Соответствие мерам защиты ФСТЭК

Оглавление

Введение

Вопросы защиты информации и соответствия требованиям законодательства являются ключевыми для организаций, работающих с персональными данными, государственными информационными системами и критически важными ИТ-объектами.

Платформа RooX UIDM поддерживает реализацию мер защиты информации, установленных нормативными документами ФСТЭК России, и может использоваться в составе инфраструктуры организаций, которым необходимо соблюдение обязательных требований.

Области применения

RooX UIDM предназначен для применения

- в государственных информационных системах до 1 класса защищенности включительно согласно требованиям приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах»
- в информационных системах персональных данных до 1 класса защищенности включительно согласно требованиям приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
- в автоматизированных системах управления до 1 класса защищенности включительно согласно требованиям приказа ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»
- в значимых объектах до 1 категории включительно согласно требованиям приказа ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

- в информационных системах общего пользования до II класса защищенности включительно согласно требованиям приказа ФСТЭК России от 31 августа 2010 г. № 489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования».

Меры защиты

RooX UIDM предназначен для применения в вышеуказанных системах для реализации следующих мер защиты.

Идентификация и аутентификация

- **ИАФ.1** Идентификация и аутентификация пользователей, являющихся работниками оператора;
- **ИАФ.2** Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных
- **ИАФ.3** Управление идентификаторами, в том числе создание, присвоение, редактирование, уничтожение идентификаторов;
- **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;
- **ИАФ.5** Защита обратной связи при вводе аутентификационной информации;
- **ИАФ.6** Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей);

Управление доступом

- **УПД.1** Управление (заведение, корректировку, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;
- **УПД.2** Реализация необходимых методов (ролевой, атрибутный), типов (чтение, запись, редактирование, удаление) и правил разграничения доступа;
- **УПД.4** Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;
- **УПД.5** Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;
- **УПД.6** Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе);
- **УПД.7** Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры защиты информации, и о необходимости соблюдения им установленных оператором правил обработки информации;
- **УПД.8** Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему;
- **УПД.9** Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы;
- **УПД.10** Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу;
- **УПД.11** Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации;
- **УПД.13** Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети;
- **УПД.14** Регламентация и контроль использования в информационной системе технологий беспроводного доступа;
- **УПД.16** Управление взаимодействием с информационными системами сторонних организаций (внешние

информационные системы);

Регистрация событий безопасности

- **РСБ.1** Определение событий безопасности, подлежащих регистрации, и сроков их хранения;
- **РСБ.2** Определение состава и содержания информации о событиях безопасности, подлежащих регистрации;
- **РСБ.3** Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- **РСБ.4** Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти;
- **РСБ.5** Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;
- **РСБ.7** Защита информации о событиях безопасности;
- **РСБ.8** Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе;

Контроль (анализ) защищенности информации

- **АНЗ.5** Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе;

Защита информационных систем

- **ЗИС.1** Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы;
- **ЗИС.11** Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов.