**Модель угроз безопасности   
системы защищенного хранения**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Наименование угрозы | Возможность реализации | Опасность угрозы | Актуальность угрозы | Меры по противодействию угрозе |
| **Угрозы несанкционированного доступа к информации** | | | | |
| **Угрозы физического доступа к элементам системы** | | | | |
| Получение несанкционированного физического доступа к серверу | Низкая | Высокая | Актуальная | Ограничение физического доступа к серверу;  Шифрование данных на сервере;  Опломбирование; |
| Получение несанкционированного физического доступа к ЭВМ-клиентам | Средняя | Средняя | Актуальная | Запрос пароля при входе в ЭВМ-клиент;  Запрос пароля клиента при подключении к серверу;  Запрет внешних подключений через ЭВМ-клиенты; |
| Получение несанкционированного физического доступа к каналам связи с дальнейшим подключением несанкционированных устройств | Низкая | Средняя | Неактуальная | Запрет внешних подключений;  Запрет беспроводных подключений;  Идентификация устройств по уникальным значениям (напр., номер жесткого диска); |
| **Угрозы преднамеренных действий и нарушений безопасности системы** | | | | |
| Заражение компьютеров системы | Средняя | Средняя | Актуальная | Защита компьютеров антивирусом; |
| Загрузка вредоносного файла или вируса на сервер | Высокая | Высокая | Актуальная | Защита сервера антивирусом;  Запрет на загрузку на сервер определенных разрешений (напр., .EXE); |
| Перехват информации при передаче по каналам связи | Низкая | Средняя | Неактуальная | Запрет внешних подключений;  Запрет беспроводных подключений; |
| Получение доступа к файлам других клиентов | Средняя | Средняя | Актуальная | Разграничение доступа к файлам клиентов; |
| Получение доступа к базам данных, содержащим информацию о клиентах | Низкая | Высокая | Актуальная | Запрет на отображение файлов БД клиентам; |
| **Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования системы** | | | | |
| Загрузка конфиденциальных файлов в публичный каталог | Высокая | Средняя | Актуальная | Организационные меры;  Запрет перемещения файлов между частным и публичным каталогом; |
| Переполнение хранилища сервера | Средняя | Средняя | Актуальная | Ограничение суммарного размера файлов клиента по 3 каталогам (частный, публичный, «корзина»);  Ограничение максимального размера файлов;  Уничтожение файлов в корзине через 3 дня нахождения в ней; |
| Совпадение названий загружаемого и существующего в системе файла | Высокая | Низкая | Актуальная | Принудительное переименование загружаемого файла; |
| Создание слабого пароля | Высокая | Средняя | Актуальная | Определение правил создания пароля; |
| Непреднамеренное удаление файла | Высокая | Низкая | Актуальная | Перемещение удаленных файлов в «корзину» |
| **Угрозы ошибок работы системы и отказов в обслуживании** | | | | |
| Отключение сервера или отказ в работе | Средняя | Средняя | Актуальная | Оповещение клиентов о недоступности сервера |
| Повреждение файлов в процессе хранения | Низкая | Средняя | Неактуальная | Создание резервных копий хранилища (2 полных ежедневных копии системы);  Проверка контрольных сумм MD5 файлов при запуске системы; |
| Повреждение файлов в процессе передачи | Средняя | Средняя | Актуальная | Проверка контрольных сумм MD5 оригинального и загруженного файлов после передачи файла; |
| Программные ошибки при внесении данных в БД и проверке аутентификационных данных | Низкая | Средняя | Неактуальная |  |