УДК 004.056.24

Вестник УрФО № 3(37) / 2020, с. 27–33

Куц Д. В., Поршнев С. В.

DOI: 10.14529/secur200303

ОСОБЕННОСТИ ПРИМЕНЕНИЯ ПОЛНОМОЧНОЙ МОДЕЛИ РАЗГРАНИЧЕНИЯ ДОСТУПА В СОВРЕМЕННЫХ СРЕДСТВАХ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

В статье рассмотрены особенности эксплуатации полномочной модели разграничения доступа в средствах защиты информации (СЗИ) от несанкционированного доступа (НСД), влияющие на её эффективность. Проведен анализ некоторых недостатков средств защиты и возможные сценарии, позволяющие нарушителю получить доступ к данным в обход действующей модели. Предложены меры по противодействию НСД и способы их применения, обеспечивающие устранение обнаруженных недостатков СЗИ. Сделан обоснованный вывод о необходимости целенаправленного анализа политик настройки СЗИ от НСД и, при необходимости, их пересмотра в сторону ужесточения.

Ключевые слова: *разграничение доступа, СЗИ от НСД, несанкционированный доступ, Secret Net Studio, Страж NT, полномочная модель, мандатная модель, уязвимость, защитные механизмы, альтернативные потоки данных, аппаратный модуль доверенной загрузки, безопасный режим ОС.*

THE FEATURES OF MANDATORY ACCESS CONTROL MODEL IN MODERN UNAUTHORIZED ACCESS DATA PROTECTION TOOLS

This article describes the features of mandatory access control model in unauthorized access data protection tools, which can affect its efficiency. Also, some flaws of unauthorized access data protection tools and possible scenarios of unauthorized access bypassing these tools are analyzed. The countermeasures and methods of its application, eliminating detected flaws are offered. The conclusions about necessarity of analyze of unauthorized access data protection tools policies and revision of its severeness, if it is necessary, were made.

Keywords: *access control, SZI from NSD, unauthorized access, Secret Net Studio, Guardian NT, authoritative model, mandatory model, vulnerability, protective mechanisms, alternative data streams, hardware trusted boot module, safe mode OS.*

При работе с данными, требующими полномочного разграничения доступа, применяют те или иные защитные механизмы, которые призваны обеспечить доступность защищаемых файлов и каталогов только для пользователей, работающих в системе с уровнем допуска, соответствующим метке доступа защищаемого ресурса. Используемые при этом защитные механизмы являются компонентами операционной системы (ОС) или частью специального программного обеспечения (СПО). Полномочная модель разграничения доступа реализована, например, в отечественной ОС специального назначения Astra Linux [1], а также в отечественных средствах защиты от НСД (например, Secret Net Studio [2], Dallas Lock [3], Страж NT [4] и др.).

Однако оказывается, что в ряде случаев даже правильно настроенная модель разграничения доступа не способна обеспечить надёжную и эффективную защиту от НСД к данным пользователя, не обладающего необходимыми полномочиями, поскольку защитные механизмы как дискреционной, так и полномочной системы разграничения доступа могут быть нарушены с помощью специальных действий, предпринятых со стороны пользователя. В этой связи разработка подходов, обеспечивающих надежную защиту от НСД, является актуальной.

В статье обсуждается способ защиты от НСД, основанный на комплексном использовании механизмов безопасности ОС и средств защиты.

Для обоснования актуальности темы исследования, на примере Secret Net Studio, рассмотрим некоторые компьютерные системы и сценарии поведения злоумышленника, в которых современные сертифицированные средства защиты от НСД, представленные в соответствующем сегменте рынка СПО, оказываются неэффективными.

1. Компьютер, в котором отсутствует аппаратный модуль доверенной загрузки, или он был извлечён злоумышленником. Здесь злоумышленник имеет возможность реализовать загрузку ОС с внешнего носителя (параметр UEFI в BIOS), что даёт неограниченный доступ к незашифрованным данным, хранящимся на жестком диске, так как все атрибуты безопасности файлов и каталогов в случае неактивной системы защиты будут игнорироваться. Это становится возможным, поскольку используемый для защиты доступа к BIOS и изменению его настроек пароль оказывается достаточно просто сбросить [5].

Более эффективным решением для обсуждаемой системы является механизм защиты диска, реализованный в ряде СЗИ от НСД, суть которого заключается в модификации системных структур диска (например, MBR и/или BR). В этом случае злоумышленник не может получить доступ к файлам и каталогам, так как загружаемая ОС не может распознать на диске разделы и файловые системы на них. Однако злоумышленник имеет возможность сделать побайтную копию всего жесткого диска и далее восстановить данные с образа жесткого диска, используя автоматизированные утилиты, например, RStudio или Easy Recovery.

Отметим, что интеграция аппаратного модуля доверенной загрузки с СЗИ от НСД, не позволяющая злоумышленнику пройти аутентификацию в ОС при извлеченной плате защиты, не исключает возможность загрузки с внешнего носителя.

В этой связи, по-видимому, единственной по настоящему эффективной защитой является шифрование критичных данных на жёстком диске, что делает доступ и/или съём информации с диска бесполезным.

2. Получение злоумышленником прав локального администратора компьютерной системы, которые он может получить несколькими способами. Во-первых, при наличии физического доступа к системе и возможности загрузки с внешнего носителя злоумышленник может сбросить пароль на встроенной учётной записи администратора или на любой другой учётной записи с правами администратора, а так же назначить полномочия администратора системы любой учётной записи. Более того, злоумышленник способен скопировать файлы базы учётных данных пользователей Windows и выполнить подбор пароля по хэшу, хранящемуся в этой базе, и тем самым узнать пароль администратора системы, не сбрасывая его. Во-вторых, злоумышленник может использовать уязвимость системного или прикладного ПО, которое своевременно не было обновлено. Для этого используются вредоносные программы, содержащие данные или исполняемый код, которые способны воспользоваться одной или несколькими уязвимостями используемого ПО на локальном или удаленном компьютере (эксплойты) и получить права администратора компьютерной системы. Получив права администратора, злоумышленник становится способным управлять защитными механизмами СЗИ от НСД, включать и отключать модули защиты (отметим, что ряд СЗИ от НСД имеют механизм самозащиты с сервисным паролем, который не позволит отключить или удалить СЗИ администраторам, не знающим данный пароль). В случае развёртывания средства защиты с централизованным управлением, о манипуляциях злоумышленника по отключению средства защиты станет известно на сервере при анализе журналов событий СЗИ от НСД. Однако, имея права администратора системы, существует возможность обращаться к защищаемым ресурсам напрямую, в обход механизмов защиты, и соответственно, без ведения записей в журналах СЗИ. Для этого злоумышленник может использовать специализированное ПО, обеспечивающее прямой доступ к диску – так называемые HEX–редакторы или шестнадцатеричные редакторы.

Для подтверждения данного утверждения рассмотрим модель компьютерной системы, в которой используется одно из популярных сегодня СЗИ от НСД Secret Net Studio 8. В изучаемой системе авторами были созданы три пользователя: User1, User2 и Администратор. Пользователь User1 имел максимальный уровень допуска – «строго конфиденциально», пользователь User2 – «не конфиденциально» и права администратора. Пользователь User1 создал файл text.txt, в котором разместил текст следующего содержания: «Строго конфиденциальное содержимое файла» и присвоил значению метки доступа к файлу «строго конфиденциально». Рабочее окно шестнадцатеричного редактора, в котором пользователь User2, имеющий права администратора и работающий в режиме «не конфиденциально», представлено на рис. 1.

Из рис. 1 видно, что в шестнадцатеричном редакторе оказалось доступным содержимое файла с меткой доступа «строго конфиденциально». При этом в журналах используемого СЗИ от НСД имеется запись о факте запуска пользователем User2 шестнадцатеричного редактора, однако, каких-либо записей о факте доступа к защищенному конфиденциальному файлу с помощью использованного редактора каких-либо записей обнаружить не удалось.

Исключить возникновение описанной ситуации можно, если использовать специальную настройку изолированной программной среды, включающую в себя составление спи-

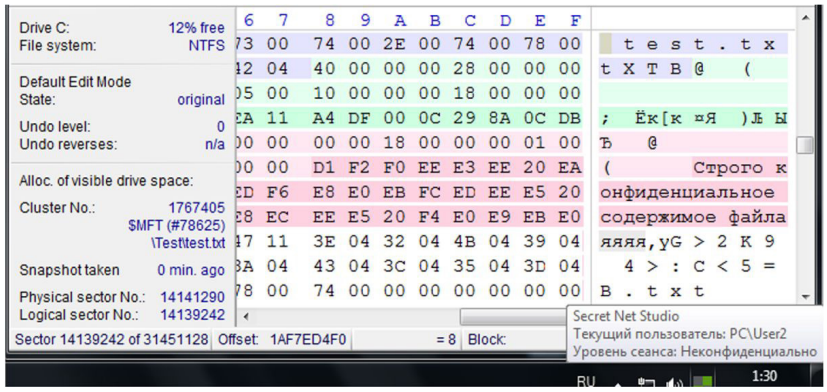

Рис. 1. Демонстрация доступа к содержимому файла с максимальным уровнем конфиденциальности

ска процессов, которые данный субъект может порождать [6]. В этой ситуации субъект (пользователь компьютерной системы) не сможет запустить стороннее ПО. Также целесообразно использовать двухфакторную аутентификацию, так как в данном случае, даже зная пароль локального администратора, злоумышленник не сможет пройти аутентификацию.

3. Загрузка компьютерной системы в безопасном режиме. В безопасном режиме компоненты системы защиты компьютерной системы не загружаются, что позволяет злоумышленнику получать доступ к закрытой информации (рис. 2).

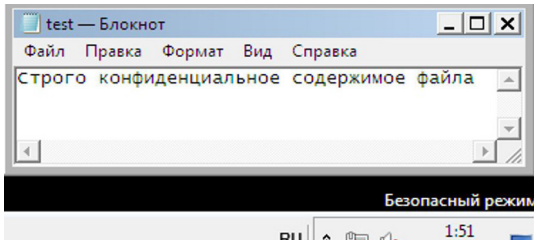

Рис. 2. Доступ к строго конфиденциальному файлу из безопасного режима

С нашей точки зрения, наиболее эффективное решение, позволяющее избежать обсуждаемой ситуации, состоит в запрещении запуска системы в безопасном режиме, которая реализуется редактированием некоторых разделов реестра ОС Windows. Отметим, что штатными механизмами администрирования ОС реализовать данное решение затруднительно.

4. Использование недостатков собственно СЗИ от НСД, к которым следует отнести ряд особенностей работы полномочной системы разграничения доступа, которыми может воспользоваться злоумышленник для извлечения части содержимого строго конфиденциального документа и далее его сохранении с понижением метки конфиденциальности. Проиллюстрируем данный недостаток следующим примером. В модели компьютерной системы установлено одно из популярных на рынке СЗИ от НСД (например, Secret Net Studio 8), полномочная модель которого позволяет создавать неконфиденциальные папки в неконфиденциальных расположениях в строго конфиденциальном режиме. Здесь злоумышленник, имеющий права доступа «строго конфиденциально» может открыть обсуждавшийся выше файл test.txt и скопировать его содержание, далее создать неконфиденциальную папку в не конфиденциальном разделе и вставить в ее название содержимое файла test.txt, имеющего метку конфиденциальности «строго конфиденциально» (рис. 3).

Из рис. 3 видно, что злоумышленнику с уровнем допуска в системе «строго конфиденциально», работающему в строго конфиденциальном режиме, удалось вставить в название неконфиденциальной папки, расположенной в неконфиденциальном расположении, и сохранить содержимое строго конфиденциального текстового документа. Разумеется, возможность такой операции ограничено 256 символами имени папки. Однако данное ограничение не снимает описанных выше проблем безопасности информации. Кроме того, злоумышленник вместо одной папки может создать множество папок данного типа. Также обойти ограничение в 256 символов злоумышленник может путём использования командной строки и записи скопированного текста из строго конфиденциального документа в альтернативный поток данных неконфиденциального каталога (рис. 4).

Из рис. 4 видно, что в неконфиденциаль-

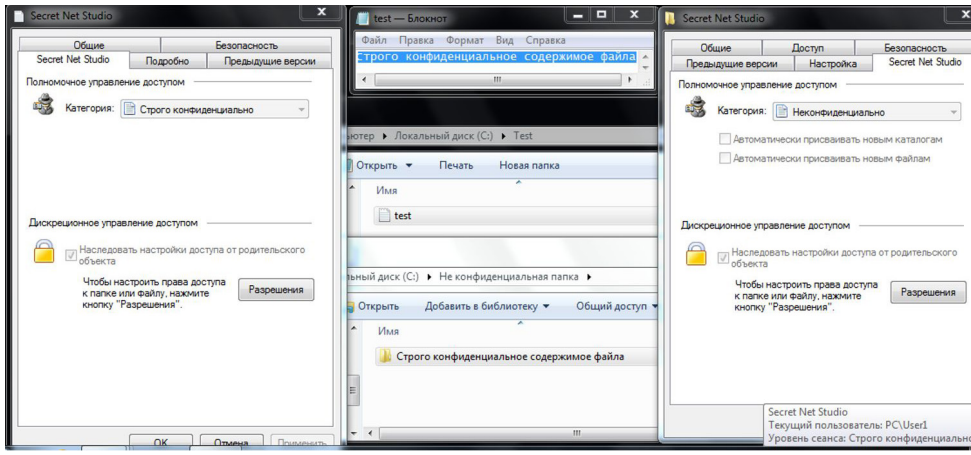

Рис. 3. Возможность понижения категории данных в строго конфиденциальном режиме работы

ном каталоге действительно удается создать альтернативный поток данных с именем ADS объёмом 45 байт, содержащий текст строго конфиденциального документа. При этом объём записываемого текста ограничен только возможностями командной строки. Данный каталог впоследствии может быть скопирован в неконфиденциальном режиме работы на носитель с файловой системой NTFS без потери данных в альтернативном потоке. При копировании или перемещении файла из одного NTFS-раздела в другой NTFS-раздел потоки сохраняются, и ОС никак не сигнализирует об их присутствии [7]. Кроме того, другой пользователь, работающий в неконфиденциальном режиме, может вывести содержимое альтернативного потока данных на экран (рис. 5).

Для пользователей данного СЗИ мы рекомендуем ограничить с помощью дискреционной модели создание и переименование папок в любых директориях (включая корневую), кроме тех, на которые реализовано перенаправление. В этом случае утечка информации вышеописанным способом будет исключена. Однако это может вызвать сбои в работе прикладного и системного ПО. Кроме этого, в целях обеспечения безопасности, пользователям необходимо запрещать доступ к командной строке и к запуску командных файлов «bat».

В целом, принимая во внимание вышеизложенное, мы считаем, что полномочная модель разграничения доступа будет работать эффективно, и СЗИ от НСД будут обеспечи-

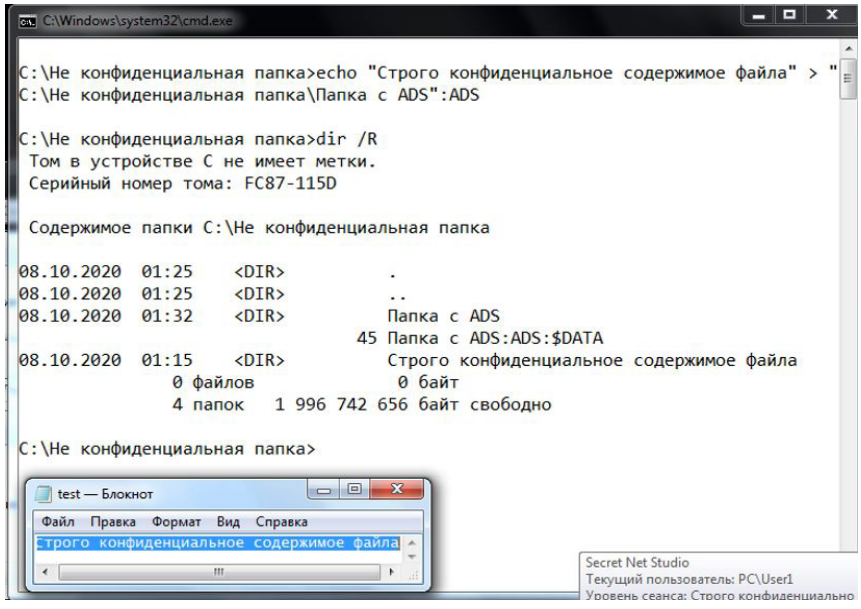

Рис. 4. Сохранение данных в альтернативном потоке

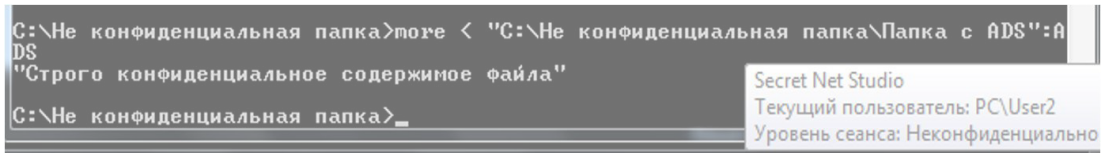

Рис. 5. Доступ к ADS в не конфиденциальном режиме

вать надёжную защиту данных только в случае использования комплексного, грамотного и неформального подхода к реализации защитных механизмов СЗИ. Для этого настройку средства защиты необходимо проводить с учётом специфики данного СЗИ от НСД, ОС, а также аппаратной части компьютерной системы, на которой оно применяется. Для исключения возможности несанкционированного доступа к данным во многих случаях требуется пересмотреть требования, применяемые при настройке средств защиты информации в компьютерных системах, в сторону их ужесточения.

Литература

1. Операционная система специального назначения «Astra Linux Special Edition» Руководство администратора. Часть 1. [Электронный ресурс] URL: https://astralinux.ru/products/astra-linux-special-edition/documents-astra-se/rukovodstvo-administratora-chast-1-astra-se.pdf

2. Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Локальная защита. [Электронный ресурс] URL: https://www.securitycode.ru/upload/iblock/6fe/Руководство администратора. Настройка и эксплуатация. Локальная защита.pdf

3. Система защиты информации от несанкционированного доступа Dallas Lock 8.0 Руководство по эксплуатации. [Электронный ресурс] URL: https://www.dallaslock.ru/upload/medialibrary/cp/documents/С ИК5 2017/RU.48957919.501410-02 92 Руководство по эксплуатации.pdf

4. Страж NT. Система защиты информации от несанкционированного доступа. Руководство администратора. [Электронный ресурс] URL: https://guardnt.ru/doc/gnt_40_admin_guide.pdf

5. Духан Е.И., Синадский Н.И., Хорьков Д.А. Применение программно-аппаратных средств защиты компьютерной информации: учебное пособие. — 3-е изд., перераб. и доп. – Екатеринбург: УрФУ, 2013. — 240 с.

6. Проскурин, В.Г. Защита в операционных системах: учеб. пособие для вузов / В.Г. Проскурин. — М.: Горячая линия – Телеком, 2014. — 193 с.: ил.

7. Анализ и восстановление данных на носителях с файловой системой NTFS: учебное пособие / Н. И. Синадский; научный редактор канд. техн. наук, доц. В.В. Бакланов. Екатеринбург: ГОУ ВПО УГТУ–УПИ, 2007. – 136 с.

References

1. Operacionnaja sistema special'nogo naznachenija «Astra Linux Special Edition» Rukovodstvo administratora. Chast' 1. [Jelektronnyj resurs] URL: https://astralinux.ru/products/astra-linux-special-edition/documents-astra-se/rukovodstvo-administratora-chast-1-astra-se.pdf

2. Sredstvo zashhity informacii Secret Net Studio. Rukovodstvo administratora. Nastrojka i jekspluatacija. Lokal'naja zashhita. [Jelektronnyj resurs] URL: https://www.securitycode.ru/upload/iblock/6fe/Rukovodstvo administratora. Nastrojka i jekspluatacija. Lokal'naja zashhita.pdf

3. Sistema zashhity informacii ot nesankcionirovannogo dostupa Dallas Lock 8.0 Rukovodstvo po jekspluatacii. [Jelektronnyj resurs] URL: https://www.dallaslock.ru/upload/medialibrary/cp/documents/SIK5 2017/RU.48957919.501410-02 92 Rukovodstvo po jekspluatacii.pdf

4. Strazh NT. Sistema zashhity informacii ot nesankcionirovannogo dostupa. Rukovodstvo administratora. [Jelektronnyj resurs] URL: https://guardnt.ru/doc/gnt_40_admin_guide.pdf

5. Duhan E.I., Sinadskij N.I., Hor'kov D.A. Primenenie programmno-apparatnyh sredstv zashhity komp'juternoj informacii: uchebnoe posobie. — 3-e izd., pererab. i dop. – Ekaterinburg: UrFU, 2013. — 240 s.

6. Proskurin, V.G. Zashhita v operacionnyh sistemah: ucheb. posobie dlja vuzov / V.G. Proskurin. — M.: Gorjachaja linija – Telekom, 2014. — 193 s.: il.

7. Analiz i vosstanovlenie dannyh na nositeljah s fajlovoj sistemoj NTFS: uchebnoe posobie / N. I. Sinadskij; nauchnyj redaktor kand. tehn. nauk, doc. V.V. Baklanov. Ekaterinburg: GOU VPO UGTU–UPI, 2007. – 136 s.

КУЦ Дмитрий Владимирович, старший преподаватель Учебно-научного центра «Информационная безопасность» Уральского федерального университета имени первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 19. E-mail: d.v.kutc@urfu.ru

ПОРШНЕВ Сергей Владимирович, доктор технических наук, профессор, директор Учебно-научного центра «Информационная безопасность» Уральского федерального университета имени первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 19. E-mail: s.v.porshnev@urfu.ru

KUTS Dmitry Vladimirovich, senior teacher of the Training and Scientific Center "Information Security", Ural Federal University named after the first President of Russia B.N.Yeltsin. 620002, Sverdlovsk region, Ekaterinburg, Mira street, 19. E-mail:d.v.kutc@urfu.ru

PORSHNEV Sergey Vladimirovich, Doctor of Technical Sciences, Full Professor, Head of Unit, Training and Scientific Center "Information Security", Ural Federal University named after the first President of Russia B.N.Yeltsin. 620002, Sverdlovsk region, Ekaterinburg, Mira street, 19. E-mail: s.v.porshnev@urfu.ru