1.1.2.4 Функциональные характеристики

ПК представляет собой набор инструментов, используемых для мониторинга и реагирования на инциденты безопасности в защищаемой инфраструктуре, при этом обеспечивается выполнение ряда функций безопасности (ФБ):

1.1.2.4.1 Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)

1.1.2.4.1.1 Идентификация и аутентификация пользователей ОО (ИАФ.1)

ПК реализует идентификацию и аутентификацию пользователей для всех видов доступа с использованием паролей и запрещением любых действий пользователей до выполнения аутентификации.

ПК выполняет меру безопасности (ИАФ.1) «Идентификация и аутентификация пользователей ОО».

В части следующих требований к мере защиты информации ИАФ.1:

– идентификация и аутентификация пользователей ОО;

– аутентификация пользователя осуществляется с использованием паролей.

1.1.2.4.1.2 Управление средствами аутентификации (ИАФ.4)

ПК предоставляет (посредством приложения «Администратор») механизм управления средствами аутентификации (в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации).

В части следующих требований к мере защиты информации ИАФ.4:

– защита аутентификационной информации от неправомерного доступа к ней и модифицирования.

1.1.2.4.1.3 Защита обратной связи при вводе аутентификационной информации (ИАФ.5)

ПК обеспечивает исключение отображения для пользователя действительного значения аутентификационной информации при вводе пароля.

В части следующих требований к мере защиты информации ИАФ.5:

– защита обратной связи при вводе аутентификационной информации путем исключения отображения для пользователя действительного значения аутентификационной информации с заменой вводимых символов пароля условным знаком «*».

1.1.2.4.2 Управление доступом субъектов доступа к объектам доступа (УПД)

1.1.2.4.2.1 Управление учетными записями пользователей (УПД.1)

ПК предоставляет механизм управления (заведение, активация, блокирование и уничтожение) учетными записями пользователей.

В части следующих требований к мере защиты информации УПД.1:

– управление учетными записями пользователей, назначение или отзыв соответствующих ролей пользователей, объединение пользователей в ролевые группы;

– функции заведения, активации, блокирования и уничтожения учетных записей пользователей.

1.1.2.4.2.2 Реализация ролевого метода управления доступом (УПД.2)

ПК обеспечивает ролевой метод управления доступом.

В части следующих требований к мере защиты информации УПД.2:

– ПК обеспечивает ролевой метод управления пользователями, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа;

– ПК обеспечивает ведение произвольного набора ролей с правами доступа

– ПК обеспечивает назначение пользователям ролей с правами доступа.

1.1.2.4.2.3 Разделение обязанностей полномочий (ролей), администраторов и лиц, обеспечивающих функционирование информационной системы (УПД.4)

В части следующих требований к мере защиты информации УПД.4:

– ПК обеспечивает разделение обязанностей полномочий (ролей), администраторов и лиц, отвечающих за функционирование информационной системы.

1.1.2.4.2.5 Блокирование сеанса доступа

ПК обеспечивает блокирование сеанса доступа к Web-интерфейсу.

В части следующих требований к мере защиты информации УПД.10:

Обеспечивает блокирование сеанса доступа пользователя после заданного времени его бездействия (неактивности) в ПК.

В части следующих требований к усилению меры защиты информации УПД.10:

– ПК обеспечивает блокирование сеанса доступа пользователя после времени бездействия (неактивности) пользователя до 5 мин;

– на устройстве отображения (мониторе) после блокировки сеанса не должна отображаться информация сеанса пользователя (в том числе использование «хранителя экрана», гашение экрана или иные способы).

1.1.2.4.3 Регистрация событий безопасности (РСБ)

1.1.2.4.3.1 ПК выполняет сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения

В части следующих требований к мере защиты информации РСБ.3:

– ПК обеспечивает сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;

– ПК предоставляет возможность администратору в текущий момент времени выбирать события безопасности.

Регистрируются следующие события безопасности:

– вход/выход в/из систему(ы);

– действия с данными в БД.

Для каждого события безопасности регистрируются:

– тип события безопасности;

– идентификатор пользователя;

– дата и время события безопасности.