УДК 004.056.53 + 004.4.056

**Скурлаев С. В., Соколов А. Н.**

# ТЕХНИЧЕСКИЕ РЕШЕНИЯ, ПРИМЕНЯЕМЫЕ ДЛЯ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В СИСТЕМАХ КЛАССОВ 3А И 2А

*Рассмотрены основные подходы к реализации механизмов защиты информации от несанкционированного доступа на примере некоторых средств защиты. Они идентичны друг другу или отличаются в зависимости от производителя. Выбраны наиболее распространенные реализации механизмов защиты и проанализированы взаимодействия соответствующих средств защиты с операционной системой и защищаемой информацией. Проведены исследования с применением продуктов Sysinternals: Autoruns, Process Explorer и Process Monitor. Показано, что все реализации обладают недостатками, которые можно компенсировать, применяя ручные настройки соответствующих служб операционной системы.*

***Ключевые слова:*** *автоматизированная система (АС), несанкционированный доступ (НСД), операционная система (ОС), средства вычислительной техники (СВТ), средство защиты информации (СЗИ).*

**Skurlaev S. V., Sokolov A. N.**

# TECHNICAL SOLUTIONS USED FOR 3A/2A CLASS SYSTEMS OF UNAUTHORIZED ACCESS PROTECTION

*The article discusses the main approaches to the implementation of typical technical solutions used for preventing unauthorized access to information. Certain approaches are identical to each other; others have differences depending on the manufacturer. Several most commonly used implementations were analyzed in terms of interaction with operating system and protected information. The following means of Windows Sysinternals products were used in research: Autoruns, Process Explorer and Process Monitor. It is shown that all approaches have its disadvantages which can be compensated using manual settings of appropriate operating system's services.*

***Keyword:*** *automated system (AS), unauthorized access (UA), operating system (OS), means of protecting information from unauthorized access.*

Основные положения по технической защите информации закреплены специальным нормативным актом Гостехкомиссии России «Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»[1]. В нём изложены цели и направления технической защиты информации в автоматизированных системах (АС) от несанкционированного доступа (НСД), а также основные способы обеспечения защиты. НСД определен как доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или АС[1]. Концептуальные положения по технической защите информации (такие как классификация АС, модель нарушителя в АС, основные способы НСД и др.) раскрыты в других специальных нормативных актах. Классификация АС приведена в руководящем документе (РД) «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»[2]. В нём закреплены три основных класса АС, каждый из которых подразделяется на подклассы. К подклассам предъявляются определённые требования по реализации тех или иных механизмов. В связи с этим можно применять средства защиты, отвечающие требованиям, предъявляемым в ряде других специальных нормативных документов – РД Гостехкомиссии и ФСТЭК.

Довольно распространёнными АС являются системы 3-го и 2-го классов, с одним или несколькими пользователями соответственно, но обрабатываемая информация имеет одинаковый уровень ограничений к распространению. В то же время среди средств защиты информации (СЗИ) чаще встречаются такие, которые отвечают требованиям для АС классов 1Г (обработка несекретной информации) или 1Б (обработка до совершенно секретно включительно), потому что требования на более низкие классы выполняются автоматически. Но сами средства при этом весьма разнообразны, подходы разработчиков к реализации одних механизмов схожи, для других – отличны.

Для выполнения определённых требований все СЗИ используют системные функции операционных систем (ОС) семейства Microsoft Windows, например, дискреционную модель разделения доступа. Для выполнения других требований РД АС схожим остаётся только принцип функционирования. Соответственно, для реализации одних механизмов СЗИ сами предъявляют требования к системе, а для других – используют свои драйвера и службы. С целью узнать слабые и сильные стороны различных технических решений проведён эксперимент по изучению взаимодействия СЗИ с ОС.

Для эксперимента выбран следующий ряд СЗИ: Secret Net 6, СтражNT 3.0, Аура. Выбор основан на двух критериях: доступность экземпляра средства защиты для эксперимента и различие в технологических подходах к решению тех или иных задач. Эксперимент проведен с помощью программных продуктов от «Sysinternals» (Марк Руссинович, Брайс Когсвелл):

- Autoruns (отражает перечень драйверов, служб, модулей оболочки и входа в операционную систему и другое);
- Process Explorer (показывает работающие процессы, а также их подчинённость, используемые файлы и директории);
- Process Monitor (отслеживает действия всех процессов в системе, в том числе драйверов и библиотек, позволяет установить драйвер мониторинга с самого начала загрузки операционной системы).

С помощью этих программ проанализировано взаимодействие СЗИ с ОС, в том числе влияние на запросы ПО к защищаемой информации и устойчивость к сбоям.

**Secret Net 6** имеет сертификат соответствия требованиям РД СВТ[3] по 3 классу защищённости и РД НДВ[3] по 2 уровню. При выполнении технических условий применение этого средства возможно в подавляющем большинстве АС. Например, для ограничения загрузки с внешних носителей устанавливается плата аппаратной поддержки или электронный замок «Соболь» (в который можно установить считыватель идентификаторов iButton). При этом не исключается возможность использования других аппаратных идентификаторов, например eToken или Rutoken. Для функционирования требуются версии Professional операционных систем Windows от 2000 до 7, поскольку для управления средством требуются некоторые оснастки консоли (например, управление групповыми политиками).

В составе СЗИ имеются следующие компоненты:

- служба ядра;
- локальная база данных системы защиты;
- подсистема регистрации и журнал Secret Net;
- подсистема локального управления;
- защитные подсистемы;
- модуль входа;
- подсистема контроля целостности;
- подсистема работы с аппаратной поддержкой,

а также криптоядро, которое производителем не выделяется в отдельную компоненту, так как в нем применяются несертифицированные алгоритмы.

Некоторые из механизмов, включая драйвер ядра, работают как службы ОС. В случае отказа одной из служб перестают выполняться связанные с ней механизмы. Отказ службы драйвера ядра может привести к неработоспособности СЗИ в целом, позволяя зайти в систему только с административными правами. В случае использования СЗИ в АС третьего класса единственный пользователь будет иметь такие полномочия. В общем случае средство защиты расширяет возможности ОС, внедряя драйверы-фильтры в файловые операции, обращения к устройствам, подсистему входа-выхода и другие подсистемы. Настройки СЗИ хранятся в реестре и файле настроек СЗИ. При их повреждении не всегда остаётся возможной корректная деинсталляция средства защиты, что можно отнести к недостаткам Secret Net 6.

**СтражNT 3.0** имеет сертификат соответствия требованиям РД СВТ[3] по 3 классу защищённости и РД НДВ[4] по 2 уровню. Ограничение загрузки с внешних носителей реализовано путём сокрытия логической структуры диска – изменением информации в загрузочном секторе диска. В качестве аппаратных идентификаторов возможно применение различных устройств: гибких магнитных дисков, iButton, eToken, Rutoken и Guardant ID. СЗИ функционирует в любых версиях ОС Windows, начиная от 2000 и заканчивая 7.

СЗИ СтражNT 3.0 имеет следующие модули[5]:

- модуль входа в систему;
- модуль загрузки;
- модуль ядра системы защиты;
- службу доступа к устройствам;
- подсистемы защиты.

Ядро этого СЗИ реализовано как драйвер ядра ОС, поэтому вариант отказа средства защиты ввиду незапустившейся службы невозможен (все драйверы активны с момента загрузки ОС). Поскольку СЗИ при использовании модуля входа в систему обеспечивает сокрытие логической структуры диска, то слабым местом остаётся носитель-идентификатор: в случае утраты или неработоспособности вход в систему будет невозможен. Необходимо отметить, что само СЗИ при этом позволяет сделать дубликат идентификатора. Для разделения доступа так же, как и в Secret Net 6, используются драйверы-фильтры, которые перенаправляют запросы в случае обращений к файлам и устройствам внутренним механизмам СЗИ. Благодаря такому подходу данное средство является относительно независимым от ОС, под которой оно будет работать.

**Аура** имеет сертификат соответствия требованиям РД СВТ[3] по 3 классу защищённости и РД НДВ[4] по 2 уровню. Ограничение загрузки со сторонних носителей реализовано с помощью прозрачного преобразования дисков при помощи патентованных методов. В качестве аппаратных идентификаторов могут применяться Rutoken или iButton (для последнего необходимо использование электронного замка «Соболь»). ОС, поддерживаемые этим СЗИ, ограничены следующим перечнем: Microsoft Windows 2000 Professional SP4, 2000 Server SP4, XP Professional SP3, Server 2003 Standard Edition SP2, Server 2003 Enterprise Edition SP2, Server 2008 Standard Edition SP2, Server 2008 Enterprise Edition SP2, Vista Business SP2, Vista Ultimate SP2.

СЗИ имеет множество модулей, реализованных как в качестве службы, так и в качестве драйверов системы и библиотек оболочки. Примечательным является также механизм контроля целостности и редактирования базы данных пользователей, включая их полномочия, до загрузки операционной системы. Как и в случае с Secret Net 6, СЗИ поддерживает несертифицированное шифрование, но способно полностью преобразовывать диски, включая виртуальные, инструменты для создания которых имеются в самом СЗИ. Производитель отмечает следующие минусы своего продукта:

- отсутствие автоматизированной настройки мандатной системы разграничения доступа, что компенсируется выбором метки сессии (но сами метки можно устанавливать поверх файловой системы NTFS);

• отсутствие на данный момент возможности разделения доступа к конкретным устройствам, кроме накопителей (как правило, в большей части автоматизированных систем третьего и второго класса имеет лишь одно автоматизированное рабочее место, не включающее несколько различных устройств).

На данный момент слабым местом средства защиты информации является не очень широкий перечень поддерживаемых ОС.

Таблица 1 отражает основные подходы к реализации некоторых механизмов защиты, их достоинства и недостатки.

Таблица 1. Сравнение средств защиты информации

| **Средство защиты информации** | **Secret Net 6** | **Страж NT 3.0** | **Аура** |
|---|---|---|---|
| Ядро СЗИ | Служба и драйвер операционной системы | Драйвер ядра операционной системы | Отсутствует как таковое – служба операционной системы SKernel только обслуживает централизованную БД СЗИ |
| Механизмы контроля доступа к файлам | Реализованы как отдельные драйверы-фильтры операционной системы (запросы программ сравниваются с меткой сессии, объекта и разрешений пользователя) | Реализованы как отдельные драйверы-фильтры операционной системы | Реализованы как отдельные драйверы-фильтры операционной системы (запросы программ сравниваются с меткой сессии, объекта и разрешений пользователя), а также ряд служб, осуществляющих служебные операции |
| Ограничение загрузки | Аппаратный модуль (или программный для АС класса 1В) | Сокрытие логической структуры диска | Прозрачное преобразование (кодирование) дисков |
| Недостатки СЗИ | Слабым местом является служба ядра СЗИ, так как в случае отказа вход разрешается только администраторам. В случае отказа аппаратной части (хищения жёсткого диска с программным модулем ограничения загрузки) возможна загрузка со сторонних носителей | При контроле потоков не требуется выбирать уровень метки сессии, но значительно усложняется процесс настройки подсистемы мандатного доступа (для часто используемых программ есть шаблоны от производителя). В случае потери ключа преобразования загрузка ОС невозможна. Запросы программ перенаправляются механизмам СЗИ, поэтому для них логика их работы прозрачна, любая операция всегда завершается успешно, метка сессии не требуется. Широкий спектр поддерживаемых операционных систем | В случае отказа службы ядра СЗИ продолжает функционировать. В случае потери ключа шифрования загрузка операционной системы невозможна. Узкий перечень совместимых ОС |
| Достоинства СЗИ | Хорошая интегрируемость в операционную систему | Завершённость данного СЗИ – не требует дополнительных программных и аппаратных средств, кроме идентификаторов | Запуск данного СЗИ до загрузки ОС |

Таким образом, все СЗИ обладают как достоинствами, так и недостатками, наличие которых определяется используемыми технологиями и конкретными реализациями. Большую часть недостатков можно компенсировать, применяя ручные настройки соответствующих служб ОС. Например, проблема со службой ядра Secret Net 6 решается путём ручной настройки этой службы так, чтобы ОС сама перезапускала её. Все угрозы, связанные с потерей ключевых носителей, решаются путём создания резервной копии каждого из них с дальнейшим хранением этих копий в надёжном хранилище.

Таким образом, любые выявленные недостатки СЗИ можно устранить или уменьшить эффект их нежелательных последствий. Тем не менее выбор того или иного СЗИ должен определяться степенью риска потери защищаемых носителей или идентификаторов, а также утраты защищаемых данных во внештатных ситуациях.

## Примечания

[1] Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. – Утверждено решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. — http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty (дата обращения 10.10.2013).

[2] Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. – Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. — http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty (дата обращения 10.10.2013).

[3] Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. – Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. — http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty (дата обращения 10.10.2013).

[4] Руководящий документ. Защита от несанкционированного доступа к информации. Ч. 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. – Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114. — http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty (дата обращения 10.10.2013).

[5] Система защиты информации от несанкционированного доступа «СТРАЖ NT». Версия 3.0. Описание применения. – 2010 г. — http://guardnt.ru/download/doc/app_guide_nt_3_0.pdf (дата обращения 10.10.2013).

## References

[1] Directive document. Concept of protection of hardware, computer equipment, and automated systems from unauthorized access. – Upheld by the State Presidential Technical Commission of the Russian Federation as of March 30, 1992. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty (accessed 10.10.2013).

[2] Directive document. Automated systems. Protection from unauthorized access. Classification of automated systems and requirements on information protection. – Upheld by the State Presidential Technical Commission of the Russian Federation as of March 30, 1992. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty (accessed 10.10.2013).

[3] Directive document. Hardware and computer equipment. Protection from unauthorized access. Index of protection from unauthorized access. – Upheld by the State Presidential Technical Commission of the Russian Federation as of March 30, 1992. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty (accessed 10.10.2013).

[4] Directive document. Protection from unauthorized access. Part 1. Software of the means of information security. Classification on the basis of the level of control over the absence of undocumented features.. – Upheld by the State Presidential Technical Commission of the Russian Federation as of June 4, 1999. No. 114. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty (accessed 10.10.2013).

[5] System of protection of information from unauthorized access «STRAZh NT» Version 3.0. – 2010 URL: http://guardnt.ru/download/doc/app_guide_nt_3_0.pdf (accessed 10.10.2013).

**Скурлаев Сергей Вадимович,** специалист по защите информации ООО «Стратегия безопасности». E-mail: sch1081024@mail.ru

**Соколов Александр Николаевич,** кандидат технических наук, доцент, зав. кафедрой безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет). E-mail: ANSokolov@inbox.ru

**Sergey Vadimovich Skurlaev,** security engineer of the LLC "Strategy of security". E-mail: sch1081024@mail.ru

**Aleksand Nikolaevich Sokolov,** cand. Sc. Engineering, associated professor, head of the Department of Information system Security of South Ural State University (National Research University). E-mail: ANSokolov@inbox.ru