DOI 10.37882/2223-2966.2024.02.15

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В ОПЕРАЦИОННОЙ СИСТЕМЕ ASTRALINUX

ENSURING INFORMATION PROTECTION IN THE ASTRA LINUX OPERATING SYSTEM

S. Danilyuk
A. Markov
A. Donchuk

Summary. The subject of the research in this article is information protection mechanisms in the Astra Linux operating system, the goal is to present theoretical and practical — within the framework of an experiment — information about the possibilities of implementing information protection methods in the Astra Linux operating system. The scope of application of the results is domestic information systems designed for processing information with increased security requirements. To achieve the objectives, the authors provide a brief summary of the available methods and means of information security, and then study the features of the use of mandatory access control, closed software environment mode, and mandatory integrity control in the Astra Linux operating system using specific practical examples. Based on the results of the work, a conclusion was drawn about the effectiveness of the considered information security mechanisms and recommendations were given for software developers.

Keywords: operating system, Astra Linux, information, methods and means of protecting information, information security.

Данилюк Сергей Сергеевич
Старший преподаватель, Московский государственный технический университет имени Н. Э. Баумана
vin.90@mail.ru
Марков Артём Дмитриевич
Аспирант, Московский государственный технический университет имени Н. Э. Баумана
lobart00@list.ru
Дончук Александра Ивановна
Аспирант, Московский государственный технический университет имени Н. Э. Баумана
sachadonchuk2001@mail.ru

Аннотация. Предметом исследования в данной статье являются механизмы защиты информации в операционной системе AstraLinux, целью — представление теоретических и практических — в рамках эксперимента — сведений о возможностях реализации методов защиты информации в операционной системе AstraLinux. Областью применения результатов являются отечественные информационные системы, предназначенные для обработки информации с требованиями повышенной защиты. Для реализации поставленных задач авторами дана кратка справка об имеющихся методах и средствах защиты информации, далее изучены особенности применения мандатного управления доступом, режима замкнутой программной среды, мандатного контроля целостности в операционной системе AstraLinux на конкретных практических примерах. По итогам работы сделан вывод об эффективности рассмотренных механизмов защиты информации и даны рекомендации для разработчиков программного обеспечения.

Ключевые слова: операционная система, AstraLinux, информация, методы и средства защиты информации, информационная безопасность.

Развитие новых информационных технологий сопровождается такими негативными событиями, как промышленный шпионаж, компьютерные преступления и несанкционированный доступ (НСД) к конфиденциальной и секретной информации. В связи с этим, защита данных становится крайне важным национальным заданием в любой стране. Неотложная потребность в обеспечении информационной безопасности нашла свое выражение в формировании Государственной системы защиты информации (ГСЗИ) и разработке законодательной базы для информационной безопасности. Приняты и введены в действие нормативные акты, такие как «О государственной тайне», «О данных, информатизации и защите информации», «Об правовой охране программ для электронных вычислительных устройств и баз данных», «Доктрина информационной безопасности Российской Федерации» и другие [9, с. 9].

Сбережение информации требует предотвращения ущерба, который может возникнуть из-за потери (кражи, утраты, деформации, подделки) информации во всех ее формах. Процедуры по обеспечению безопасности информации должны соответствовать важным законам и нормам, регулирующим безопасность информации, а также учитывать интересы пользователей. Для обеспечения высокой степени защиты информации необходимо решать сложные научно-технические задачи, связанные с разработкой и усовершенствованием средств ее защиты.

Обеспечение безопасности данных включает в себя комплекс действий и методов, направленных на сохранение конфиденциальности, целостности и доступности данных с целью предотвращения несанкционированного доступа, изменений или уничтожения информации. Теория обеспечения безопасности данных включает в себя ряд ключевых идей и принципов [8, с. 21].

1. Тайна. Этот принцип предполагает ограничение доступа к данным только для тех лиц, которым эта информация действительно необходима. Для

обеспечения конфиденциальности используются разные методы, включая шифрование данных, управление доступом, аутентификацию и авторизацию.
2. Целостность. Целостность данных означает, что информация остается неизменной и не подверглась несанкционированным изменениям. Для достижения целостности используются хэши, контрольные суммы, цифровые подписи и системы обнаружения изменений.
3. Доступность. Гарантирование того, что информация доступна только для уполномоченных пользователей в необходимое время. Для обеспечения доступности используются резервирование систем, равномерное распределение нагрузки и методы обнаружения и устранения сбоев.
4. Идентификация. Процесс проверки подлинности пользователя или системы перед предоставлением доступа. Это включает в себя использование паролей, биометрических данных, смарт-карт и других способов идентификации.
5. Авторизация. Процесс определения прав доступа к ресурсам или операциям после успешной аутентификации. Это гарантирует, что пользователи имеют доступ только к необходимой им информации.
6. Шифрование. Преобразование информации в зашифрованный вид с помощью определенных алгоритмов и ключей. Это обеспечивает конфиденциальность данных, даже если к ним будет получен несанкционированный доступ.
7. Управление рисками. Теория обеспечения безопасности данных также включает анализ и управление рисками. Это включает оценку уязвимостей, вероятности инцидентов, возможных ущербов и разработку стратегий для снижения рисков.
8. Обучение и информированность. Подход, при котором сотрудники и пользователи обучаются основам информационной безопасности. Чем лучше информированы люди, тем меньше вероятность случайных действий, которые могут привести к утечке данных.
9. Физическая защита. Большое значение имеет защита физической инфраструктуры, включая оборудование и серверные помещения. Системы контроля доступа, видеонаблюдение, биометрические методы обеспечивают безопасность.
10. Системы обнаружения и реагирования. Использование систем, способных обнаружить аномалии и атаки в реальном времени, а также оперативно реагировать на них для уменьшения ущерба.

Концепция обеспечения безопасности информации представляет собой всесторонний подход, объединяющий технические, организационные и человеческие элементы, с целью разработки надежных механизмов защиты данных в современном информационном обществе. Основной задачей обеспечения безопасности информации является сохранение целостности данных и уменьшение возможных повреждений. Следует подчеркнуть, что информационная безопасность зависит не только от компьютерных систем, но также от поддерживающей инфраструктуры. Существует несколько подходов к защите информации. Практически наиболее часто используются следующие методы [1, с. 60]:

1. Преграды для потенциальных злоумышленников, создаваемые физическими и программными средствами.
2. Изменение данных.
3. Установление условий, которые требуют от пользователя соблюдения правил обращения с информацией.
4. Формирование ситуации, мотивирующей пользователя к соответствующему поведению.

Также информационная безопасность оценивается на основе различных подходов:

1. Юридические — это законы, указы и постановления, имеющие юридическую силу в стране. В частности, эти меры направлены на профилактику нарушений.
2. Этические и моральные — аналогично юридическим мерам, они имеют профилактический характер и требуют постоянного создания здорового этического климата.
3. Технологические — ориентированы на снижение возможных ошибок, допускаемых сотрудниками.
4. Физические — включают меры и инструменты для обеспечения физической целостности компонентов.
5. Технические — основаны на использовании специализированных программ, выполняющих функции защиты.

Для снижения несанкционированного доступа к данным стали использовать методы аутентификации и идентификации. Аутентификация представляет собой проверку подлинности. Этот метод разделяется на два вида: односторонняя аутентификация, когда пользователь демонстрирует свою подлинность, и взаимная аутентификация. Главное преимущество аутентификации заключается в ее простоте и понятности. Идентификация — это распознавание пользователя по его уникальным характеристикам.

Так, в статье Булдаковой Т.И., Микова Д.А., Соколовой А.В. «Защита данных при дистанционном мониторинге состояния человека» приведены способы защиты данных в телемедицинских системах мониторинга состояния здоровья человека. Авторы придают особое значение аутентификации и идентификации, на основании которых может быть реализовано разграничение

прав доступа путем присвоения пользователем определенных категорий, наделенных теми или иными правами [4, с. 51].

Для повышения защищенности информации могут быть применены смарт-карты. Так, в медицинских информационных системах применение смарт-карт позволяет однозначно идентифицировать пациента и обеспечить отсутствие доступа к истории болезни сотрудников медицинских организаций, для которых данная информация не предназначена [3, с. 96–97]. Особенности их применения рассмотрены авторами Булдаковой Т.И., Ланцберг А.В., Смоляниновой К.А. в статье «Безопасный доступ к информации с использованием смарт-карт».

Существует также большое количество программного обеспечения, обрабатывающего информацию, подлежащую защите от несанкционированного доступа. Так, в статье Н.В. Бакланова, Д.А. Богданова, М.А. Попова, М.Ф. Симонова «Система расчета повреждаемости агрегатов самолета во время типового полета» рассмотрена идея создания подобного программного обеспечения, которое осуществляло бы обработку информации, поступаемой с датчиков, расположенных на различных агрегатах планера [2, с. 21]. При этом авторами заявлена совместимость с операционными системами семейства Windows. Авторы А.В. Герасименко, В.В. Пенегина, Б.Е. Кожуро, М.В. Виноградова в статье «Автоматизированная система расчета и анализа учебной нагрузки кафедры вуза» представили проект собственного программного обеспечения для решения указанных задач применительно к МГТУ им. Н.Э. Баумана [6, с. 43], работающего на базе операционных систем семейства Windows.

Обеспечить защиту информации можно различными способами, в том числе теми, о которых уже было рассказано выше. Однако для достижения данных целей могут быть использованы и другие инструменты. Высокую эффективность демонстрирует использование защищенных операционных систем, обладающих комплексом средств защиты информации (далее — СЗИ), адекватным потенциальным угрозам безопасности. Одна из таких операционных систем — операционная система специального назначения AstraLinuxSpecialEdition (далее — ОССН), разработанная АО «НПО РусБИТех» и являющаяся дериативом Debian. ОССН имеет сертификаты соответствия системы сертификации СЗИ по требованиям безопасности для сведений, составляющих государственную тайну (№ СФ/СЗИ-0343, № СФ/СЗИ-0342, № СФ/СЗИ-0614), а также сертификат соответствия ФСТЭК России №2557.

Основным преимуществом данной ОС является реализация мандатной сущностно-ролевой ДП-модели управления доступом и информационными потоками (МРОСЛ ДП-модель), сочетающей мандатное управление доступом, мандатный контроль целостности и ролевое управление доступом [5, с. 91]. Далее будет продемонстрировано применение некоторых ее элементов для обеспечения зашиты информации.

Механизм мандатного управления доступом позволяет управлять информационными потоками, содержащими информацию различных уровней конфиденциальности, снижая тем самым риск утечки такой информации. Для его реализации используется подсистема безопасности PARSEC, включающая модуль расширения ядра ОССН и программный интерфейс [5, с. 194]. Модуль PARSEC осуществляет контроль над предоставлением доступа процессам (субъект-сессиям) к тем или иным сущностям.

К элементам мандатного управления доступом относят мандатные атрибуты, представленные уровнями конфиденциальности, неиерархическими категориями и другими [5, с. 195]. Каждому уровню конфиденциальности соответствует числовое значение — чем оно больше, тем выше уровень конфиденциальности. Неиерархические категории представлены битовой маской; в данном случае числовые значения указывают на принадлежность информации к определенной категории.

Далее будет рассмотрено применение механизма мандатного управления доступом на примере работы с данными, относящимися к разным кафедрам университета, в ОССН версии 1.7.4. Для демонстрации применения данного механизма был использован следующий алгоритм:

1. Выполнить в терминале команду «sudofly-admin-smc» для перехода в раздел управления политикой безопасности
2. В разделе «Пользователи» создать пользователей ivanov и petrov, задать мандатные атрибуты. Для обоих пользователей минимальный уровень конфиденциальности 0, максимальный 1 (см. рис. 2, 3).
3. Создать каталог mgtu; создать внутри два подкаталога: IU-6 и UR. В каталоге IU-6 создать подкаталоги 0 и 1; в каталоге UR создать подкаталоги 0 и 1. Далее необходимо создать группы пользователей, которые будут иметь доступ к тем или иным каталогам. В группу IU-6 необходимо добавить пользователей u и ivanov; далее предоставить права для этой группы на каталог IU-6. В группу UR необходимо добавить пользователей u и petrov; далее предоставить права для этой группы на каталог UR. Следует отметить, что данные подготовительные действия реализуются в рамках дискреционного управления доступом, которое также применяется в ОССН. Совершить указанные действия возможно путем выполнения следующих команд:

```
sudosu
mkdir /mgtu
chownu:<пароль пользователя> /mgtu
```

```
chmod 750 /mgtu
mkdir /mgtu/IU-6
mkdir /mgtu/IU-6/0
mkdir /mgtu/IU-6/1
mkdir /mgtu/UR
mkdir /mgtu/UR/0
mkdir /mgtu/UR/1
groupadd IU-6
usermod -a -G IU-6 u
usermod -a -G IU-6 ivanov
groupadd UR
usermod -a -G UR u
usermod -a -G petrov
chgrp -R IU-6 /mgtu/IU-6/
chgrp -R UR /mgtu/UR/
chmod 750 /mgtu/IU-6/
chmod 750 /mgtu/UR/
chmod 777 /mgtu/IU-6/0
chmod 777 /mgtu/IU-6/1
chmod 777 /mgtu/UR/0
chmod 777 /mgtu/UR/1
```

4. Задать каталогам мандатные атрибуты. У каталогов /mgtu, /IU-6, /IU-6/1, /UR, /UR/1 уровень конфиденциальности равен 1; у каталогов /IU-6/0, /UR/0 уровень конфиденциальности равен 0. При этом атрибут ccnrпоказывает, что каталог может содержать сущности с различными уровнями конфиденциальности или неиерархическими категориями, но не большими, чем его собственные значения данных атрибутов. Совершить указанные действия возможно путем выполнения следующих команд:

```
pdpl-file1:0:0:ccnr /mgtu
pdpl-file 1:0:0:ccnr /mgtu/IU-6
pdpl-file 1:0:0:ccnr /mgtu/IU-6/1
pdpl-file 0:0:0:ccnr /mgtu/IU-6/0
pdpl-file 1:0:0:ccnr /mgtu/UR
pdpl-file 1:0:0:ccnr /mgtu/UR/1
pdpl-file 0:0:0:ccnr /mgtu/UR/0
```

5. Произвести вход под учетной записью пользователя ivanovc уровнем конфиденциальности 1
6. Перейти в каталог /mgtu. Обратить внимание на то, что перейти в подкаталог /UR не представляется возможным, поскольку пользователь ivanov не входит в группу пользователей, имеющих права на данный каталог
7. Перейти в каталог /mgtu/IU-6/1 и создать текстовый файл «важно.txt». Пользователю ivanov разрешено данное действие, поскольку уровень конфиденциальности сессии (1) равен уровню конфиденциальности каталога (1)
8. Выйти из сессии и произвести вход под учетной записью пользователя ivanovc уровнем конфиденциальности 0
9. Перейти в каталог /mgtu/IU-6/1. Обратить внимание на то, что созданный тем же пользователем файл «важно.txt» недоступен. Это обусловлено тем, что уровень конфиденциальности сессии (0) ниже уровня конфиденциальности каталога (1)

Далее будет рассмотрен режим замкнутой программной среды, позволяющий минимизировать перечень программного обеспечения, доступного для запуска [4, с. 58]. Для этого применяется невыгружаемый модуль ядра digsig_verif, входящий в состав подсистемы безопасности PARSEC, осуществляющий проверку цифровой подписи при обращении к сущностямфайловой системы [7, с. 57]. В данный модуль внедрены встроенные открытые ключи изготовителя, использующиеся для проверок; также имеется возможность добавлять дополнительные публичные ключи [7, с. 59]. Для демонстрации применения данного механизма был использован следующий алгоритм:

1. Загрузить из сети «Интернет» какое-либо программное обеспечение, например, пакет прикладных математических программ «Scilab», совместимый с операционными системами на базе ядра Linuxи распространяемый в виде архива «scilab-2023.1.0.bin.x86_64-linux-gnu.tar.xz».
2. Убедиться, что режим замкнутой программной среды включен, с помощью файла /etc/digsig/digsig_initramfs.conf (DIGSIG_ELF_MODE=1). Разархивировать архив и осуществить попытку запуска какого-либо исполняемого файла, входящего в его состав, например, scilab-cli. В результате запуска обнаружена ошибка сегментирования; программное обеспечение не может быть запущено, так как запускаемый файл не подписан цифровой подписью В нижней части экрана обнаружено уведомление «Загрузка неподписанного файла заблокирована СЗ ОС
3. Проанализировать ситуацию, в которой режим замкнутой программной среды был бы выключен (отключить данный режим можно только с правами суперпользователя). Убедиться, что DIGSIG_ELF_MODE=0. Осуществить попытку запуска исполняемого файлascilab-cli. Ошибок в процессе запуска не обнаружено Далее будет рассмотрен мандатный контроль целостности, также реализованный подсистемой безопасности PARSEC. Самыми важными уровнями целостности являются «Низкий» (0) и «Высокий» (63). При этом все процессы, выполняющиеся в пользовательской сессии, функционируют на том же уровни целостности, который выбран для сессии. Это обеспечивает защиту объектов более высокого уровня целостности от операций записи, перемещения, удаления [5, с. 213]. Для демонстрации применения данного механизма был использован следующий алгоритм:

1. Задать уровни целостности у пользователя u, обладающего правами суперпользователя: минимальный уровень целостности 0:Низкий, максимальный уровень целостности 63:Высокий .
2. Произвести вход под учетной записью пользователя uc низким уровнем целостности
3. Произвести попытку удаления файла scilab-2023.1.0.bin.x86_64-linux-gnu.tar.xz с помощью команды rm. Результат выполнения команды неуспешен как случае использования прав суперпользователя, так и без них.
4. Произвести вход под учетной записью пользователя u с высоким уровнем целостности
5. Произвести попытку удаления файла scilab-2023.1.0.bin.x86_64-linux-gnu.tar.xzc помощью команды rm. Результат выполнения команды успешен

Таким образом, механизмы, реализованные в ОССН, позволяют обеспечивать защиту информации, обрабатываемой в системе. Авторы рекомендуют разработчикам программного обеспечения обратить внимание на целесообразность использования данной операционной системы и реализации совместимости с ней своих продуктов.

ЛИТЕРАТУРА

1. Аваков, А.О. Обеспечение защиты информации в обществе / А.О. Аваков, Р.А. Скворцов // Форум молодых ученых. — 2019. — № 5(33). — С. 60–62
2. Бакланов Н.В., Богданов Д.А., Попов М.А., Симонов М.Ф. Система расчета повреждаемости агрегатов самолета во время типового полета // ИИАСУ'22. Искусственный интеллект в автоматизированных системах управления и обработки данных = Artificialintelligenceinmanagement, control, anddataprocessingsystems : сборник статей Всероссийской научной конференции, Москва, 27-28 апреля 2022 г. : в 2 т. / МГТУ им. Н.Э. Баумана (национальный исследовательский у-т). — 2022. — Т. 1. — С. 20–24.
3. Булдакова Т.И., Ланцберг А.В., Смолянинова К.А. Безопасный доступ к информации с использованием смарт-карт // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2017. №3. С. 95–106.
4. Булдакова Т.И., Миков Д.А., Соколова А.В. Защита данных при дистанционном мониторинге состояния человека // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2020. №4. С. 42–57.
5. Буренин П.В., Девянин П.Н., Лебеденко Е.В., Проскурин В.Г., Цибуля А.Н. Безопасность операционной системы специального назначения AstraLinuxSpecialEdition. Учебное пособие для вузов / Под ред. Доктора техн. наук, профессора П.Н. Девянина. — 3-е издание, перераб. и доп. — М.: Горячая Линия — Телеком, 2023. — 404 с.: ил.
6. Герасименко А.В., Пенегина В.В., Кожуро Б.Е., Виноградова М.В. Автоматизированная система расчета и анализа учебной нагрузки кафедры вуза // ИИАСУ'22. Искусственный интеллект в автоматизированных системах управления и обработки данных = Artificialintelligenceinmanagement, control, anddataprocessingsystems : сборник статей Всероссийской научной конференции, Москва, 27-28 апреля 2022 г. : в 2 т. / МГТУ им. Н.Э. Баумана (национальный исследовательский у-т). — 2022. — Т. 1. — С. 40–46.
7. Девянин П.Н., Тележников В.Ю., Третьяков С.В. Основы безопасности операционной системы AstraLinuxSpecialEdition. Управление доступом. Учебное пособие / Под ред. чл.-корр. Академии криптографии России, доктора техн. наук, профессора П.Н. Девянина. — М.: Горячая линия — Телеком, 2022. — 148 с.: ил.
8. Информационная безопасность: учебное пособие / В.Н. Ясенев, А.В. Дорожкин, А.Л. Сочков, О.В. Ясенев; под редакцией В.Н. Ясенева. — Нижний Новгород: ННГУ им. Н.И. Лобачевского, 2017. — 198 с.
9. Терентьев А.И. Основы информационной безопасности. Методы и средства защиты компьютерной информации [Текст]: учебное пособие / А.И. Терентьев. — М.: ИД Академии Жуковского, 2020. — 84 с.