УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАЗЫ ДАННЫХ СИСТЕМЫ КОМПЬЮТЕРНОЙ ДИАГНОСТИКИ АВТОТЕХНИКИ

Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь

М. В. Михальцов

Г. В. Сечко − к. т. н., доцент

Анализируются угрозы информационной безопасности базы данных системы компьютерной диагностики автотехники. Выбранные угрозы предлагается разделить на 2 группы и включить в разрабатываемый профиль защиты базы данных

Система компьютерной диагностики автотехники (СКДА) резко сокращает длительность и трудоемкость ремонта автомобиля. Программное обеспечение системы включает собственно программу диагностики и автомобильную базы данных (АБД) с собственной системой управления. Программа, установленная на компьютере, посылает через ком-порт (или USB-порт) сигналы от автосканера в адаптер, который в свою очередь транслирует их на контроллер в автомобиле. Контроллер посылает ответные сигналы (данные), которые программа получает и, сравнивая их с данными автомобильной базы данных, интерпретирует (визуализирует). Обмен управляющими сигналами и данными происходит согласно определенному протоколу. Описанная сложность СКДА делает систему и, главное, ее АБД, как информационный объект, уязвимой со стороны естественных воздействий среды и преднамеренных и непреднамеренных воздействий со стороны человека. Возникает проблема обеспечения информационной безопасности (ИБ) АБД. Для повышения обоснованности задания требований безопасности АБД, оценки безопасности и возможности проведения сравнительного анализа уровня безопасности необходимо составить профиль защиты (ПЗ) АБД [1, 2].

В докладе с целью составления подраздела «Угрозы ИБ» раздела «Среда безопасности объекта оценки (ОО)» ПЗ АБД [1, 2] анализируются возможные угрозы ИБ базы. Первичный анализ угроз показал, что все возможные угрозы ИБ АБД целесообразно разделить на 2 группы. В первую группы «Угрозы, предотвращаемые ОО», на наш взгляд, необходимо отнести следующие угрозы:

- **T.ACCESS** *Несанкционированный доступ к базе данных* (Угроза возникает, когда посторонний или пользователь системы, который в настоящее время не является уполномоченным пользователем АБД, обращается к базе)*;*
- **T.DATA** *Несанкционированный доступ к информации* (пользователь АБД обращается к информации базы без разрешения собственника данных или лица, которое отвечает за их защиту*;*
- **T. ATTACK** *Необнаруженное нападение* (необнаруженная компрометация АБД в результате действий нарушителя, пытающегося выполнить действия, которые он не уполномочен выполнять)*;*
- **T.ABUSE.USER** *Неправильное использование привилегий* (Необнаруженная компрометация АБД в результате действий пользователя (преднамеренных или нет), связанных с выполнением операций индивидуума, уполномоченного на их выполнение; например, пользователь может предоставить доступ к БД, ответственным за которую он является, другому пользователю, способному использовать эту информацию для мошеннических целей).

Во вторую группы «Угрозы, предотвращаемые ОО», целесообразно отнести следующие угрозы:

- **T.OPERATE** *Опасная операция* (компрометация базы данных может произойти из-за неправильной конфигурации, администрирования и/или функционирования СКДА)*;*
- **T.CRASH** *Внезапные прерывания* (прерывания функционирования АБД, приводящие к потере или разрушению данных, связанных с безопасностью, таких как данные управления АБД и данные аудита. Такие прерывания могут являться результатом ошибки оператора (см. также **T.OPERATE**) или сбоев и отказов программного обеспечения, аппаратных средств, источников питания или носителей данных; защита от данной угрозы может быть обеспечена, например методологией, изложенной в [3])*;*
- **T.PHYSICAL** *Физическое нападение* (критичные к безопасности части АБД или базовой операционной системы и/или сетевых сервисов могут быть подвергнуты физическому нападению, которое может нарушить ИБ.

Вывод: выбранные в результате анализа угрозы ИБ АБД позволяют составить профиль защиты базы данных, обоснованно задать требования безопасности к АБД, провести оценку безопасности и сравнительный анализ уровня безопасности.

Список использованных источников

1. Голиков, В.Ф. Методологические основы информационной безопасности: учеб .- метод. пособие / В.Ф. Голиков, И. И. Черная, О. Б. Зельманский. – Мн. : БГУИР, 2010. – 67 с.

2. Цирлов, В.Л. Основы информационной безопасности автоматизированных систем: краткий курс. – Ростов-на Дону: Феникс, 2010. – 172 с.

3. Николаенко В.Л., Пачинин В.И., Сечко Г.В., Таболич Т. Г. Методика оценки количественного влияния мероприятий по повышению надежности оборудования на коэффициент его готовности // Материалы 15-й МНТК «Современные средства связи», 28 -30 сентября 2010 года, Минск, РБ / редкол.: А.О.Зеневич и [др.] – Мн. : УО ВГКС, 2010. – С. 149.