УДК 004.056.53

НЕКОТОРЫЕ ПРИКЛАДНЫЕ ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ

Долматова Я.Г., Душкин А.В., Кравченко А.С., Панычев С.Н., Сахаров С.Л.
ФКОУ ВО «Воронежский институт ФСИН России», Воронеж, e-mail: a_dushkin@mail.ru

В настоящей статье приведено описание функций программно-аппаратных средств, необходимых для организации разграничения доступа субъектов к объектам информационной системы с учетом различных политик безопасности. Приведены основополагающие принципы мандатного и дискреционного разграничения доступа. Описан подход к организации изолированной среды выполнения прикладных задач пользователя. Рассмотрены способы реализации угроз безопасности информации в информационной системе обработки данных. Предложен набор компонентов, необходимый для создания полнофункционального программно-аппаратного комплекса защиты информации от несанкционированного доступа. Практическое использование программно-аппаратных комплексов защиты информации от несанкционированного доступа с описанными в статье компонентами и характеристиками способно локально обеспечить информационную безопасность системы обработки информации, а в совокупности со средствами контроля доступа, средствами подавления утечки информации по техническим каналам, организационными мероприятиями по защите информации удовлетворить самые высокие запросы в области безопасности информации ограниченного распространения.

Ключевые слова: программно-аппаратный комплекс, несанкционированный доступ, политика безопасности, система разграничения доступа

SOME APPLIED QUESTIONS OF INFORMATION SECURITY OF INFORMATION PROCESSING SYSTEMS

Dolmatova Ya.G., Dushkin A.V., Kravchenko A.S., Panychev S.N., Saharov S.L.
Federal state educational institution of higher education Voronezh institute of the Russian Federal Penitentiary Service, Voronezh, e-mail: a_dushkin@mail.ru

This article describes the functions of software and hardware required for the organization of the subjects of differentiation of access to the objects of information systems, taking into account the different security policies. Presents the fundamental principles of discretionary and mandatory access control. The approach to the organization of the safe runtime user applications considered ways of implementing information security threats in the information processing system. A set of components needed to create a fully functional hardware and software to protect information from unauthorized access. Practical use of software and hardware systems to protect information from unauthorized access to those described in the components of the article and the characteristics able to locally ensure the information security of data processing systems, and in conjunction with the access control means, means of suppressing leakage through technical channels of information, organizational measures for the protection of information to meet the most high demands on security restricted information.

Keywords: software and hardware, unauthorized access, security policy, system access control

Степень информатизации современного общества позволяет говорить о том, что в вопросах безопасности возрастает актуальность мероприятий по устранению угроз, связанных с нарушением конфиденциальности, целостности и доступности информационных ресурсов.

От безопасности информационных систем и информационных ресурсов зависит благополучие в различных сферах деятельности, в настоящее время уже существуют примеры смерти человека из-за реализованных угроз безопасности информации.

Необходимость защиты сведений конфиденциального характера привела к образованию Государственной системы защиты информации. На современном этапе высокими темпами развивается правовая база в области безопасности информации и защиты информации, обрабатываемой в информационных системах.

В соответствии с четвертым пунктом статьи 16 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» [1]:

«Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации,

в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации;

7) нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации.»

Это накладывает на всех участников информационного взаимодействия высокие требования. Комплекс мероприятий по защите информации от несанкционированного доступа есть составная часть деятельности предприятия, учреждения, фирмы и др., независимо от его ведомственной принадлежности и формы собственности, и проводится в совокупности с административными, техническими, правовыми, инженерными мерами по обеспечению установленного режима обращения со сведениями конфиденциального характера.

Программное и аппаратное обеспечение современных информационных систем представляет собой сложную многоуровневую систему взаимодействующих компонентов, которые в разной степени интегрированы в нее.

Модульность построения систем порождает множество уязвимостей, связанных как с недоработками, так и с необходимостью организации интерфейсов взаимодействия компонентов [2].

В современных информационных системах реализованы достаточно надежные функции обеспечения безопасности, выполняющие контроль доступа к информационным ресурсам, обеспечивающие защиту от несанкционированного доступа. Как правило, такие функции реализованы в очень общем виде, не допускающем гибкой настройки. Операционные системы массового использования имеют механизмы защиты, функционирующие под управлением ядра системы. Такая ситуация дает возможность реализации угроз информационной безопасности по отношению к информационным ресурсам до загрузки ядра операционной системы. И если функции контроля доступа принципиально существуют и функционируют, то контроля целостности информационных ресурсов пользователя в распространенных операционных системах нет как такового, система лишь контролирует наличие и корректную работу собственных модулей, что, однако, не препятствует успешной их модификации вредоносным программным обеспечением [2].

Также отсутствует контроль за аппаратной конфигурацией системы обработки информации.

Преодоление указанных недостатков возможно путем применения комплексной программно-аппаратной защиты информационных ресурсов вычислительной системы.

В общем случае, такие комплексы нужны для обеспечения:

– возможности создания правил разграничения доступа к информационным ресурсам;

– идентификации и аутентификации пользователей информационной системы с применением аппаратных ключей безопасности;

– аппаратного контроля целостности информационных ресурсов до загрузки операционной системы;

– контроля доступа к ресурсам информационной системы;

– динамического контроля целостности информационных ресурсов самой системы защиты, операционной системы, наборов прикладных программ пользователя;

– журналирования всех действий пользователя.

Современные комплексы аппаратно-программной защиты информации в своём составе имеют:

– аппаратный модуль доверенной загрузки, обеспечивающий безопасность компонентов информационной системы (аппаратных и программных) от несанкционированного доступа до загрузки операционной системы и доверенную загрузку. Работа аппаратной части комплекса начинается непосредственно после проведения диагностики системы средствами базовой системы ввода/вывода, что гарантированно не дает возможность загрузить операционную систему с модифицированным кодом или в случае модификации контролируемых данных пользователя;

– специальное программное обеспечение, обеспечивающее расширенные функции защиты информации при запущенной операционной системе.

Программно-аппаратные комплексы защиты информации от несанкционированного доступа предназначены для решения задачи защиты информации в вычислительных системах, функционирующих под управлением частично контролируемых операционных систем, без внесения

изменений в ранее установленные программные средства [3, 4].

Программно-аппаратный комплекс защиты информации от несанкционированного доступа должен обеспечивать «прозрачный» режим работы, «прозрачность» заключается в том, что пользователь, не замечает работы средств защиты информации, либо ощущает ее в минимальной степени.

Такой подход обеспечивает минимизацию нагрузки на пользователя по защите информационных ресурсов системы. Всю нагрузку по организации защиты информации берет на себя администратор безопасности информации. Исходя из этого для обеспечения безотказной и эффективной работы предъявляются высокие требования к профессиональной подготовке администратора безопасности информации, он обязан правильно применять программно-аппаратные комплексы защиты информации от несанкционированного доступа к ресурсам информационной системы.

Комплекс средств защиты должен осуществлять мониторинг доступа субъектов авторизованных информационных систем к зарегистрированным ресурсам информационной системы (файлам, программам, томам и т.д.).

Контроль доступа должен быть гарантированно применим к любому ресурсу информационной системы и любому субъекту, в этой системе зарегистрированному.

Для каждой пары субъект информационной системы – ресурс информационной системы в правилах разграничения доступа информационной системы должен быть задан в явном и не допускающем неопределенности виде перечень допустимых типов доступа субъекта информационной системы к информационным ресурсам системы (объекту).

Существуют два основных подхода к организации разграничения доступа: мандатный и дискреционный, оба они допускают гибкую настройку правил разграничения доступа.

Механизм доступа, основанный на принципе дискреционного контроля, обязан обеспечивать возможности разрешенной модификации регламента разграничения доступа, в частности, должна быть предоставлена возможность разрешенного изменения списка пользователей информационной системы и списка контролируемых ресурсов информационной системы.

Право менять правила реализации политики безопасности могут быть предоставлены специализированным субъектам информационной системы [4].

Мандатный подход в организации разграничения доступа к информационным ресурсам предполагает присвоение меток доступа каждому объекту информационной системы и меток полномочий каждому субъекту или активному ее объекту. Сопоставление метки доступа объекта и метки полномочий субъекта информационной системы позволяет организовать разграничение доступа к информационным ресурсам системы.

Такие метки характеризуют различные прикладные параметры, такие как: степень уязвимости к угрозам безопасности информации, категории секретности сведений, составляющих государственную тайну, категорию доступа персонала и другие характеристики. Следует отметить, что метки могут входить как в линейные категории, так и в иерархические структуры.

Комплекс средств защиты информации полностью контролирует информационные потоки и запрашивает метку доступа ко вновь появившемуся информационному объекту информационной системы у уполномоченного пользователя (администратора безопасности информации). Аналогично, каждому новому субъекту или активному объекту при регистрации присваивается метка категории доступа к информационным ресурсам.

Одно из наиболее важных требований к механизму мандатного разграничения доступа в автоматизированной системе состоит в возможности однозначного и точного сопоставления внешних меток доступа и полномочий с внутренними (для автоматизированной системы защиты информации).

Подсистема контроля за использованием ресурсов автоматизированной системы должна иметь возможность реализации контроля относительно любых объектов информационной системы со стороны любого же субъекта или активного объекта как в явном, так и в скрытом виде.

Общий свод правил, лежащих в основе мандатного принципа разграничения доступа можно сформулировать так:

– субъект или активный объект информационной системы может получить право «чтения» объекта информационной системы или ресурса в том случае, если метка его полномочий равна или превосходит в иерархии прав доступа метку доступа объекта;

– субъект или активный объект информационной системы может осуществлять

запись в объект, если метка его полномочий равна в иерархии прав доступа метке доступа объекта.

Необходимой функцией системы разграничения доступа является контроль информационных потоков для исключения ситуаций переноса информации из ресурсов с более высокой степенью конфиденциальности в ресурсы с более низким уровнем при работе субъекта или активного объекта.

Как и любая информационная система, система, работающая на основе мандатного механизма разграничения доступа, должна допускать гибкое изменение классификационных уровней доступа и полномочий.

Комплексная система защиты информации должна работать на основе средства, осуществляющего мониторинг любых вызовов субъектов или активных объектов к объектам информационной системы – диспетчера доступа. Диспетчер доступа делает вывод о санкционированности обращения к информационному ресурсу строго после проверки на соответствие правил разграничения доступа всех используемых механизмов (дискреционными, мандатными и прочими).

Комплекс средств защиты должен управлять информационными потоками, анализируя метки конфиденциальности информационного. Требование равенства или преимущества метки конфиденциальности носителя перед информационным ресурсом должно выполняться в полной мере [3, 4].

Комплексная система защиты информации должна позволять организовывать работу пользователя в изолированной программной среде. В ситуации, когда автоматизированная система допускает работу нескольких пользователей с разным уровнем полномочий по использованию информационных ресурсов, пользователь с привилегиями администратора безопасности информации дает каждому из них подмножество разрешенных к использованию программных средств из множества всех доступных.

В такой ситуации под несанкционированным доступом уже понимается использование программного обеспечения и некоторых его методов, не разрешённых к использованию, но присутствующих в вычислительной системе. Злоумышленником же становится пользователь, который подобные действия проделывает.

Такая трактовка несанкционированного доступа предполагает, что не может нарушаться физическая целостность вычислительной системы, а злоумышленник пользуется лишь имеющимися в вычислительной системе либо установленными им же программами.

Реализация злого умысла может заключаться в непосредственном осуществлении несанкционированных операций чтения или записи с использованием стороннего либо неконтролируемого программного обеспечения или в опосредованном влиянии на работу другого пользователя информационной системы путем изменения функциональных возможностей его программного обеспечения.

Наличие возможности использования изолированной программной среды пользователя дает снижение требований к базовому программному обеспечению в плане выполнения требований информационной безопасности. Это становится возможно благодаря тому, что концепция изолированной программной среды подразумевает проверку активности процессов и используемых ими информационных потоков, как и целостность программного обеспечения еще до его запуска.

Следует отметить, что на базовое программное обеспечение накладывается требование невозможности влияния на уже запущенные программы, то есть влиять на потоки ввода / вывода и невозможность редактировать данные других программ, размещенные в оперативной памяти.

Для идентификации и аутентификации субъекта в информационной системе необходимо применять программно-аппаратные средства идентификации. Это устройство, в котором аппаратно реализован набор функций и алгоритмов защиты информации, а также набор драйверов и библиотек для использования криптографических функций в различных прикладных программах [5]. Такие средства могут быть применены для:

– аппаратной идентификации и аутентификации пользователей на автономных компьютерах, или рабочих станциях частично контролируемых и полностью контролируемых операционных систем;

– идентификации и аутентификации пользователя в типовых решениях на базе наиболее распространенных пакетов прикладных программ (например, Microsoft);

– хранения персональной информации пользователя (ключей, паролей и пр.) в защищенной памяти. Доступ к этой памяти предоставляется только после ввода аутентифицирующей информации (PIN-кода);

– шифрования и подписи файлов пользователя для их хранения и передачи по открытым каналам связи.

Практическое использование программно-аппаратных комплексов защиты информации от несанкционированного доступа с описанными выше компонентами и характеристиками способно локально обеспечить должный уровень информационной безопасности при обработке данных в вычислительной системе, а в совокупности со средствами контроля доступа, средствами подавления утечки информации по техническим каналам, организационными мероприятиями по защите информации удовлетворить самые высокие запросы в области безопасности информации ограниченного распространения.

Список литературы

1. Аккорд-Win64. Программа ACED32, установка ПРД [Электронный ресурс] / Официальный сайт ОКБ САПР. – Режим доступа: http://www.accord.ru/accwin64-aced.html, свободный. – Загл. с экрана. (дата обращения: 01.12.2015).

2. Душкин А.В. Программно-аппаратные средства обеспечения информационной безопасности: практикум / А.В. Душкин, А.С. Кравченко, А.С. Кольцов[и др.]. – Воронеж: Научная книга, 2015. – 200 с.

3. Кравченко А.С. Применение аппаратных ключей для защиты программного обеспечения / А.С. Кравченко, С.Л. Сахаров // Вестник Воронежского института ФСИН России. – 2015. – № 2. – С. 38–40.

4. Об информации, информационных технологиях и о защите информации: Федер. закон Рос. Федерации, 27 июля 2006 г., № 149-ФЗ [Электронный ресурс]. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102108264&intelsearch=%CE%E1+%E8%ED%F4%EE%F0%EC%E0%F6%E8%E8%2C+%E8%ED%F4%EE%F0%EC%E0%F6%E8%EE%ED%ED%FB%F5+%F2%E5%F5%ED%EE%EB%EE%E3%E8%FF%F5+%E8+%EE+%E7%E0%F9%E8%F2%E5+%E8%ED%F4%EE%F0%EC%E0%F6%E8%E8 (дата обращения: 17.06.2016).

5. Руководство администратора [Электронный ресурс] / Официальный сайт ОКБ САПР. – Режим доступа: http://www.accord.ru/ru_admin-le.html, свободный. – Загл. с экрана. (дата обращения: 01.12.2015).