1.8 Определение проблемы безопасности

ОО обеспечивает обнаружение и блокирование следующих основных угроз безопасности информации:

Угроза-1: Угроза восстановления и/или повторного использования аутентификационной информации.

Описание угрозы: Угроза заключается в возможности доступа к данным пользователя в результате подбора (например, путём полного перебора или перебора по словарю) аутентификационной информации дискредитируемой учётной записи пользователя в системе, а также путём перехвата и повторного использования хэша пароля, для восстановления сеанса.

Источники угрозы: Внешний нарушитель с низким потенциалом; Внутренний нарушитель с низким потенциалом.

Принятые меры противодействия угрозе:

ОО реализует ФБ защиты от указанной угрозы путем реализации для предотвращения визуального перехвата вводимой аутентификационной информации метода защиты обратной связи при вводе аутентификационной информации при доступе к функциональным возможностям (мера защиты информации ИАФ.5): вводимые символы пароля отображаются условными знаками. Для минимизации вероятности получения доступа методом подбора пароля реализована возможность задания параметров сложности парольной информации (в рамках реализации требований меры защиты информации ИАФ.4). Аутентификационная информация не передается в открытом виде.

Угроза-2: Угроза использования механизмов авторизации для повышения привилегий.

Описание угрозы: Угроза заключается в возможности получения нарушителем доступа к данным и функциям, предназначенным для учётных записей с более высокими чем у нарушителя привилегиями, за счёт ошибок в параметрах настройки средств разграничения доступа. При этом нарушитель для повышения своих привилегий не осуществляет деструктивное программное воздействие на систему, а лишь использует существующие ошибки.

Источники угрозы: Внутренний нарушитель с низким потенциалом; Внешний нарушитель со средним потенциалом.

Принятые меры противодействия угрозе:

ОО реализует ФБ защиты от указанной угрозы путем задействования функция ролевого метода разграничения доступа к выполнению операций (меры защиты УПД.2, УПД.4) в соответствии техническими условиями;

Угроза-3: Угроза несанкционированного изменения аутентификационной информации.

Описание угрозы: Угроза заключается в возможности осуществления неправомерного доступа нарушителем к аутентификационной информации других пользователей с помощью штатных средств операционной системы или специальных программных средств.

Источники угрозы: Внутренний нарушитель с низким потенциалом; Внешний нарушитель со средним потенциалом.

Принятые меры противодействия угрозе:

ОО реализует ФБ защиты от указанной угрозы путем задействования функции ролевого метода разграничения доступа к выполнению операций (меры защиты УПД.2, УПД.4) в соответствии техническими условиями.

Угроза-4: Угроза обхода некорректно настроенных механизмов аутентификации.

Описание угрозы: Угроза заключается в возможности получения нарушителем привилегий в системе без прохождения процедуры аутентификации за счёт выполнения действий, нарушающих условия корректной работы средств аутентификации (например, ввод данных неподдерживаемого формата).

Источники угрозы: Внутренний нарушитель с низким потенциалом; Внешний нарушитель со средним потенциалом.

Принятые меры противодействия угрозе:

ОО реализует ФБ защиты от указанной угрозы путем реализации механизма контроля аутентификационной информации при ее вводе, реализована настройка параметров сложности парольной информации, не допускающая применения «пустых» паролей, или паролей, обладающих низкой сложностью (в части реализации меры защиты ИАФ.4), настройка параметров парольной защиты выполняется администратором программного изделия.

Угроза-5: Угроза повышения привилегий.

Описание угрозы: Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на дискредитируемый процесс (или систему) или на другие процессы (или системы) от его (её) имени путём эксплуатации неправомерно полученных нарушителем дополнительных прав на управление дискредитированным объектом.

Источники угрозы: Внешний нарушитель со средним потенциалом; Внутренний нарушитель со средним потенциалом.

Принятые меры противодействия угрозе:

ОО реализует ФБ защиты от указанной угрозы путем задействования функции ролевого метода разграничения доступа к выполнению операций (меры защиты УПД.2, УПД.4) в соответствии техническими условиями.

Угроза-6: Угроза несанкционированного воздействия на средство защиты информации.

Описание угрозы: Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к программной среде управления средством защиты информации и изменения режима его функционирования.

Источники угрозы: Внешний нарушитель со средним потенциалом; Внутренний нарушитель со средним потенциалом.

Принятые меры противодействия угрозе:

ОО реализует ФБ защиты от указанной угрозы путем задействования функции ролевого метода разграничения доступа к выполнению операций (меры защиты УПД.2, УПД.4) в соответствии техническими условиями.