ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.414.2=161.1

А.В. Гуляев[1]
Э.И. Митряев[2]

СОВЕРШЕНСТВОВАНИЕ МОДЕЛИ УПРАВЛЕНИЯ ДОСТУПОМ К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ С ОГРАНИЧЕННОЙ ПО ВРЕМЕНИ АВТОРИЗАЦИЕЙ

A.V. Gulyaev
E.I. Mitryaev

PERFECTION OF CASE FRAME BY ACCESS TO CONFIDENTIAL INFORMATION FOR USERS WITH A LIMIT ON TIME AUTHORIZING

Для программно-аппаратной реализации допуска к конфиденциальной информации с учетом необходимости выполнения требований ГОСТ Р 50739-95 (Защита от несанкционированного доступа к информации) [4] на практике используются различные модификации модели мандатного управления допуском. Однако в данной модели отсутствует алгоритм управления допуском с ограничением времени использования разрешительного мандата на допуск к конкретным конфиденциальным документам. В сложившейся практике в организациях временно́й доступ предоставляется только по служебным запискам, подтвержденным и одобренным старшим руководством. Данная служебная записка отправляется в отдел безопасности, и там уже на основании ее выдается временной доступ к файлам и информации. Так как организация крупная, то данных запросов поступает большое количество, и существует вероятность человеческого фактора и неснятие доступа с человека по окончании его работы с информацией. При прохождении проверки данные несоответствия уровней допуска выявляются, сотрудник, забывший снять доступ, наказывается.

В связи с тем что в имеющейся программной реализации мандатной модели управления допуском отсутствует алгоритм автоматизированного управления временным доступом, и для предотвращения вышеописанных ситуаций необходимо в данную модель внедрить дополнительный модуль, решающий задачи управления временным доступом в информационную систему организации санкционированных пользователей.

В данном модуле должны быть реализованы следующие задачи:

- удовлетворение потребности в предоставлении временного доступа;
- удаление доступа по завершении отведенного рабочего времени с документом;
- поддержка защиты от несанкционированного доступа;
- защита от инсайдерских угроз, в том числе мониторинг ввода клавиатуры, на основании одобрения руководством и предупреждения работающего персонала о мониторинге.

При этом необходимо выполнение организационных мер защиты в соответствии с Приказом ФСТЭК России от 11 февраля 2013 г. № 17 [1]

[1] Магистрант АНО ВО «Российский новый университет».

[2] Доктор технических наук, профессор, профессор кафедры информационной безопасности факультета информационных систем и компьютерных технологий АНО ВПО «Российский новый университет».

и Федеральным законом от 27.07.2010 № 224-ФЗ [2].

Для программно-аппаратной реализации данного модуля необходимо выполнение условий в соответствии с руководящим документом «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» [3].

Необходимо также выполнение требований ГОСТ Р 50739-95 (Защита от несанкционированного доступа к информации) [4].

Среди требований ГОСТ Р 50739-95 выделим требования по:

1) разграничению доступа, предусматривающие то, что СВТ (средства вычислительной техники) должны поддерживать непротиворечивые, однозначно определенные правила разграничения доступа;

2) учету, предусматривающие то, что СВТ должны поддерживать регистрацию событий, имеющих отношение к защищенности информации;

3) гарантиям, предусматривающим необходимость наличия в составе СВТ технических и программных механизмов, позволяющих получить гарантии того, что СВТ обеспечивает выполнение требований к разграничению доступа к учету.

Для реализации этих требований в разрабатываемом модуле необходимо решить ряд задач организационно-технического и программно-аппаратного уровней. Конкретно эти задачи можно сгруппировать по выполнению выделенных выше требований ГОСТ Р 50739-95.

Для выполнения требований (1) защищенности системы по разграничению доступа необходимо реализовать следующие требования:

- дискретизационный принцип контроля доступа;
- мандатный принцип контроля доступа;
- идентификация и аутентификация;
- очистка памяти;
- изоляция модулей;
- защита ввода и вывода на физический носитель информации.

Для выполнения требований (2) защищенности системы по учету необходимы:

- регистрация;
- маркировка документов.

Для выполнения требований (3) защищенности системы по гарантиям необходимы:

- надежное восстановление;
- целостность КСЗ (комплекс средств защиты);
- контроль модификаций;
- взаимодействие пользователей с КСЗ;
- тестирование.

Предлагаемый алгоритм работы службы безопасности организации с данным модулем может быть представлен в виде следующей блок-схемы:

Литература

1. Приказ ФСТЭК России от 11 февраля 2013 г. № 17.

2. Федеральный закон от 27.07.2010 № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации».

3. Руководящий документ «Средства вычислительной техники». Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

4. ГОСТ Р 50739-95 Защита от несанкционированного доступа к информации.