МойОфис

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

Комплекс средств защиты платформы МойОфис

КСЗ МойОфис обеспечивает выполнение следующих функций по защите информации в соответствии с «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (утверждены приказом ФСТЭК России № 17 от 11.02.2013), «Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждены приказом ФСТЭК России № 21 от 18.02.2013) и «Меры защиты информации в государственных информационных системах» (утверждены ФСТЭК России от 11.02.2014):

1) ИАФ.1 Идентификация и аутентификация пользователей, являющихся работниками оператора;

2) ИАФ.3 Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;

3) ИАФ.У3.1б Исключение повторного использования идентификатора пользователя в течение не менее трех лет;

4) ИАФ.У3.2б Блокирование идентификатора пользователя через период времени неиспользования не более 45 дней;

5) ИАФ.4 Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;

6) ИАФ.У4.1г Длина пароля не менее восьми символов, алфавит пароля не менее 70 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 4 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 15 до 60 минут, смена паролей не более чем через 60 дней;

7) ИАФ.5 Защита обратной связи при вводе аутентификационной информации;

8) ИАФ.6 Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей);

9) УПД.1 Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;

10) УПД.У1.1 Автоматизированные средства поддержки управления учетными записями пользователей;

11) УПД.У1.2 Автоматическое блокирование временных учетных записей пользователей по окончании установленного периода времени для их использования;

12) УПД.У1.3б Автоматическое блокирование неактивных (неиспользуемых) учетных записей пользователей после периода времени неиспользования более 45 дней;

13) УПД.2 Реализация необходимых методов (дискреционный), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;

14) УПД.У2.4 Управление доступом субъектов к объектам, создаваемым прикладным и специальным программным обеспечением;

15) УПД.6 Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе);

16) УПД.У6.3 Противодействие автоматизированному подбору паролей с использованием однократных кодов, требующих визуального распознавания (в том числе с использованием технологии CAPTCHA);

17) УПД.10 Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу;

18) УПД.11 Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации;

19) РСБ.1 Определение событий безопасности, подлежащих регистрации, и сроков их хранения;

20) РСБ.У1.2 Определение событий безопасности, подлежащих регистрации, связанных с действиями от имени привилегированных учетных записей (администраторов);

21) РСБ.У1.3 Определение событий безопасности, подлежащих регистрации, связанных с изменением привилегий учетных записей;

22) РСБ.2 Определение состава и содержания информации о событиях безопасности, подлежащих регистрации;

23) РСБ.У2.1а Запись дополнительной информации о событиях безопасности, включающую полнотекстовую запись привилегированных команд (команд, управляющих системными функциями);

24) РСБ.У2.3 Индивидуальная регистрация пользователей групповых учетных записей;

25) РСБ.У2.4 Регистрация информации о месте (сетевой адрес), с которого осуществляется вход субъектов доступа в информационную систему;

26) РСБ.У2.6 Запись следующей информации, связанной с доступом к объектам доступа (в частности к файлам):

– тип доступа (в том числе чтение, исполнение, запись и (или) иные типы);

– изменение атрибутов объектов доступа (права доступа, контрольные суммы, размер, содержание, путь, тип и (или) иные атрибуты);

– продолжительность доступа;

27) РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;

28) РСБ.УЗ.1 Централизованное автоматизированное управление сбором, записью и хранением информации о событиях безопасности;

29) ОЦЛ.8 Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях.

Пользователю КСЗ МойОфис доступны следующие настройки:

– настройка времени, в течение которого пользователь переходит в статус «заблокирован» и не имеет возможности осуществления входа в систему от своего имени,

– настройка времени, в течение которого система отслеживает совершение пользователем неуспешных действий,

– настройка числа неуспешных (подряд) попыток авторизации, после которых пользователю предлагается ввести код CAPTCHA,

– настройка максимально допустимого числа попыток входа в систему в течение периода,

– настройка исключения блокировки доступа для внутренних адресов, настройка адресов, являющихся для системы внутренними, доступ с которых не подлежит блокировке,

– настройка допустимого периода получения запросов с одного ip-адреса (ddos_period),

– настройка допустимого числа запросов в течение ddos_period секунд с одного ip-адреса,

– настройка допустимого периода времени попыток доступа с одного ip-адреса (bruteforce_period),

– настройка допустимого числа неверных попыток доступа в течение bruteforce_period времени с одного ip-адреса.