ALD Pro

ALD Pro 3.2.0c

Реализация мер
Приказа ФСТЭК России №117

Содержание

I Идентификация и аутентификация (ИАФ) 3
II Управление доступом (УПД) 4
III Регистрация событий безопасности (РСБ) 8
IV Защита виртуализации и облачных вычислений (ЗСВ) 9
V Защита технологий контейнерных сред и их оркестрации (ЗКО) 11
VI Защита сервисов электронной почты (ЗЭП) 13
VII Защита веб-технологий (ЗВТ) 14
VIII Защита программных интерфейсов взаимодействия приложений (API) (ЗПИ) 16
IX Защита конечных устройств (ЗКУ) 17
X Защита мобильных устройств (ЗМУ) 18
XI Защита технологий «интернета вещей» (ЗИВ) 21
XII Защита точек беспроводного доступа (ЗБД) 21
XIII Антивирусная защита (АВЗ) 22
XIV Обнаружение и предотвращение вторжений на сетевом уровне (СОВ) 23
XV Сегментация и межсетевое экранирование (МСЭ) 23
XVI Защита от компьютерных атак, направленных на отказ в обслуживании (ЗОО) 25
XVII Защита каналов связи и сетевого взаимодействия (ЗКС) 26

Легенда

1	ALD Pro реализует меру в соответствии с формуляром (совместно с ОС Astra Linux)
2	ALD Pro реализует совместно со средой функционирования
3	Мера реализуется клиентом домена - ALSE, имеется групповая политика
4	Мера реализуется клиентом домена - ALSE, есть возможность реализации с помощью групповой политики
5	Мера реализуется сторонними средствами
6	Организационная мера

Меры защиты и обеспечения безопасности		Классы защищенности ИС			Описание	Реализация
Код	Наименование меры	3	2	1		
I Идентификация и аутентификация (ИАФ)						
ИАФ.1	Идентификация пользователей	+	+ 1	+ 1	Реализуется средствами ALD Pro согласно формуляру. *Примечание: В соответствии с формуляром, реализацию отдельных мер защиты ALD Pro обеспечивает только совместно с ОС Astra Linux*	За идентификацию и аутентификацию пользователей в ALD Pro отвечают доменные службы из состава ОС Astra Linux - Kerberos для аутентификации, LDAP - для идентификации.
ИАФ.2	Идентификация устройств				Реализуется средствами ALD Pro согласно формуляру. *Примечание: В соответствии с формуляром, реализацию отдельных мер защиты ALD Pro обеспечивает только совместно с ОС Astra Linux*	Идентификация и аутентификация компьютеров выполняется средствами Kerberos. На доменном компьютере хранится файл (/etc/krb5.keytab), содержащий криптографические ключи его учетной записи Kerberos. Вместо пароля устройство использует эти ключи для получения билетов Kerberos и доступа к сетевым службам, таким как LDAP или SSH. За идентификацию съемных носителей при подключении к компьютеру отвечает менеджер устройств udev - служба из состава ОС. ALD Pro позволяет осуществлять регистрацию съемных носителей в базе учета устройств с использованием веб-интерфейса путем создания записей об этих устройствах и глобальных правил для устройств: **Управление доменом → МРД → Учтенные устройства**
ИАФ.3	Аутентификация пользователей	+	+	+ 1	Реализуется средствами ALD Pro согласно формуляру. *Примечание: В соответствии с формуляром, реализацию отдельных мер защиты ALD Pro обеспечивает только совместно с ОС Astra Linux*	За идентификацию и аутентификацию пользователей в ALD Pro отвечают доменные службы из состава ОС Astra Linux - Kerberos для аутентификации, LDAP - для идентификации.

Меры защиты и обеспечения безопасности		Классы защищенности ИС			Описание	Реализация
Код	Наименование меры	3	2	1		
ИАФ.4	Аутентификация устройств				Реализуется средствами ALD Pro согласно формуляру. *Примечание:* *В соответствии с формуляром, реализацию отдельных мер защиты ALD Pro обеспечивает только совместно с ОС Astra Linux*	Идентификация и аутентификация компьютеров выполняется средствами Kerberos. На доменном компьютере хранится файл (/etc/krb5.keytab), содержащий криптографические ключи его учетной записи Kerberos. Вместо пароля устройство использует эти ключи для получения билетов Kerberos и доступа к сетевым службам, таким как LDAP или SSH. За идентификацию съемных носителей при подключении к компьютеру отвечает менеджер устройств udev - служба из состава ОС. Аутентификация внешних устройств осуществляется с использованием средств контроля подключения машинных носителей информации – менеджера устройств udev, обеспечивающего надежное сопоставление пользователя с устройством и записями об устройстве. ALD Pro позволяет осуществлять регистрацию съемных носителей в базе учета устройств с использованием веб-интерфейса путем создания записей об этих устройствах и глобальных правил для устройств: **Управление доменом → МРД → Учтенные устройства**
II Управление доступом (УПД)						
УПД.1	Реализация модели управления доступом	+	+ 1, 2	+ 1, 2	Взаимодействуя с реализованными в ОС моделями управления доступом, ALD Pro поддерживает: • дискреционное управление доступом • мандатное управление доступом • ролевое управление доступом	Дискреционное управление доступом: На портале управления пользователю можно задать UID и включить в группы: **Пользователи и компьютеры → Пользователи → <Имя пользователя> → <Идентификатор пользователя (UID)>** **Пользователи и компьютеры → Пользователи → <Имя пользователя> → Группы** С использованием консольных утилит FreeIPA: **ipa user-add username <имя> --uidnumber=<номер>** **ipa group-add-member groupname --users=username**

Меры защиты и обеспечения безопасности		Классы защищенности ИС			Описание	Реализация
Код	Наименование меры	3	2	1		
						Мандатное управление доступом: На портале управления ALD Pro можно задать уровень целостности, привилегии PARSEC, уровни и категории конфиденциальности пользователя **Управление доменом → МРД** Ролевое управление доступом: На портале управления пользователю можно назначить роли: **Пользователи и компьютеры → Пользователи → <Имя пользователя> → Роли**
УПД.2	Разграничение и контроль прав доступа	+	+ 1	+ 1, 2	Реализуется средствами ALD Pro согласно формуляру. *Примечание: В соответствии с формуляром, реализацию отдельных мер защиты ALD Pro обеспечивает только совместно с ОС Astra Linux*	ALD Pro реализует назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы с помощью механизмов повышения привилегий SUDO и разграничения доступа к собственным функциям. 1. Разграничение доступа к функциям ALD Pro: **Пользователи и компьютеры → Пользователи → <Имя пользователя> → Роли** 2. Механизм повышения привилегий sudo: **Групповые политики → Политики повышения привилегий** При создании нового пользователя ему назначаются минимально возможные права.
УПД.3	Управление учетными записями	+	+ 1	+ 1, 2	Реализуется средствами ALD Pro согласно формуляру. *Примечание: В соответствии с формуляром, реализацию отдельных мер защиты ALD Pro обеспечивает только совместно с ОС Astra Linux*	ALD Pro реализует следующий функционал: • создание, назначение, активацию, блокирование и удаление учетных записей; • учет учетных записей; • назначение, изменение, удаление правил доступа учетных записей; • объединение учетных записей в группы учетных записей; • регистрацию событий безопасности, связанных с управлением учетными записями.

Меры защиты и обеспечения безопасности		Классы защищенности ИС			Описание	Реализация
Код	Наименование меры	3	2	1		
						Создание учетной записи: **Пользователи и компьютеры → Пользователи → Создать** Удаление учетной записи: **Пользователи и компьютеры → Пользователи → <имя учетной записи> → Удалить учетную запись** Блокирование учетной записи: **Пользователи и компьютеры → Пользователи → <имя учетной записи> → Заблокировать УЗ** Активация учетной записи: **Пользователи и компьютеры → Пользователи → <имя учетной записи> → Разблокировать УЗ** Перечень учетных записей: **Пользователи и компьютеры → Пользователи** Изменение правил доступа учетной записи реализуется включением пользователя в группы, назначением учетной записи ролей, назначением мандатных атрибутов Регистрация событий безопасности реализуется средой функционирования ALSE
УПД.4	Ограничение неуспешных и нерегламентированных попыток доступа в информационную систему	+	+ 1, 2	+ 1, 2	ALD Pro реализует ограничение числа неуспешных попыток входа. *Примечание: В соответствии с формуляром, реализацию отдельных мер защиты ALD Pro обеспечивает только совместно с ОС Astra Linux*	Ограничение реализуется с использованием портала управления: **Групповые политики → Политики паролей → <имя политики> → Максимальное количество ошибок**
УПД.5	Предупреждение пользователя при его доступе к информационной системе				ALD Pro реализует групповую политику для централизованной настройки предупреждения пользователя при графическом доступе к клиенту домена ALSE. Возможна централизованная настройка предупреждения пользователя при	Централизованная настройка предупреждения пользователя при графическом доступе к клиенту домена ALSE: **Групповые политики → Групповые политики → <имя_групповой_политики> → Параметры компьютеров → Система → Вход в систему → Диалог. Поле: Настройка атрибутов → Приглашение.** В данном поле можно определить текст, который будет продемонстрирован

Меры защиты и обеспечения безопасности		Классы защищенности ИС			Описание	Реализация
Код	Наименование меры	3	2	1		
					консольном доступе к клиенту домена ALSE при разработке дополнительной групповой политики.	пользователю при показе окна авторизации.
УПД.6	Оповещение пользователя о предыдущем входе в информационную систему				Реализуется средой функционирования ALSE - оповещение последнего входа доменного пользователя. ALD Pro реализует групповую политику для централизованной настройки оповещения пользователя о предыдущем входе в информационную систему.	Сведения о предыдущей аутентификации, количестве успешных и неуспешных попыток входа предоставляются пользователю автоматически при входе пользователя в систему. Настройка с помощью групповой политики: **Групповые политики → Групповые политики → <имя_групповой_политики> → Параметры компьютеров → Политики мер защиты ФСТЭК России → Авторизация → Отображение информации о сеансе пользователя**
УПД.7	Ограничение числа параллельных сеансов доступа		+	+ 1а	Реализуется клиентом домена - ALSE, имеется групповая политика для настройки числа параллельных сансов доступа. ALD Pro реализует групповую политику для централизованного ограничения числа параллельных сеансов доступа пользователя в пределах одного АРМ.	Настройка ограничение числа параллельных сеансов доступа для всех учетных записей домена: **Групповые политики → <имя_групповой_политики> → Параметры компьютеров → Политики мер защиты ФСТЭК России → Ограничение числа параллельных сеансов → Количество параллельных сеансов**
УПД.8	Блокирование сеанса доступа пользователя при неактивности	+	+	+	Реализуется клиентом домена - ALSE, имеется групповая политика для централизованной настройки блокирования санаса пользователя при неактивности. ALD Pro реализует групповую политику для централизованного ограничения числа параллельных сеансов доступа пользователя в пределах одного АРМ.	Настройка ограничение числа параллельных сеансов доступа для всех учетных записей домена: **Групповые политики → <имя_групповой_политики> → Параметры компьютеров → Политики мер защиты ФСТЭК России → Авторизация → Блокировка экрана после бездействия**

Меры защиты и обеспечения безопасности		Классы защищенности ИС			Описание	Реализация
Код	Наименование меры	3	2	1		
УПД.9	Контроль действий субъектов доступа до идентификации и аутентификации	+	+	+	Реализуется средствами ALD Pro. Для клиентов домена реализуется средой функционирования ALSE по умолчанию.	Любые действия пользователя на портале управления ALD Pro (в графическом web интерфейсе или с использованием API) запрещены до прохождения идентификации и аутентификации. Защищенная графическая подсистема ALSE обеспечивает запрет пользователям на любые действия до прохождения процедур идентификации и аутентификации.
III Регистрация событий безопасности (РСБ)						
РСБ.1	Определение событий безопасности и данных о них, подлежащих регистрации	+ 1	+ 1, 2	+ 1, 2, 3	Реализуется организационными мерами	—
РСБ.2	Анализ событий безопасности и реагирование на них	+	+	+	Реализуется SIEM системами, средствами обнаружения вторжений	—
РСБ.3	Генерация временных меток при регистрации событий безопасности	+	+	+	Реализуется средой функционирования ALSE - контроллер домена является сервером точного времени. Ценрализованное развертывание и настройка сервера точного времени реализуется ALD Pro.	Развертывание сервера точного времени и настройка: **Роли и службы сайта → Служба синхронизации времени.** Есть возможность определить внешний пул NTP серверов и корневые NTP серверы домена
РСБ.4	Требования к сбору, хранению и защите данных о событиях безопасности	+	+	+	Реализуется средой функционирования ALSE. Централизованное развертывание и настройка сервера журнала событий реализуется ALD Pro.	Сбор, запись и хранение информации о событиях безопасности в ALSE осуществляются с помощью подсистемы регистрации событий путем ведения журналов аудита событий безопасности согласно заданным правилам. Состав регистрируемой информации соответствует ГОСТ Р 59548-2022. ALD Pro позволяет централизованно развернуть в домене сервер журнала событий, а также настроить сбор журналов событий: **Журнал событий → Серверы журнала событий, Настройка сбора журналов событий**

Меры защиты и обеспечения безопасности		Классы защищенности ИС			Описание	Реализация
Код	Наименование меры	3	2	1		
РСБ.5	Реагирование на сбои при регистрации событий безопасности	+	+	+	Реализуется ALD Pro путем централизованного развертывания и настройки сервера мониторинга Zabbix. Реализуется средой функционирования ALSE - клиент домена реализует механизм уведомлений пользователя, в т.ч. о сбоях в работе системы регистрации событий	Развертывание сервер мониторинга Zabbix **Мониторинг → Журнал событий мониторинга → Серверы мониторинга** Параметры уведомлений службы astra-event-watcher определены в файле /usr/share/knotifications5/astra-event-watcher.notifyrc. Также параметры можно настроить с помощью графической утилиты «Настройка регистрации системных событий» (fly-admin-events). С помощью подсистемы регистрации событий fly-admin-events (astra-admin-events) можно настроить оповещение о сбоях в системе регистрации событий: остановка служб syslog-ng, auditd, удаление журнала событий, исчерпание свободного дискового пространства. Параметры уведомлений для определенного пользователя могут быть переопределены в файле /home/<имя_пользователя>/.config/astra-event-watcher.notifyrc.
IV Защита виртуализации и облачных вычислений (ЗСВ)						
ЗСВ.1	Доверенная загрузка средства виртуализации и виртуальных машин	+	+ 1	+ 1, 2	При использовании виртуалиации ALSE, мера реализуется клиентом домена. Возможна централизованная настройка при разработке дополнительной групповой политики.	Реализуется средой функционирования ALSE в соответствии с https://wiki.astralinux.ru/pages/viewpage.action?pageId=471538657 (механизмы контроля целостности в среде виртуализации, ЗСВ.1)
ЗСВ.2	Контроль целостности средств виртуализации и виртуальных машин	+	+ 1	+ 1, 2	При использовании виртуалиации ALSE, мера реализуется клиентом домена. Возможна централизованная настройка при разработке дополнительной групповой политики.	Реализуется средой функционирования ALSE в соответствии с https://wiki.astralinux.ru/pages/viewpage.action?pageId=471538657 (механизмы контроля целостности в среде виртуализации, ЗСВ.2)

Меры защиты и обеспечения безопасности		Классы защищенности ИС			Описание	Реализация
Код	Наименование меры	3	2	1		
ЗСВ.3	Регистрация событий безопасности в среде виртуализации	+	+	+	При использовании виртуализации ALSE, мера реализуется клиентом домена. Возможна централизованная настройка при разработке дополнительной групповой политики.	Реализуется средой функционирования ALSE в соответствии с https://wiki.astralinux.ru/pages/viewpage.action?pageId=471538657 (регистрация событий в среде виртуализации, ЗСВ.3)
ЗСВ.4	Управление доступом в среде виртуализации	+	+	+	При использовании виртуализации ALSE, мера реализуется клиентом домена по умолчанию	Реализуется средой функционирования ALSE в соответствии с https://wiki.astralinux.ru/pages/viewpage.action?pageId=471538657 (управление доступом в среде виртуализации, ЗСВ.4)
ЗСВ.5	Резервное копирование в среде виртуализации	+	+	+	При использовании виртуализации ALSE, мера реализуется клиентом домена. Возможна централизованная настройка при разработке дополнительной групповой политики.	Реализуется средой функционирования ALSE в соответствии с https://wiki.astralinux.ru/pages/viewpage.action?pageId=471538657 (резервное копирование в среде виртуализации, ЗСВ.5)
ЗСВ.6	Ограничение программной среды в среде виртуализации	+	+	+ 1	При использовании виртуализации ALSE, мера реализуется клиентом домена. Имеется групповая политика для настройки ограничения программной среды на хосте виртуализации Astra Linux.	Реализуется средой функционирования ALSE в соответствии с https://wiki.astralinux.ru/pages/viewpage.action?pageId=471538657 (ограничение программной среды в среде виртуализации, ЗСВ.6) **Групповые политики → <имя групповой политики> → Параметры компьютеров → Политика безопасности → Замкнутая программная среда** **Групповые политики → <имя групповой политики> → Параметры компьютеров → Политика безопасности → Политика консоли и интерпретаторов**
ЗСВ.7	Защита памяти в среде виртуализации	+	+	+	При использовании виртуализации ALSE, мера реализуется клиентом домена. Имеется групповая политика для настройки ограничения программной	Реализуется средой функционирования ALSE в соответствии с https://wiki.astralinux.ru/pages/viewpage.action?pageId=471538657 (защита памяти в среде виртуализации, ЗСВ.7)

Меры защиты и обеспечения безопасности		Классы защищенности ИС			Описание	Реализация
Код	Наименование меры	3	2	1		
					среды на хосте виртуализации Astra Linux.	**Групповые политики → <имя групповой политики> → Параметры компьютеров → Политики очистки памяти → Настройка гарантированного удаления файлов на устройстве / Настройки**
ЗСВ.8	Идентификация и аутентификация в среде виртуализации	+	+	+	При использовании виртуалиации ALSE, мера реализуется клиентом домена по умолчанию.	Реализуется средой функционирования ALSE в соответствии с https://wiki.astralinux.ru/pages/viewpage.action?pageId=471538657 (идентификация и аутентификация в среде виртуализации, ЗСВ.8)
ЗСВ.9	Управление виртуальными машинами		+	+	При использовании виртуалиации ALSE, мера реализуется клиентом домена. Возможна централизованная настройка при разработке дополнительной групповой политики.	Реализуется средой функционирования ALSE в соответствии с https://wiki.astralinux.ru/pages/viewpage.action?pageId=471538657 (управление виртуальными машинами, ЗСВ.9)
V Защита технологий контейнерных сред и их оркестрации (ЗКО)						
ЗКО.1	Контроль целостности в контейнерных средах	+ 1	+ 1, 2	+ 1, 2, 3, 4, 5, 6	При использовании механизмов контейнеризации из состава ALSE, мера реализуется клиентом домена. Имеются групповые политики для настройки контроля целостности хостовой ОС. Реализация контроля целостности средства контейнеризации реализуется клиентом домена ALSE по умолчанию (Мандатный контроль целостности, Замкнутая программная среда).	Реализуется средой функционирования ALSE в соответствии с https://wiki.astralinux.ru/pages/viewpage.action?pageId=471538657 (контроль целостности в контейнерных средах, ЗКО.1) Групповые политики для настройки контроля целостности хостовой ОС: **Групповые политики → <имя групповой политики> → Параметры компьютеров → Безопасность → Мандатный контроль целостности (МКЦ)** **Групповые политики → <имя групповой политики> → Параметры компьютеров → Безопасность → Политика безопасности → Замкнутая программная среда** **Групповые политики → <имя групповой политики> → Параметры компьютеров → Безопасность → Проверка целостности системы**

Меры защиты и обеспечения безопасности		Классы защищенности ИС			Описание	Реализация
Код	Наименование меры	3	2	1		
ЗКО.2	Регистрация событий безопасности в контейнерных средах	+	+	+	При использовании механизмов контейнеризации из состава ALSE, мера реализуется клиентом домена. Возможна централизованная настройка при разработке дополнительной групповой политики.	Реализуется средой функционирования ALSE в соответствии с https://wiki.astralinux.ru/pages/viewpage.action?pageId=471538657 (регистрация событий безопасности в контейнерных средах, ЗКО.2)
ЗКО.3	Управление доступом в контейнерных средах	+	+	+	При использовании механизмов контейнеризации из состава ALSE, мера реализуется клиентом домена. Возможна централизованная настройка при разработке дополнительной групповой политики.	Реализуется средой функционирования ALSE в соответствии с https://wiki.astralinux.ru/pages/viewpage.action?pageId=471538657 (управление доступом в контейнерных средах, ЗКО.3)
ЗКО.4	Резервное копирование в контейнерных средах	+	+	+	При использовании механизмов контейнеризации из состава ALSE, мера реализуется клиентом домена. Возможна централизованная настройка при разработке дополнительной групповой политики.	Реализуется средой функционирования ALSE в соответствии с https://wiki.astralinux.ru/pages/viewpage.action?pageId=471538657 (резервное копирование в контейнерных средах, ЗКО.4)
ЗКО.5	Изоляция контейнеров в контейнерной среде	+	+ 1	+ 1	При использовании механизмов контейнеризации из состава ALSE, мера реализуется клиентом домена по умолчанию.	Реализуется средой функционирования ALSE в соответствии с https://wiki.astralinux.ru/pages/viewpage.action?pageId=471538657 (изоляция контейнеров в контейнерной среде, ЗКО.5)
ЗКО.6	Идентификация и аутентификация в контейнерной среде	+	+	+	При использовании механизмов контейнеризации из состава ALSE, мера реализуется клиентом домена по умолчанию.	Реализуется средой функционирования ALSE в соответствии с https://wiki.astralinux.ru/pages/viewpage.action?pageId=471538657 (идентификация и аутентификация в контейнерной среде, ЗКО.6)

Меры защиты и обеспечения безопасности		Классы защищенности ИС			Описание	Реализация
Код	Наименование меры	3	2	1		
ЗКО.7	Управление контейнерами и их образами (оркестрация)	+	+	+	При использовании механизмов контейнеризации из состава ALSE, мера реализуется клиентом домена по умолчанию.	Реализуется средой функционирования ALSE в соответствии с https://wiki.astralinux.ru/pages/viewpage.action?pageId=471538657 (управление контейнерами и их образами (оркестрация), ЗКО.7)
ЗКО.8	Выявление и устранение уязвимостей в контейнерной среде	+	+ 1, 2	+ 1, 2	При использовании механизмов контейнеризации из состава ALSE, мера реализуется клиентом домена. Возможна централизованная настройка при разработке дополнительной групповой политики.	Реализуется средой функционирования ALSE в соответствии с https://wiki.astralinux.ru/pages/viewpage.action?pageId=471538657 (выявление и устранение уязвимостей в контейнерной среде, ЗКО.8)
VI Защита сервисов электронной почты (ЗЭП)						
ЗЭП.1	Защита ящиков и сообщений электронной почты	+	+	+	При использовании защищенного комплекса программ электронной почты из состава ALSE, мера реализуется клиентом домена.	Реализуется средой функционирования ALSE в соответствии с https://wiki.astralinux.ru/pages/viewpage.action?pageId=471538657 (защита ящиков и сообщений электронной почты, ЗЭП.1)
ЗЭП.2	Управление доступом пользователей	+	+	+	При использовании защищенного комплекса программ электронной почты из состава ALSE, мера реализуется клиентом домена.	Реализуется средой функционирования ALSE в соответствии с https://wiki.astralinux.ru/pages/viewpage.action?pageId=471538657 (управление доступом пользователей, ЗЭП.2)
ЗЭП.3	Защита от вредоносных вложений	+	+	+	Реализуется сторонними средствами	–
ЗЭП.4	Защита от фишинга	+	+ 1	+ 1	Реализуется сторонними средствами	–
ЗЭП.5	Защита от спама	+	+	+	Реализуется сторонними средствами	–
ЗЭП.6	Защита метаданных и иной технической информации сервисов электронной почты	+	+	+	При использовании защищенного комплекса программ электронной почты из состава ALSE, мера реализуется клиентом домена.	Реализуется средой функционирования ALSE в соответствии с https://wiki.astralinux.ru/pages/viewpage.action?pageId=471538657 (защита метаданных и иной технической информации сервисов электронной почты, ЗЭП.6)

Меры защиты и обеспечения безопасности		Классы защищенности ИС			Описание	Реализация
Код	Наименование меры	3	2	1		
					Возможна централизованная настройка при разработке дополнительной групповой политики.	
VII Защита веб-технологий (ЗВТ)						
ЗВТ.1	Защита пользовательских данных	+	+	+	Для информационной системы мера реализуется средствами межсетевых экранов уровня приложений (WAF). При использовании web-сервера Apache из состава ALSE, мера может частично реализовываться клиентом домена. Возможна централизованная настройка web-сервера Apache на клиентах домена с помощью дополнительной групповой политики. ALD Pro реализует меру в части защиты пользовательских данных, обрабатываемых web-приложением «Портал управления» ALD Pro.	Реализуется средой функционирования ALSE в соответствии с https://wiki.astralinux.ru/pages/viewpage.action?pageId=471538657 (защита пользовательских данных, ЗВТ.1) Взаимодействие пользователя с web-приложением «Портал управления» реализуется в соответствии с требованиями меры ЗПИ.1 - API портала управления не доступен до аутентификации. Доступ пользователей к данным, хранящимся в веб-приложении «Портал управления», осуществляется в соответствии с требованиями меры УПД.2 - ALD Pro реализует разграничение и контроль прав доступа.
ЗВТ.2	Управление доступом пользователей	+ 1	+ 1	+ 1	Для информационной системы мера реализуется средствами межсетевых экранов уровня приложений (WAF). При использовании web-сервера Apache из состава ALSE, мера может частично реализовываться клиентом домена. Возможна централизованная настройка web-сервера Apache на клиентах домена с помощью дополнительной групповой политики.	Реализуется средой функционирования ALSE в соответствии с https://wiki.astralinux.ru/pages/viewpage.action?pageId=471538657 (управление доступом пользователей, ЗВТ.2). Для получения доступа к web-приложению «Портал управления» ALD Pro, необходимо пройти идентификацию и аутентификацию (выполняется в соответствии с мерами ИАФ.1 - ИАФ.3). Управление доступом пользователей web-приложения «Портал управления» ALD Pro реализуется в соответствии с мерами УПД.1 - УПД.4

Меры защиты и обеспечения безопасности		Классы защищенности ИС			Описание	Реализация
Код	Наименование меры	3	2	1		
					ALD Pro частично реализует меру в части управления доступом пользователей web-приложения «Портал управления» ALD Pro.	Веб-приложение «Портал управления» ALD Pro не поддерживает предупреждение пользователя при доступе в систему (УПД.5), оповещение пользователя о предыдущем входе на портал управления (УПД.6), ограничение параллельных сессий при работе на портале управления (УПД.7) и завершение сеанса доступа к порталу управления при неактивности (УПД.8).
ЗВТ.3	Контроль и фильтрация трафика веб-приложений	+	+	+ 1	Реализуется средствами межсетевых экранов уровня приложений (WAF). При использовании web-сервера Apache из состава ALSE, мера может частично реализовываться клиентом домена. Возможна централизованная настройка при разработке дополнительной групповой политики.	Частично реализуется средой функционирования ALSE в соответствии с https://wiki.astralinux.ru/pages/viewpage.action?pageId=471538657 (управление доступом пользователей, ЗВТ.2 - настройка управления доступа к ресурсам виртуального хоста, настройка мандатного управления доступом)
ЗВТ.4	Регистрация событий безопасности в веб-приложениях и реагирование на них	+	+	+	Реализуется средствами межсетевых экранов уровня приложений (WAF) При использовании web-сервера Apache из состава ALSE, мера может частично реализовываться клиентом домена. Возможна централизованная настройка при разработке дополнительной групповой политики.	Частично реализуется средой функционирования ALSE в соответствии с https://wiki.astralinux.ru/pages/viewpage.action?pageId=471538657 (управление доступом пользователей, ЗВТ.2 - настройка управления доступа к ресурсам виртуального хоста, настройка мандатного управления доступом)
ЗВТ.5	Проверка файлов, передаваемых веб-приложениями, на вредоносное программное обеспечение	+	+	+	Реализуется средствами межсетевых экранов уровня приложений (WAF) и средств антивирусной защиты (АВЗ)	–

Меры защиты и обеспечения безопасности		Классы защищенности ИС			Описание	Реализация
Код	Наименование меры	3	2	1		
VIII Защита программных интерфейсов взаимодействия приложений (API) (ЗПИ)						
ЗПИ.1	Защита данных API	+	+ 1	+ 1	Реализуется средствами межсетевых экранов уровня приложений (WAF) В части защиты ALD Pro - API не доступно до прохождения процедур идентификации и аутентификации.	Для получения доступа к ресурсам ALD Pro через API необходимо пройти идентификацию и аутентификацию (выполняется в соответствии с мерами ИАФ.1 - ИАФ.3) Выполнить ее можно следующими способами: 1. Используя kerberos аутентификацию 2. Передать логин/пароль на /api/ds/login При первом HTTP-запросе передаются логин и пароль. В ответ ALD Pro возвращает в заголовках Set-cookie параметры авторизации, которые при последующих HTTP-запросах можно будет использовать вместо передачи логина и пароля. Срок действия токена (т.е. сессии) ограничен и составляет 23 часа.
ЗПИ.2	Управление доступом пользователей и приложений	+	+	+	Реализуется за счет применения шлюзов API (API Gateway), серверов централизованной аутентификации (IdP), межсетевых экранов нового поколения (NGFW) и межсетевых экранов уровня веб-приложений (WAF). В части защиты ALD Pro - защита при обращении к API частично реализуется собственными средствами.	Для получения доступа к ресурсам ALD Pro через API необходимо пройти идентификацию и аутентификацию (выполняется в соответствии с мерами ИАФ.1 - ИАФ.3). Выполнить ее можно следующими способами: 1. Используя kerberos аутентификацию 2. Передать логин/пароль на /api/ds/login При первом HTTP-запросе передаются логин и пароль. В ответ ALD Pro возвращает в заголовках Set-cookie параметры авторизации, которые при последующих HTTP-запросах можно будет использовать вместо передачи логина и пароля. Срок действия токена (т.е. сессии) ограничен и составляет 23 часа. Управление доступом к ресурсам ALD Pro по API реализуется в соответствии с меами УПД.1 - УПД.4 Веб-приложение «Портал управления» ALD Pro не поддерживает предупреждение

Меры защиты и обеспечения безопасности		Классы защищенности ИС			Описание	Реализация
Код	Наименование меры	3	2	1		
						пользователя при доступе в систему (УПД.5), оповещение пользователя о предыдущем входе на портал управления (УПД.6), ограничение параллельных сессий при работе на портале управления (УПД.7) и завершение сеанса доступа к порталу управления при неактивности (УПД.8).
ЗПИ.3	Проверка на соответствие спецификации API	+	+	+ 1	Реализуется межсетевыми экранами	–
IX Защита конечных устройств (ЗКУ)						
ЗКУ.1	Управление доступом к конечным устройствам	+	+	+	Реализуется средствами ALD Pro и средствами клиента домена - ALSE	Идентификация и аутентификация пользователей конечных устройств (клиентов домена) осуществляется в соответствии с мерами ИАФ.1, ИАФ.3; Управление доступом пользователей к конечным устройствам осуществляется в соответствии с мерами защиты информации из блока УПД.1 - УПД.4
ЗКУ.2	Обеспечение целостности программного обеспечения конечного устройства	+	+ 1, 2	+ 1, 2	Реализуется средой функционирования ALSE и групповыми политиками ALD Pro	Групповые политики для централизованной настройки контроля целостности на клиентах домена: **Групповые политики → Групповые политики → <имя_групповой_политики> → Параметры компьютеров → Безопасность → Проверка целостности системы** **Групповые политики → Групповые политики → <имя_групповой_политики> → Параметры компьютеров → Безопасность → Мандатный контроль целостности** **Групповые политики → Групповые политики → <имя групповой политики> → Параметры компьютеров → Безопасность → Политика безопасности → Замкнутая программная среда**

Меры защиты и обеспечения безопасности		Классы защищенности ИС			Описание	Реализация
Код	Наименование меры	3	2	1		
ЗКУ.3	Антивирусная защита и обнаружение и предотвращение вторжений на конечных устройствах	+	+ 1	+ 1	Реализуется средствами антивирусной защиты	–
ЗКУ.4	Мониторинг процессов и состояния устройства	+	+	+	Реализуется средой функционирования ALSE и средствами ALD Pro. ALD Pro реализует групповые политики для централизованной настройки регистрации событий.	Клиент домена реализует функционал журналирования в соответствии с мерами блока РСБ. ALD Pro позволяет централизованно развернуть в домене сервер журнала событий, а также настроить сбор журналов событий: **Журнал событий → Серверы журнала событий, Настройка сбора журналов событий** Групповые политики для централизованной настройки регистрации событий: **Групповые политики → Групповые политики → <имя_групповой_политики> → Параметры компьютеров → Политики мер защиты ФСТЭК Росии → Настройка регистрации событий**
ЗКУ.5	Контроль и фильтрация трафика на конечном устройстве				Реализуется межсетевыми экранами	–
ЗКУ.6	Анализ и реагирование на события безопасности	+	+ 1	+ 1	Реализуется средой функционирования ALSE и средствами ALD Pro	Клиент домена реализует функционал журналирования в соответствии с мерами блока РСБ. ALD Pro позволяет централизованно развернуть в домене сервер журнала событий, а также настроить сбор журналов событий: **Журнал событий → Серверы журнала событий, Настройка сбора журналов событий**
X Защита мобильных устройств (ЗМУ)						
ЗМУ.1	Идентификация и аутентификация пользователей	+	+ 1	+ 1	Реализуется средствами ALD Pro и клиента домена ALSE	Идентификация и аутентификация пользователей конечных устройств осуществляется в соответствии с мерами ИАФ.1 - ИАФ.4;

Меры защиты и обеспечения безопасности		Классы защищенности ИС			Описание	Реализация
Код	Наименование меры	3	2	1		
ЗМУ.2	Управление доступом пользователей к мобильным устройствам	+	+	+	Реализуется средствами ALD Pro и клиента домена ALSE	Управление доступом пользователей к мобильным устройствам обеспечивается в соответствии с мерами защиты информации УПД.1 – УПД.9.
ЗМУ.3	Обеспечение целостности	+	+ 1	+ 1, 2	Реализуется средой функционирования ALSE ALD Pro реализует групповую политику для централизованной настройки контроля целостности на клиентах домена	Групповые политики для централизованной настройки контроля целостности на клиентах домена: **Групповые политики → Групповые политики → <имя_групповой_политики> → Параметры компьютеров → Безопасность → Проверка целостности системы** **Групповые политики → Групповые политики → <имя_групповой_политики> → Параметры компьютеров → Безопасность → Мандатный контроль целостности** **Групповые политики → Групповые политики → <имя групповой политики> → Параметры компьютеров → Безопасность → Политика безопасности → Замкнутая программная среда**
ЗМУ.4	Защита данных	+	+	+ 1	Реализуется прикладным ПО	
ЗМУ.5	Антивирусная защита	+	+	+	Реализуется средствами антивирусной защиты	
ЗМУ.6	Контроль приложений	+	+	+	Реализуется средой функционирования ALSE ALD Pro реализует групповые политики для централизованной настройки ограничения приложений. ALD Pro позволяет централизованно развернуть - сервер репозиториев ПО, который будет содержать разрешенные к установке пакеты.	Реализуется средой функционирования ALSE (механизмы ЗПС и МКЦ) в соответствии с https://wiki.astralinux.ru/pages/viewpage.action?pageId=471538657 Групповые политики ALD Pro для централизованной настройки ограничения приложений: **Групповые политики → <имя групповой политики> → Параметры компьютеров → Мандатный контроль целостности** **Групповые политики → <имя групповой политики> → Параметры компьютеров → Политика безопасности → Замкнутая программная среда**

Меры защиты и обеспечения безопасности		Классы защищенности ИС			Описание	Реализация
Код	Наименование меры	3	2	1		
						Централизованное развертывание сервера репозиториев ПО: **Установка и обновление ПО → Репозитории ПО → Серверы репозиториев ПО → Развернуть сервер репозиториев ПО**
ЗМУ.7	Ограничение и контроль функциональности	+	+	+	Реализуется средой функционирования ALSE ALD Pro реализует групповую политику для ограничения функциональности клиента домена ALSE	Реализуется средой функционирования ALSE (исключение возможности применения технологий беспроводного доступа) в соответствии с https://wiki.astralinux.ru/pages/viewpage.action?pageId=471538657 Групповая политика для отключения функции Bluetooth на клиенте домена: **Групповые политики → <имя групповой политики> → Параметры компьютеров → Политика мер защиты ФСТЭК России → Прочие аспекты безопасности → Ограничение доступа к Bluetooth**
ЗМУ.8	Определение и контроль геопозиции				Реализуется средой функционирования ALSE. Возможна централизованная настройка при разработке дополнительной групповой политики.	Реализуется средой функционирования ALSE (применения встроенных в мобильные устройства приемников сигналов глобальных навигационных спутниковых систем) в соответствии с https://wiki.astralinux.ru/pages/viewpage.action?pageId=471538657
ЗМУ.9	Регистрация, анализ и реагирование на события безопасности	+	+ 1	+ 1	Реализуется организационными мероприятиями, SIEM-системой, клиентом домена ALSE и групповыми политиками ALD Pro для централизованной настройки регистрации событий на клиентах домена и централизованного разворачивания сервера регистрации событий и сервера мониторинга.	Описание реализации средствами клиента домена и ALD Pro приведено в блоке РСБ.

Меры защиты и обеспечения безопасности		Классы защищенности ИС			Описание	Реализация
Код	Наименование меры	3	2	1		
XI Защита технологий «интернета вещей» (ЗИВ)						
ЗИВ.1	Идентификация и аутентификация	+	+	+	Реализуется за счет применения специализированных шлюзов и платформ управления устройствами «интернета вещей».	–
ЗИВ.2	Управление доступом	+	+	+	Реализуется за счет применения специализированных платформ управления «интернета вещей» и межсетевых экранов.	–
ЗИВ.3	Защита данных	+	+ 1	+ 1	Реализуется за счет применения систем инвентаризации и управления «интернета вещей» и межсетевых экранов.	–
ЗИВ.4	Контроль целостности	+	+	+	Реализуется за счет применения централизованных платформ управления «интернета вещей», а также сканеров уязвимостей.	–
ЗИВ.5	Регистрация, анализ и реагирование на события безопасности	+	+ 1	+ 1	Реализуется за счет применения централизованных платформ управления «интернета вещей» и SIEM-систем.	–
XII Защита точек беспроводного доступа (ЗБД)						
ЗБД.1	Идентификация и аутентификация	+	+	+ 1	Реализуется за счет применения средств идентификации и аутентификации, реализованных и (или) применяемых в точках беспроводного доступа, ином оборудовании беспроводной локальной вычислительной сети, устройствах пользователей.	–

Меры защиты и обеспечения безопасности		Классы защищенности ИС			Описание	Реализация
Код	Наименование меры	3	2	1		
ЗБД.2	Управление доступом	+	+	+	Реализуется за счет применения встроенных в точки беспроводного доступа и контроллеры беспроводной сети средств управления доступом.	–
ЗБД.3	Защита пользовательских данных	+	+	+	Реализуется за счет применения межсетевых экранов и систем централизованного управления точками доступа для, а также сканеров уязвимостей.	–
ЗБД.4	Контроль целостности	+	+	+	Реализуется за счет применения систем централизованного управления точками беспроводного доступа, организационно-технических мер по размещению точек доступа в пределах контролируемой зоны, а также сканеров уязвимостей.	–
ЗБД.5	Ограничение уровней сигналов	+	+	+	Реализуется за счет применения организационно-технических мер.	–
ЗБД.6	Регистрация, анализ и реагирование на события безопасности	+	+ 1	+ 1	Реализуется за счет применения централизованных систем сбора и анализа логов точек беспроводного доступа и контроллеров беспроводной сети, интегрированных с системами мониторинга событий информационной безопасности.	–
XIII Антивирусная защита (АВЗ)						
АВЗ.1	Антивирусная защита устройств	+	+	+	Реализуется за счет применения средств антивирусной защиты.	–
АВЗ.2	Антивирусная защита электронной почты	+	+	+	Реализуется за счет применения средств антивирусной защиты. электронной почты.	–

Меры защиты и обеспечения безопасности		Классы защищенности ИС			Описание	Реализация
Код	Наименование меры	3	2	1		
АВ3.3	Антивирусная проверка сетевого трафика	+	+	+	Реализуется за счет применения средств антивирусной защиты и (или) многофункциональных межсетевых экранов уровня сети, и (или) иных средств защиты информации.	–
АВ3.4	Применение замкнутой системы (среды) предварительного выполнения программ («песочницы»)				Реализуется за счет применения средств антивирусной защиты и (или) иных средств защиты информации.	–
XIV Обнаружение и предотвращение вторжений на сетевом уровне (СОВ)						
СОВ.1	Обнаружение и предотвращение вторжений на периметре	+	+ 1	+ 1	Реализуется за счет применения систем обнаружения вторжений уровня сети, и (или) многофункциональных межсетевых экранов уровня сети, и (или) иных средств защиты информации.	–
СОВ.2	Обнаружение и предотвращение вторжений в сегментах информационной системы	+	+	+	Реализуются за счет применения систем обнаружения вторжений уровня сети, и (или) многофункциональных межсетевых экранов уровня сети, и (или) иных средств защиты информации.	–
XV Сегментация и межсетевое экранирование (МСЭ)						
МСЭ.1	Сегментация сети	+	+	+ 1	Реализуется за счет применения межсетевых экранов, и (или) многофункциональных межсетевых экранов уровня сети, и (или) средств однонаправленной передачи информации, а также (при необходимости) за счет физической изоляции отдельных сегментов информационной системы, определяемых оператором.	–

Меры защиты и обеспечения безопасности		Классы защищенности ИС			Описание	Реализация
Код	Наименование меры	3	2	1		
МСЭ.2	Организация демилитаризованной зоны	+	+	+	Реализуется за счет применения межсетевых экранов, и (или) многофункциональных межсетевых экранов уровня сети.	–
МСЭ.3	Контроль сетевого доступа и фильтрация трафика	+	+	+	Реализуется за счет применения в информационной системе межсетевых экранов, и (или) многофункциональных межсетевых экранов уровня сети, и (или) средств однонаправленной передачи информации, а также (при необходимости) за счет физической изоляции отдельных сегментов информационной системы, определяемых оператором.	–
МСЭ.4	Маскирование системы				Реализуется за счет применения межсетевых экранов и пограничных маршрутизаторов.	–
МСЭ.5	Создание ложных систем				Реализуется путем проведения организационно-технических мероприятий по развертыванию изолированной ложной информационной системы, имитирующей функционирование реальных сервисов, с целью обнаружения, регистрации и анализа действий нарушителей.	–

Меры защиты и обеспечения безопасности		Классы защищенности ИС			Описание	Реализация
Код	Наименование меры	3	2	1		
XVI Защита от компьютерных атак, направленных на отказ в обслуживании (ЗОО)						
ЗОО.1	Защита от компьютерных атак, направленных на отказ в обслуживании, при доступе внешних пользователей к прикладным сервисам, предоставляемым информационной системой	+	+	+	Реализуется за счет применения межсетевых экранов уровня сети, а также с использованием специализированных программно-аппаратных средств защиты от DDoS-атак, предоставляемых провайдерами хостинга, организациями связи и поставщиками услуг по контролю и блокированию вредоносного трафика.	–
ЗОО.2	Контроль и фильтрация входящего трафика	+	+	+ 1	Реализуется за счет применения межсетевых экранов уровня сети, а также с использованием специализированных программно-аппаратных средств защиты от DDoS-атак, предоставляемых провайдерами хостинга, организациями связи и поставщиками услуг по контролю и блокированию вредоносного трафика.	–
ЗОО.3	Мониторинг состояния сервисов и интерфейсов	+	+	+	Реализуется ALD Pro путем централизованного развертывания и настройки сервера мониторинга Zabbix.	Централизованное развертывание сервера мониторинга Zabbix: **Мониторинг → Журнал событий мониторинга → Серверы мониторинга → Развернуть сервер мониторинга**
ЗОО.4	Балансировка нагрузки				Реализуется за счет применения балансировщиков нагрузки, использования услуг провайдеров хостинга, а также средств виртуализации и контейнеризации, обеспечивающих возможность вертикального масштабирования вычислительных ресурсов прикладных сервисов.	–

Меры защиты и обеспечения безопасности		Классы защищенности ИС			Описание	Реализация
Код	Наименование меры	3	2	1		
ЗОО.5	Ограничение нагрузки	+	+	+	Реализуется за счет применения межсетевых экранов уровня приложений, балансировщиков нагрузки, а также с использованием систем мониторинга трафика	–
ЗОО.6	Поддержка резерва достаточной пропускной способности и расширение ресурсов при сбоях		+	+	Реализуется за счет применения сервисов фильтрации трафика, выделенных средств защиты от DDoS-атак на уровне сети, межсетевых экранов и балансировщиков нагрузки.	–
XVII Защита каналов связи и сетевого взаимодействия (ЗКС)						
ЗКС.1	Защита данных при передаче по каналам связи	+	+	+	Реализуется за счет применения межсетевых экранов, и (или) многофункциональных межсетевых экранов уровня сети, и (или) средств однонаправленной передачи информации, а также с использованием шифровальных (криптографических) средств защиты информации в соответствии с законодательством Российской Федерации.	–
ЗКС.2	Контроль атрибутов безопасности при сетевом взаимодействии	+	+	+	Реализуется за счет применения межсетевых экранов и (или) многофункциональных межсетевых экранов.	–
ЗКС.3	Контроль доступа к внешним ресурсам	+	+	+	Реализуется за счет применения межсетевых экранов и (или) многофункциональных межсетевых экранов.	–
ЗКС.4	Контекстная проверка исходящего трафика				Реализуется за счет применения систем обнаружения вторжений уровня сети, и (или) многофункциональных межсетевых экранов уровня сети, и (или) иных средств защиты информации.	–