доступом в Astra Linux SE основана на подсистеме безопасности PARSEC, самостоятельно разработанной ОАО «НПО «РусБИТех» и включающей соответствующие программный интерфейс и модуль расширения ядра Astra Linux, поддерживающий виртуальную файловую систему /parsecfs, и набор системных вызовов, позволяющих уполномоченным пользователям управлять политикой безопасности Astra.

Другими словами, Parsec – это такой монитор обращений, который контролирует и определяет какой из категорий, какому файлу можно получить доступ. По сколько решение предоставления доступа принимается именно Parsec, а не пользователем, как в случае с дискреционным разграничением, то этот вид доступа называют принудительным контролем доступа.

Помимо мандатного управления доступом, подсистема безопасности PARSEC также реализует мандатный контроль целостности и дополнительные функции аудита. На рисунке 3.2 показано место

подсистемы безопасности PARSEC в архитектуре Astra Linux и порядок её взаимодействия с другими компонентами ОССН.

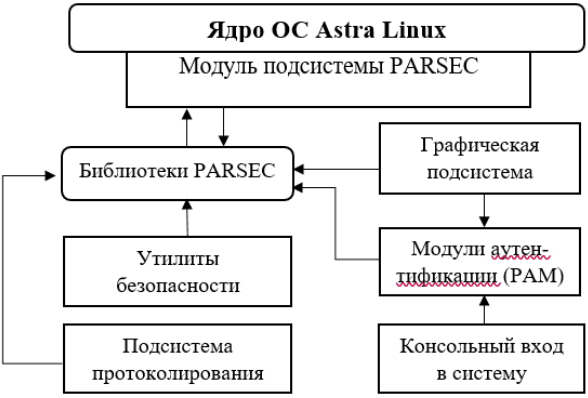

Рис. 3.2. Архитектура подсистемы защиты Astra Linux

Модуль PARSEC устанавливает в ядре ОССН собственные обработчики контролируемых информационных потоков, которые получают управление всякий раз, когда необходимо принять решение, следует ли разрешить или запретить то или иное обращение субъекта к сущности. Эти обработчики функционируют автономно, непосредственное взаимодействие модуля PARSEC с другими компонентами подсистемы защиты происходит лишь в тех случаях, когда клиентская программа получает информацию о действующей политике безопасности или модифицирует эту политику. Рисунок 3.3 иллюстрирует внутреннюю архитектуру модуля PARSEC. Подсистема MAC – подсистема Mandatory Access Control.

Плюсы мандатного разграничения доступа: многократно снижается риск утеки данных в результате ошибки пользователя в плане назначения дискреционных прав. Пользователь не может полностью управлять доступом к ресурсам, которые он создает.

Если пользователь создал файл в папке, файл унаследует определённую метку конфиденциальности.

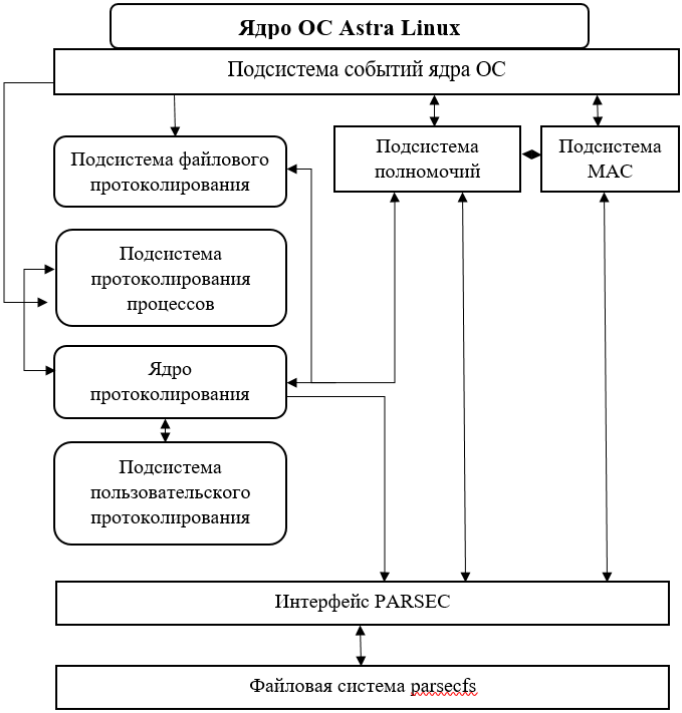

Рис. 3.3. Внутренняя архитектура модуля PARSEC

Доступ к этому ресурсу на основе только дискреционных прав доступа уже получить нельзя. Также происходит запрет пользователю или процессу получать доступ к информации и устройствам более защищённого уровня. Пользователь с меткой несекретно не получит доступ к информации особой важности.

Существует еще одна задача – защита приложений при помощи принудительных мер контроля, когда решение о том, кто имеет право вносить изменения в настройку приложений, конфигураци-

онных файлов, принимает монитор обращений PARSEC. Для решения этой задачи в Astra Linux SE была введена технология мандатного контроля целостности. Данная технология решает такие вопросы, как права на изменение приложений, доступ к ним, изменение конфигураций приложения, опций настроек. И как раз занимается этим монитор обращений PARSEC.

Основой реализованных в Astra Linux SE мандатных управления доступом и контроля целостности является иерархическая МРОСЛ ДП-модель, вид которой показан на рисунке 3.4.

Рис. 3.4. Иерархическая МРОСЛ ДП-модель

Указанная модель включает в себя четыре уровня:

– первый уровень (базовый): модель системы ролевого управление доступом (1.1);

– второй уровень: модель системы ролевого управление доступом и мандатного контроля целостности (2.1);

– третий уровень: модель системы ролевого управление доступом, мандатного контроля целостности и мандатного управления доступом только с информационными потоками по памяти (3.1);

– четвертый уровень: модель системы ролевого управление доступом, мандатного контроля целостности и мандатного управления доступом с информационными потоками по памяти и по времени (4.1).

Подробное описание модели приведено в [3].

4. Регламентный контроль целостности. Организация регламентного контроля целостности ОС, прикладного ПО и СЗИ обеспечивается набором программных средств на основе «Another File Integrity Checker». Регламентный контроль целостности использует для своей работы базу хэшей файлов, таким образом есть возможность по расписанию сверять хэши файлов с этой базой. Если в файле есть отличие, то при сравнении хэша этого файла оно будет найдено.

Дополнительным элементом защиты является полная поддержка технологии аппаратного контроля исполняемого пространства No Execute Bit (NX–bit) для предотвращения выполняемого произвольного кода. Эта защита реализована на уровне процессора. После включения этой опции становится невозможным создания в системе файлов и скриптов с битом исполнения.

5. Очистка памяти. Ядро ОС гарантирует, что обычный непривилегированный процесс не получит данные чужого процесса, если это явно не разрешено правилами разграничения доступа (ПРД). Это означает, что средства IPC контролируются с помощью ПРД, и процесс не может получить неочищенную память (как оперативную, так и дисковую).

Есть дополнительные возможности по очистке остаточной информации, представленные ядром с усиленной защитой HARDENED. А именно: очистка остаточной информации в ядерном стеке (STACKLEAK) и очистка остаточной информации в ядерной куче (PAGE_POISONING).

Очистка осуществляется посредством перезаписи каждого байта в освобождаемой области посредством четырех сигнатур следующего вида: 11111111, 01010101, 10101010, 00000000. Использование режима включается параметром secdel в конфигурационном файле /etc/fstab для раздела ФС, на котором требуется очищать блоки памяти при их освобождении (например, /dev/sda1). В список параметров монтирования добавляется параметр secdel. Количество перезаписей определяется администратором. Использование режима включается установкой значения параметра secdel в конфигурационном файле /etc/fstab для раздела ФС, на котором требуется очищать блоки памяти при их освобождении. При установке числа перезаписей больше четырех сигнатуры используются повторно.

Перейдем к очистке разделов подкачки. Чем же опасно попадание данных в разделы подкачки, если мы не можем их защитить. В ОС область подкачки может быть и не быть. Наличие области подкачки является важной составляющей ОС управления памятью. Эта область необходима для нормального функционирования системы. Основным назначением области подкачки в Astra Linux является обеспечение эффективного освобождения и балансировка имеющейся памяти. Существуют разные типы страниц оперативной памяти, но для понимания нужности подкачки существенны 2 типа:

1) страницы, содержимое которых можно восстановить, повторно прочитав содержимое из файлов (страницы с командами, исполняемых процессов, кэши файловых данных);

2) страницы данных распределения памяти между процессами, так называемые анонимы страницы, не имеющие исходных файлов.

Основное назначение области подкачки – это освобождать в оперативной памяти место для файлового кэша за счет выгрузки неактуальных анонимных страницы.

Дополнительно область подкачки используется для режимов сна (режим гибернации). При входе в такие режимы в область подкачки сохраняется полная копия оперативной памяти. Страницы памяти, которые динамически копируются из оперативной памяти в область подкачки в процессе работы компьютера, могут содержать конфиденциальную информацию, не закрытую какими–либо защитными преобразованиями.

Таким образом наличие доступа на чтение к области подкачки создают угрозу утечки конфиденциальной информации. Отдельную проблему с точки зрения безопасности представляет собой хранение в области подкачки содержимого оперативной памяти выключенных компьютеров. Копия содержимого оперативной памяти может оставаться в области подкачки при неожиданном выключении компьютера в результате аппаратного сбоя, при неожиданном отключении электропитания и всегда остается в этой области в компьютерах, находящихся в режиме гибернации. При наличии физического доступа к оборудованию такие данные можно прочитать независимо от дискреционных и мандатных ограничений.

3.3 Настройка идентификации и аутентификации

Перед выполнением практических заданий следует ознакомиться с главой 3 в учебного пособия [3].

Настройка и проверка политик подсистемы будет демонстрироваться на учетной записи *user*.

1. Настроить политику блокировки учетной записи, со следующими параметрами:

– период блокировки 4 секунды;

– период разблокировки 900 секунд.

В результате окно настройки параметров будет выглядеть так, как показано на рисунке 3.5.

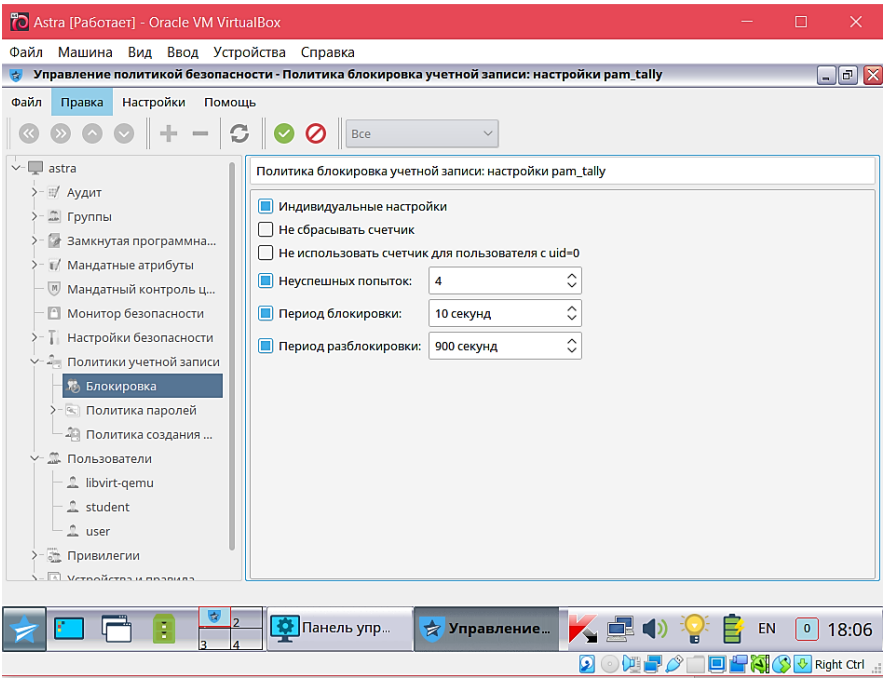

Рис. 3.5. Окно политики блокировки учетной записи

2. Настроить политику парольной защиты, со следующими параметрами:

– минимальная длина пароля – 8;

– минимальное количество строчных букв в новом пароле – 2;

– минимальное количество заглавных букв в новом пароле – 2;

– минимальное количество цифр в новом пароле – 1;

– минимальное количество других символов в новом пароле – 4.

3. Проверить работоспособность политики блокировки учетной записи. Для этого следует несколько раз ввести неправильный пароль и убедиться, что учетная запись заблокирована.

4. Проверить работоспособность политики парольной защиты. Для этого следует произвести попытку для учетной записи user задать пароль, не соответствующий требованиям п.2. Убедиться, что выведено сообщение об ошибке.

3.4 Настройка разграничения доступа

1. Создать новую папку. Для пользователя user настроить дискреционный доступ к папке так, как показано на рисунке 3.6.

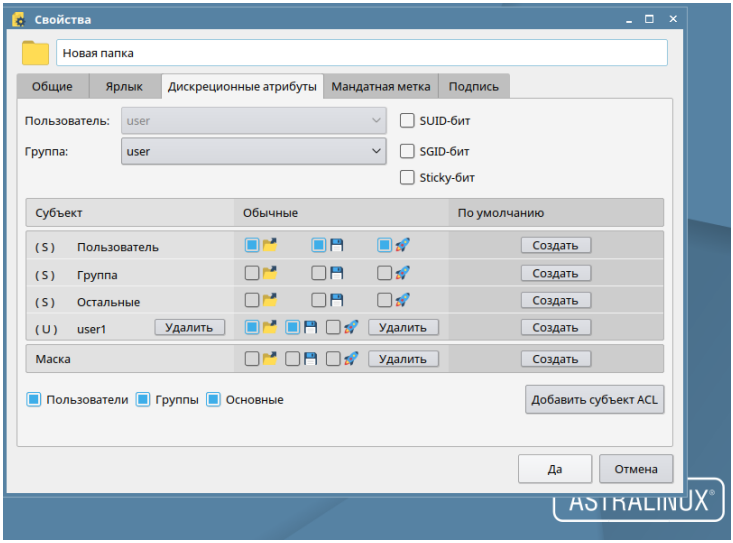

Рис. 3.6. Права дискреционного доступа для пользователя user

2. Настроить мандатное разграничение доступа (МРД). МРД содержит мандатный контроль целостности и конфиденциальности.

Выполнить настройку уровней целостности и конфиденциальности для пользователей student и user так, как представлено на рисунке 3.7.

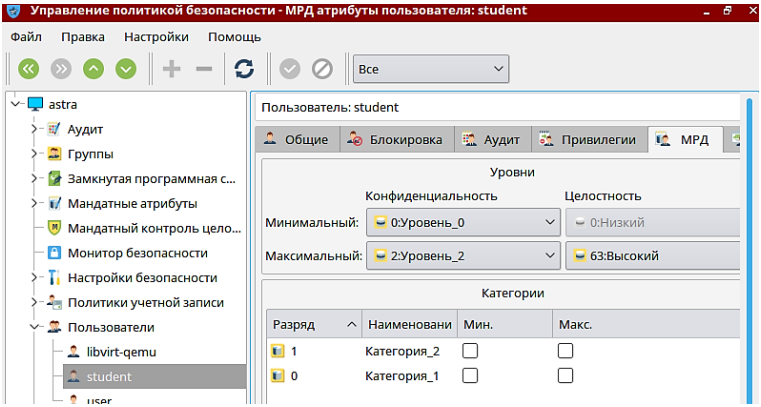

Рис. 3.7. Настройка уровней целостности
и конфиденциальности пользователя student

3. Проверку работоспособности мандатного разграничения доступа выполнить путём реализации попытки доступа пользователя с низким уровнем конфиденциальности к папке с более высоким уровнем конфиденциальности.

Для этого следует выполнить следующие действия:

1) авторизоваться в системе пользователем *student* с меткой конфиденциальности «Уровень 2»;
2) создать файл с названием «Секретные пароли» и добавить в него некую информацию;
3) авторизоваться пользователем *student* с низким уровнем конфиденциальности – «Уровень 0»;
4) убедиться, что файла «Секретные пароли» для пользователя с уровнем «Уровень 0» не существует.

3.5 Настройка регламентного контроля целостности

Контроль целостности будет продемонстрирован с помощью стандартной утилиты *afic*. Указанная утилита создает базу данных, содержащую хэши для любых файлов. Файлы и каталоги, включенные в эту базу данных, выбираются соответственно входным данным из файла конфигурации *afick*, называемого afick.conf, после того, как *afick* установит этот файл в /etc каталог.

Во время инсталляции программы задача проверки целостности добавляется в планировщик автоматически и запускается один раз в день. Чтобы осуществить внеплановый контроль целостности, нужно запустить утилиту вручную. Для изучения работы утилиты контроля целостности следует выполнить перечисленные ниже действия.

1. В домашнем каталоге создать новую папку и разместить в ней любой файл.

2. Запустить утилиту *afick*, чтобы она обновила базу данных хэшей.

3. Удалить созданный ранее файл и повторно запустить утилиту *afick*.

4. Убедиться, что в окне утилиты отображено сделанное изменение, так, как показано на рисунке 3.8.

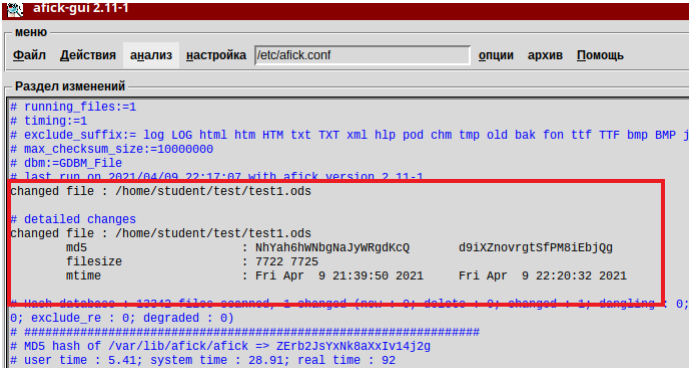

Рис. 3.8. Фрагмент окна утилиты контроля целостности

3.6 Активация системных блокировок

Важным шагом в настройке механизмов защиты информации в Astra Linux SE является включение блокировок. В данном разделе будут рассмотрены следующие блокировки:

– макросов офисных пакетов;

– трассировщика процессов;

– повышения уровня конфиденциальности в пределах одной сессии.

Макрос – сохраненная последовательность команд или нажатий клавиши, которые предназначены для использования в будущем. Другими словами, это программа, которая встраивается в документы и шаблоны офисных пакетов, например, в LibreOffice. Основная цель макросов – повышение удобства подготовки документов, снижение затрат времени за счёт программного выполнения повторяющихся рутинных операций. Макрос распространяется вместе с документом, поэтому сторонним пользователям документа не требуется дополнительная установка какого-либо программного обеспечения для работы с документом.

Отрицательной стороной макросов является возможность выполнения вредоносного кода в теле макроса. Кроме этого, пакет LibreOffice имеет право запускать программный код, написанный на языке Pyton. Это обстоятельство дополняется тем, что вредоносный код в макросе распространяется вместе с кажущимся безобидным документом, который сам по себе не является исполняемым файлом.

Однако, полный отказ от макросов является неправильным решением, поскольку лишит пользователя указанных выше удобств и снизит производительность труда. Поэтому, при включенной блокировке, разрешается выполнение макросов из специальной папки,

для которой задан высокий уровень контроля целостности, запрет на изменение и приняты другие защитные меры.

1. Указать папку, из которой LibreOffice будет разрешен запуск макросов. Для этого следует открыть LibreOffice и перейти в окно Сервис → Параметры → Безопасность → Доверенные источники. Добавить путь к папке в список доверенных источников.

2. Включить блокировку макросов. Для этого следует выполнить переход Панель управления → Безопасность → Управление политикой безопасности → Настройки безопасности → Системные параметры и активизировать опцию Блокировка макросов. Вид окна, в котором находятся опции системных блокировок показан на рисунке 3.9.

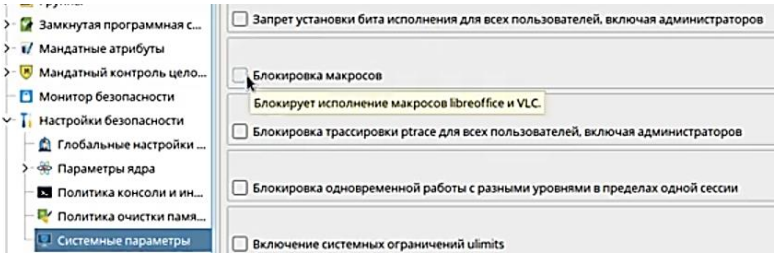

Рис. 3.9. Окно блокировки макросов

Следующим шагом является блокировка трассировщика процессов *ptrace*. *Ptrace* – это системный вызов, который дает возможность одному процессу управлять исполнением другого. Он так же имеет доступ к содержимому памяти трассируемого процесса, что даёт возможность утечки информации.

3. Включить блокировку *ptrace*. Для этого следует перейти к оснастке, указанной в предыдущем пункте и активизировать опцию Блокировка трассировки *ptrace* для всех пользователей, включая администраторов (рис. 3.9).

Операционная система Linux предоставляет возможность запуска с более высоким уровнем конфиденциальности во время сессии пользователя с низким уровнем конфиденциальности. Администратор системы может выдать соответствующую привилегию некоторым пользователям. Это создаёт потенциальную возможность утечки информации, поэтому указанную опцию следует заблокировать средствами Astra Linux для всех пользователей, вследствие чего запуск процессов с другим уровнем конфиденциальности будет невозможен даже при наличии соответствующей привилегии.

4. Для упрощения понимания дальнейших действий зададим названия уровням мандатного доступа – ДСП и Секретно. Для это следует выполнить переход Панель управления → Безопасность → Управление политикой безопасности → Мандатные атрибуты → Уровни конфиденциальности. Переименовать «Уровень_1» в «ДСП», «Уровень_2» в «Секретно».

5. Выдать пользователю *user* привилегию запуска процессов с разным уровнем конфиденциальности. Для этого следует выполнить переход Панель управления → Безопасность → Управление политикой безопасности → Пользователи → User и перейти на вкладку Привилегии. Активизировать опцию *parsec_cap_sumac*, как показано на рисунке 3.10.

Рис. 3.10. Фрагмент окна «Панели управления» вкладки выдачи привилегии пользователю

6. Задать пользователю *user* минимальный уровень конфиденциальности – «Уровень_0», максимальный – «Секретно». Указанные параметры задаются на вкладке МРД этого же окна, как показано на рисунке 3.11.

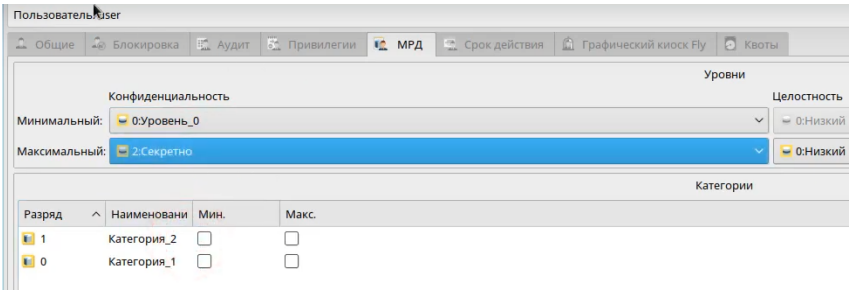

Рис. 3.11. Фрагмент окна выдачи привилегии пользователю

7. Убедиться, что пользователю user доступен запуск процессов с разными уровнями конфиденциальности. Для этого следует войти в систему под учетной записью user с уровнем конфиденциальности ДСП. Вызвать утилиту «Выполнить команду» и проверить, что в появившемся окне доступна опция запуска процесса с другим мандатным уровнем, как показано на рисунке 3.11.

8. Запустить любое приложение с уровнем конфиденциальности «Секретно», например, графический редактор GIMP.

9. В графическом редакторе создать и сохранить на диске новое изображение.

10. Открыть папку, в которой сохранено изображение и убедиться, оно не отображается в окне, поскольку текущий уровень конфиденциальности «ДСП», а графический редактор был запущен с уровнем конфиденциальности «Секретно».

11. Выполнить переход Панель управления → Безопасность → Управление политикой безопасности → Настройки безопасности →

Системные параметры и активизировать опцию блокировки одновременной работы с разными уровнями конфиденциальности (рис. 3.12).

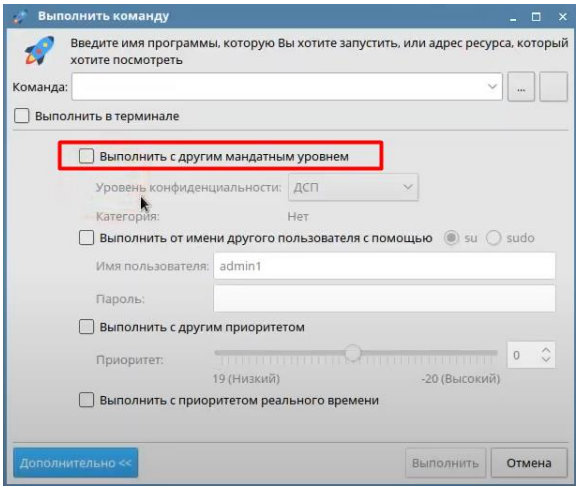

Рис. 3.12. Фрагмент окна утилиты «Выполнить команду»

12. Вызвать утилиту «Выполнить команду» и убедиться, что опция запуска приложения с другим уровнем конфиденциальности заблокирована.

В завершение рассмотрения вопросов настройки системных блокировок следует упомянуть о блокировке, включенной по умолчанию. Речь идёт о блокировке кнопки *SysRq*, полное название которой – *System Request*.

В операционных системах семейства *Linux* указанная кнопка имеет прямую связь с ядром системы и используется для вызова различных низкоуровневых функций, таких как перезагрузка графического интерфейса, остановка всех процессов, размонтирование файловых систем и многое другое. Однако, в защищенной автома-

тизированной системе вызов низкоуровневых функций, в обход защитных механизмов, может создать угрозу безопасности информации.

13. Убедиться, что блокировка кнопки *SysRq* включена. Для этого следует выполнить переход Панель управления → Безопасность → Управление политикой безопасности → Настройки безопасности → Системные параметры и проверить активизацию опции соответствующей блокировки.

3.7 Настройка замкнутой программной среды

Работа механизма ЗПС в Astra Linux SE основана на использовании электронно-цифровой подписи. Это означает, что при включенном режиме ЗПС разрешен запуск только тех программ, которые имеют цифровую подпись. Запуск любого стороннего программного обеспечения, не имеющего цифровую подпись, будет блокироваться. Этот механизм позволяет эффективно противодействовать запуску вредоносного программного обеспечение, которое попало на защищаемую автоматизированную систему в обход других мер защиты.

Механизм контроля целостности исполняемых файлов и разделяемых библиотек формата ELF при запуске программы на выполнение реализован в модуле ядра ОС digsig_verif, который является не выгружаемым модулем ядра Linux и может функционировать в одном из следующих режимов: 1) исполняемым файлам и разделяемым библиотекам с неверной ЭП, а также без ЭП загрузка на исполнение запрещается (штатный режим функционирования); 2) исполняемым файлам и разделяемым библиотекам с неверной ЭП, а также без ЭП загрузка на исполнение разрешается, при этом выдается сообщение об ошибке проверки ЭП (режим для проверки ЭП в

СПО); 3) ЭП при загрузке исполняемых файлов и разделяемых библиотек не проверяется (отладочный режим для тестирования СПО).

Механизм контроля целостности файлов при их открытии на основе ЭП в расширенных атрибутах файловой системы также реализован в модуле ядра ОС *digsig_verif* и может функционировать в одном из следующих режимов: 1) запрещается открытие файлов, поставленных на контроль, с неверной ЭП или без ЭП; 2) открытие файлов, поставленных на контроль, с неверной ЭП или без ЭП разрешается, при этом выдается сообщение об ошибке проверки ЭП (режим для проверки ЭП в расширенных атрибутах файловой системы); 3) ЭП при открытии файлов не проверяется.

Применение режима ЗПС эффективно в тех случаях, когда состав пользовательского программного обеспечения или не меняется совсем или меняется очень редко. При частом изменении пользовательского программного обеспечения возрастают операционные затраты на администрирование системы.

1. Работу механизма ЗПС рассмотрим на примере игры «Сапёр», входящей в дистрибутив Astra Linux SE. Необходимо открыть свойства файла *kmines* и убедиться в наличии электронной подписи в поле «Подпись» (рис. 3.13).

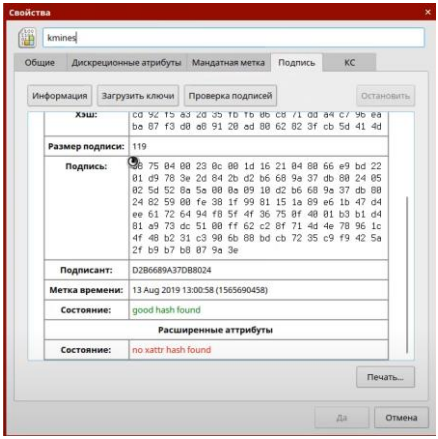

Рис. 3.13. Окно свойств подписанного файла

Файлы, входящие в состав Astra Linux SE подписаны ЭП ООО «РусБИТех-Астра». Для того, чтобы подписать стороннее ПО, следует получить собственные ключи у производителя системы, оформив соответствующий запрос. Подробности можно узнать на сайте производителя.

2. Получить у лаборанта сторонний файл *kmines* и убедиться, что у него отсутствует подпись.

3. Запустить подписанный и неподписанный файлы kmines и убедиться, что их запуск не блокируется.

4. Включить режим ЗПС. Для этого выполнить переход Панель управления → Безопасность → Управление политикой безопасности → Замкнутая программная среда. Включить режим ЗПС, активировав соответствующие опции в разделах «Контроль исполняемых файлов» и «Контроль атрибутов».

5. Перезагрузить систему, запустить подписанный и неподписанный файлы *kmines*. Убедиться, что запуск подписанного файла не блокируется, подписанного – блокируется с отображением соответствующего сообщения.

Контрольные вопросы по разделу 3

1. Какие параметры входя в состав политики парольной защиты?

2. Объясните принцип работы утилиты контроля целостности.

3. Обоснуйте необходимость использования блокировки макросов. Запуск каких макросов разрешен при включенной блокировке макросов?

4. Обоснуйте необходимость блокировки трассировки процессов.

5. При каких условиях возможен запуск процессов с разным уровнем конфиденциальности? Чем обоснована блокировка вызова функции *System Request*?

6. На каком принципе основана работа механизма замкнутой программной среды? Каким образом можно обеспечить работу стороннего программного обеспечения при включенном режиме замкнутой программной среды?

ЗАКЛЮЧЕНИЕ

В учебном пособии проведено первоначальное знакомство с основными механизмами защиты информации в широко применяемых на сегодняшний день программно-аппаратных средствах. Полученные знания являются хорошей основой для дальнейшего самостоятельного и более глубокого изучения возможностей программных продуктов.

Необходимо понимать, что на сегодняшний день происходит постоянное развитие информационных технологий и аппаратной платформы автоматизированных систем, ширится номенклатура системного и прикладного программного обеспечения. Вместе с этим появляются новые виды уязвимостей и способов реализации компьютерных атак. Это обстоятельство определяет дальнейшее развитие и средств защиты информации.

Следует отметить, что производители средств защиты, которые рассмотрены в данной работе, имеют различные программы содействия углубленному изучению. В частности, в целях дальнейшего совершенствования навыков работы с механизмами защиты, вендоры предлагают участие в программах сертификации специалистов, по результатам прохождения которых выдаются официальные фирменные сертификаты.

СПИСОК ЛИТЕРАТУРЫ

1. База знаний Dallas Lock. URL https://dallaslock.ru/products/faq/szi-dallas-lock-8-0/

2. Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Локальная защита // ООО «Код безопасности» [Сайт]. Систем. требования: Adobe Acrobat Reader. URL: https://www.securitycode.ru/products/secret-net-studio/?tab=support

3. Буренин П.В., Девянин П.Н., Лебеденко Е.В., Проскурин В.Г., Цибуля А.Н. Безопасность операционной системы специального назначения Astra Linux Special Edition. 3-е изд., перераб. и доп. М.: Горячая линия – Телеком, 2019. 404 с.

Учебное издание

Жмуров Денис Борисович,
Жуков Семен Викторович

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Учебное пособие

Редакционно-издательская обработка А.В. Ярославцевой

Подписано в печать 27.10.2022. Формат 60×84 1/16.
Бумага офсетная. Печ. л. 5,0.
Тираж 25 экз. Заказ № . Арт. – 15(Р2УП)/2021.

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САМАРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА С.П. КОРОЛЕВА» (САМАРСКИЙ УНИВЕРСИТЕТ)
443086, Самара, Московское шоссе, 34.

Издательство Самарского университета.
443086, Самара, Московское шоссе, 34.