УДК 004.056.53

Основные подсистемы защиты информации от несанкционированного доступа и особенности их настройки

© А.А. Герасимов, В.А. Кузнецов, А.В. Мозговой, К.А. Пугачев

МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

Представлен обзор существующих типов обеспечения защиты информации от несанкционированного доступа на объектах информатизации. Рассмотрены основные требования, предъявляемые к средствам защиты информации от несанкционированного доступа (СЗИ от НСД). Описаны основные подсистемы работы СЗИ от НСД, а также рекомендации по настройке этих подсистем. Сделан вывод о корректности и адекватности применения правильно настроенного комплекса СЗИ от НСД.

Ключевые слова: *защита информации, несанкционированный доступ, объект информатизации, автоматизированная система, средство защиты информации.*

Защита информации от несанкционированного доступа (ЗИ от НСД) на объектах информатизации (ОИ) представляет собой важную составляющую обеспечения безопасности информации на ОИ. Несмотря на то что требования к защите информации определенного уровня конфиденциальности от НСД закреплены законодательно, при ЗИ от НСД, в отличие от других факторов обеспечения безопасности информации (например, таких, как ЗИ от утечки по техническим каналам), применяется более творческий подход к построению системы защиты.

В настоящее время в зависимости от типа ОИ и его структуры для обеспечения ЗИ от НСД могут применяться следующие классы средств защиты:

1) средства аппаратной идентификации;
2) средства антивирусной защиты;
3) средства обнаружения вторжений;
4) межсетевые экраны;
5) программные и программно-аппаратные средства защиты информации от несанкционированного доступа (СЗИ от НСД);
6) средства шифрования.

Построение комплекса по ЗИ от НСД на каждом конкретном ОИ начинается с построения модели информационного документооборота ОИ. Проводится изучение информационных потоков на ОИ, определяются риски и основные угрозы информации на всех этапах ее

хранения, обработки и передачи на ОИ. На основании полученной информации строится матрица доступа к информации, обрабатываемой на ОИ, а также схема информационных потоков. Затем на основании собранных об ОИ сведений строится модель комплекса СЗИ от НСД для исследуемого ОИ.

Чаще всего на автоматизированных рабочих местах (АРМ) в составе ОИ применяются программные или программно-аппаратные СЗИ от НСД. В зависимости от того, имеются ли у АРМ в составе ОИ сетевые подключения, принимается решение о применении средств межсетевого экранирования, а также средств обнаружения вторжений.

Основную же роль в обеспечении безопасности на ОИ играют СЗИ от НСД. В данный момент на рынке средств защиты предлагается обширный выбор СЗИ от НСД, основными из которых являются «Аккорд», «Страж», Secret net и Dallas lock.

Каждое из приведенных средств отличается своими особенностями в работе. В связи с тем что все эти средства имеют действующие сертификаты соответствия Федеральной службы технического и экспортного контроля (ФСТЭК) России по защите информации на автоматизированных системах (АС) до класса 1Б включительно, положительно или отрицательно оценивать их можно по двум критериям: удобство в работе для пользователя; удобство и прозрачность настройки.

Согласно руководящему документу «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» СЗИ от НСД должно обеспечивать безопасность информации с помощью следующих четырех основных подсистем:

1) идентификации и аутентификации;
2) регистрации и учета;
3) криптографической защиты;
4) контроля целостности.

Подсистема идентификации и аутентификации предоставляет и контролирует доступ к работе на АРМ ОИ пользователей. В зависимости от уровня конфиденциальности информации и от класса АС, на которой эта информация обрабатывается, могут применяться разные методы идентификации и аутентификации. Однако стоит отметить, что одним из самых надежных методов является аппаратная идентификация с последующей аутентификацией по паролю определенной длины и сложности в зависимости от класса АС.

К основным задачам *подсистемы регистрации и учета* относятся: ведение журнала всех действий пользователя на АРМ АС; фиксация в журнале попыток НСД пользователя к ресурсам, доступ к которым ему запрещен; учет всех носителей информации и гарантиро-

ванное уничтожение затираемой информации. Самым уязвимым местом работы АС являются съемные носители. Связано это в первую очередь с тем, что для удобной работы пользователи часто пренебрегают некоторыми принципами защиты информации и начинают применять съемные носители разного рода и происхождения. Естественно, при этом возникает риск заражения АРМ АС компьютерными вирусами, а также риск утечки информации с использованием незарегистрированных носителей. На устранение данной угрозы и направлена работа подсистемы регистрации и учета СЗИ от НСД. Чаще всего в СЗИ жестко фиксируются набор носителей по их заводским номерам, определяемым при подключении к АРМ, и список атрибутов по доступу к ним. Это позволяет избежать несанкционированного копирования информации и, как результат, утечки ее с использованием сторонних носителей. Кроме того, удается избежать заражения АРМ АС компьютерными вирусами. Однако при настройке данной подсистемы необходимо тщательно изучить процесс работы пользователей АС, так как жесткая настройка без учета тонкостей циркуляции информации может привести к значительному ухудшению удобства применения СЗИ от НСД конечными пользователями и, как результат, к новым попыткам НСД.

Подсистема криптографической защиты преобразовывает информацию, обрабатываемую в АС, с помощью известных надежных криптографических алгоритмов. Применение данной подсистемы определяется не только классом АС, но и тем, как циркулирует информация на АС. Чаще всего информация зашифровывается при передаче по сети, реже — при ее сохранении на съемные носители.

Основной задачей *подсистемы контроля целостности* является сохранение работоспособности как программной, так и аппаратной части АС. Причем все требования, предъявляемые к АС в руководящем документе «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», СЗИ от НСД реализовать не в состоянии. В частности, они не могут реализовать требования физической охраны средств АС и наличия администратора безопасности. В обязанности СЗИ от НСД входят подсчет контрольных сумм программного обеспечения АС и контроль аппаратной конфигурации АС. В случае несовпадения контрольных сумм и (или) изменения аппаратной конфигурации компьютера работа текущего пользователя блокируется. Контроль проводится в два этапа: 1) по завершении работы пользователя СЗИ от НСД вычисляет контрольные суммы программ и сохраняет аппаратную конфигурацию АС; 2) при следующем включении АРМ АС на этапе загрузки операционной системы и СЗИ от НСД контрольные суммы и аппаратная конфи-

гурация сравниваются с эталонными значениями. По результатам сравнения принимается решение о возможности дальнейшей работы пользователя на АС.

Из вышесказанного можно сделать следующий вывод: настройка СЗИ от НСД зависит от многих факторов, и только грамотный учет всех тонкостей работы с информацией на АС, а также анализ угроз безопасности информации и соблюдение требований руководящих документов [1, 2] обеспечивают ЗИ от НСД в АС и, что немаловажно, удобную, комфортную работу пользователей.

ЛИТЕРАТУРА

[1] Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». *Российская газета*, 2012, 7 ноября.

[2] Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». *Российская газета*, 2013, 22 мая.

Статья поступила в редакцию 28.06.2013

Ссылку на эту статью просим оформлять следующим образом:

Герасимов А.А., Кузнецов В.А., Мозговой А.В., Пугачев К.А. Основные подсистемы защиты информации от несанкционированного доступа и особенности их настройки. *Инженерный журнал: наука и инновации,* 2013, вып. 11. URL: http://engjournal.ru/catalog/it/security/1017.html

Герасимов Антон Андреевич родился в 1985 г., окончил МГТУ им. Н.Э. Баумана в 2009 г. Канд. техн. наук, доцент кафедры «Защита информации» МГТУ им. Н.Э. Баумана. Автор более 15 статей, 1 монографии и 3 методических указаний по тематике «Защита информации». e-mail: ger-anton@mail.ru

Кузнецов Виктор Александрович родился в 1989 г., окончил МГТУ им. Н.Э. Баумана в 2012 г. Ассистент кафедры «Защита информации» МГТУ им. Н.Э. Баумана. e-mail: viktor__kuznetsov@mail.ru

Мозговой Андрей Валериевич родился в 1986 г., окончил МГТУ им. Н.Э. Баумана в 2009 г. Ассистент кафедры «Защита информации» МГТУ им. Н.Э. Баумана. Автор более 10 статей и 1 методических указаний по тематике «Защита информации». e-mail: runc.nsd@gmail.com

Пугачев Кирилл Александрович родился в 1987 г., окончил МГТУ им. Н.Э. Баумана в 2010 г. Ассистент кафедры «Защита информации» МГТУ им. Н.Э. Баумана. Автор 1 статьи и 1 методических указаний по тематике «Защита информации». e-mail: pugachev_ka13@mail.ru