ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

Программное обеспечение «Корпоративная система электронной почты и планирования совместной работы команд «Mailion»

Описание применения

RU.29144487.506900.001 31

На 18 листах

Москва
2023

АННОТАЦИЯ

Настоящий документ содержит сведения о применении программного обеспечения «Корпоративная система электронной почты и планирования совместной работы команд «Mailion» (далее по тексту – ПО «Mailion», изделие): условия, при которых возможна работа, входные и выходные данные, описание реализованных функций.

СОДЕРЖАНИЕ

1 НАЗНАЧЕНИЕ ПРОГРАММЫ

ПО «Mailion» является защищенным программным средством, обеспечивающим разграничение доступа к информации, не содержащей сведений, составляющих государственную тайну и представляет собой централизованную корпоративную почтовую систему на базе микросервисной архитектуры, обеспечивающую обмен электронными сообщениями, планирование рабочего времени, интеллектуальный поиск информации и работу с адресными книгами. Система отличается высокой отказоустойчивостью, способна на быстрое самовосстановление и масштабируемость в зависимости от нагрузок.

ПО «Mailion» может применяться в значимых объектах критической информационной инфраструктуры 1 категории, в государственных информационных системах 1 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных, в информационных системах общего пользования II класса.

1.1 Функции программы

ПО «Mailion» реализует следующие функции:

- получение, отправка и хранение сообщений электронной почты;
- получение, отправка и хранение календарных событий;
- работа с глобальным списком пользователей, групп, списков рассылок, ресурсов компании и локальными контактами пользователей;
- централизованное управление (создание, удаление и редактирование) субъектами ПО «Mailion» (пользователи, группы, комнаты);
- хранение и восстановление данных (метаданных объектов и сами объекты);
- поддержка криптографической защиты данных с помощью КриптоПро.

1.2 Функции безопасности

ПО «Mailion» выполняет следующие функции безопасности информации в соответствии с документами «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):

- ИАФ.1 – При доступе в ПО «Mailion» должна осуществляться идентификация и аутентификация пользователей, являющихся работниками оператора (внутренних пользователей), и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей;
- ИАФ.1 (Усиление 1а) – В информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для удаленного доступа в систему с правами привилегированных учетных записей (администраторов): с использованием сети связи общего пользования, в том числе сети Интернет;
- ИАФ.1 (Усиление 2а) – В информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для удаленного доступа в систему с правами непривилегированных учетных записей (пользователей) с использованием сети связи общего пользования, в том числе сети Интернет;
- ИАФ.1 (Усиление 3) – В информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для локального доступа в систему с правами привилегированных учетных записей (администраторов);
- ИАФ.1 (Усиление 4) – В информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для локального доступа в систему с правами непривилегированных учетных записей (пользователей);
- ИАФ.3 – Оператором должны быть установлены и реализованы следующие функции управления идентификаторами пользователей и устройств в информационной системе:
  - формирование идентификатора, который однозначно идентифицирует пользователя;

- блокирование идентификатора;
- присвоение идентификатора пользователю;
- удаление идентификатора.

– ИАФ.3 (Усиление 1б) – Оператором должно быть исключено повторное использование идентификатора пользователя в течение: не менее трех лет;
– ИАФ.3 (Усиление 2б) – оператором должно быть обеспечено блокирование идентификатора пользователя через период времени неиспользования: не более 45 дней;
– ИАФ.4 – Оператором должны быть установлены и реализованы следующие функции управления средствами аутентификации (аутентификационной информацией) пользователей и устройств в операционной системе:
- выдача средств аутентификации пользователям;
- генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации);
- блокирование (прекращение действия) и замена утерянных, скомпрометированных или поврежденных средств аутентификации;

– ИАФ.4 (Усиление 1г) – В случае использования в информационной системе механизмов аутентификации на основе пароля (иной последовательности символов, используемой для аутентификации) или применения пароля в качестве одного из факторов многофакторной аутентификации, его характеристики должны быть следующими: 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;
– ИАФ.5 – В информационной системе должна осуществляться защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий. В процессе аутентификации должна обеспечиваться исключением отображения для пользователя действительного значения аутентификационной информации и (или)

количества вводимых пользователем символов аутентификационной информации. Вводимые символы пароля могут отображаться условными знаками «*», «•» или иными знаками;

- УПД.1 – Оператором должны быть установлены и реализованы следующие функции управления учетными записями пользователей, в том числе внешних пользователей (заведение, уничтожение, блокирование, активация);
- УПД.1 (Усиление 1) – Оператором должны использоваться автоматизированные средства поддержки управления учетными записями пользователей;
- УПД.1 (Усиление 2) – В информационной системе должно осуществляться автоматическое блокирование временных учетных записей пользователей по окончании установленного периода времени для их использования;
- УПД.1 (Усиление 3б) – В информационной системе должно осуществляться автоматическое блокирование неактивных (неиспользуемых) учетных записей пользователей после периода времени неиспользования: более 45 дней;
- УПД.2 – В информационной системе для управления доступом субъектов доступа к объектам доступа должны быть реализованы установленные оператором методы управления доступом, назначены типы доступа субъектов к объектам доступа и реализованы правила разграничения доступа субъектов доступа к объектам доступа;
- УПД.2 (Усиление 1) – В информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов при входе в информационную систему;
- УПД.2 (Усиление 2) – В информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов к техническим средствам, устройствам, внешним устройствам;
- УПД.2 (Усиление 3) – В информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов к объектам, создаваемым общесистемным (общим) программным обеспечением;
- УПД.2 (Усиление 4) – В информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов к объектам, создаваемым прикладным и специальным программным обеспечением;

- УПД.4 – Оператором должно быть обеспечено разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, в соответствии с их должностными обязанностями (функциями), фиксирование в организационно-распорядительных документах по защите информации (документирование) полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, и санкционирование доступа к объектам доступа в соответствии с разделением полномочий (ролей);
- УПД.4 (Усиление 1) – Оператором должно быть обеспечено выполнение каждой роли по обработке информации, администрированию информационной системы, ее системы защиты информации, контролю (мониторингу) за обеспечением уровня защищенности информации, обеспечению функционирования информационной системы отдельным должностным лицом;
- УПД.5 – Владелец информационной системы может определить собственные регламенты по наделению учетных записей вышеописанными ролями определенных им должностных лиц. Объем разрешений администратора инсталляции ПО «Mailion» является минимально необходимым для обеспечения функционирования информационной системы, он не позволяет получить доступ к данным тенантов, администрированием которых занимается администратор конкретного тенанта;
- УПД.5 (Усиление 1) – В информационной системе обеспечивается предоставление прав и привилегий по доступу к функциям безопасности (параметрам настройки) средств защиты информации исключительно администратору, наделенному полномочиями по администрированию системы защиты информации;
- УПД.6 – В информационной системе должно быть установлено и зафиксировано в организационно-распорядительных документах оператора (задокументировано) ограничение количества неуспешных попыток входа в информационную систему (доступа к информационной системе) за период времени, установленный оператором, а также обеспечено блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в информационную систему (доступа к информационной системе). Ограничение

количества неуспешных попыток входа в информационную систему (доступа к информационной системе) должно обеспечиваться в соответствии с ИАФ.4;

- УПД.6 (Усиление 1) – В информационной системе обеспечивается автоматическое блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в информационную систему (доступа к информационной системе) за установленный период времени с возможностью разблокирования только администратором или иным лицом, имеющим соответствующие полномочия (роль);
- УПД.10 – В информационной системе должно обеспечиваться блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу;
- УПД.10 (Усиление 1б) – В информационной системе обеспечивается блокирование сеанса доступа пользователя после времени бездействия (неактивности) пользователя: до 5 минут;
- УПД.10 (Усиление 2) – В информационной системе на устройстве отображения (мониторе) после блокировки сеанса не должна отображаться информация сеанса пользователя (в том числе использование "хранителя экрана", гашение экрана или иные способы);
- УПД.11 – Оператором должен быть установлен перечень действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации, и запрет действий пользователей, не включенных в перечень разрешенных действий, до прохождения ими процедур идентификации и аутентификации;
- ОПС.2 – Оператором должны быть реализовано управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения;
- ОПС.2 (Усиление 1) – В информационной системе должно обеспечиваться использование средств автоматизации для применения и контроля параметров настройки компонентов программного обеспечения, влияющих на безопасность информации;

- РСБ.1 – В информационной системе должно обеспечиваться определение событий безопасности, подлежащих регистрации, и сроков их хранения;
- РСБ.1 (Усиление 1) – Оператором должен обеспечиваться пересмотр перечня событий безопасности, подлежащих регистрации, не менее чем один раз в год, а также по результатам контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе;
- РСБ.1 (Усиление 2) – Оператором в перечень событий безопасности, подлежащих регистрации, должны быть включены события, связанные с действиями от имени привилегированных учетных записей (администраторов);
- РСБ.1 (Усиление 3) – Оператором в перечень событий безопасности, подлежащих регистрации, должны быть включены события, связанные с изменением привилегий учетных записей;
- РСБ.1 (Усиление 4б) – Оператором должен быть обеспечен срок хранения информации о зарегистрированных событиях безопасности не менее трех месяцев, если иное не установлено требованиями законодательства Российской Федерации, при этом: осуществляется хранение записей о выявленных событиях безопасности и записей системных журналов, которые послужили основанием для регистрации события безопасности;
- РСБ.1 (Усиление 4в) – Осуществляется хранение журналов приложений, которые послужили основанием для регистрации события безопасности;
- РСБ.2 – В Изделии должно быть реализовано определение состава и содержания информации о событиях безопасности, подлежащих регистрации;
- РСБ.2 (Усиление 1а) – В информационной системе обеспечивается запись дополнительной информации о событиях безопасности, включающую: полнотекстовую запись привилегированных команд (команд, управляющих системными функциями);
- РСБ.3 – В информационной системе должны осуществляться сбор, запись и хранение информации о событиях безопасности в соответствии с РСБ.1, с составом и содержанием информации, определенными в соответствии с РСБ.2, в течение установленного оператором времени хранения информации о событиях безопасности;

- РСБ.3 (Усиление 1) – В информационной системе должно быть обеспечено централизованное автоматизированное управление сбором, записью и хранением информации о событиях безопасности;
- РСБ.6 – В информационной системе должно обеспечиваться генерирование временных меток и (или) синхронизация системного времени в информационной системе;
- РСБ.6 (Усиление 1) – Оператором информационной системы должен быть определен источник надежных меток времени; в информационной системе должна выполняться синхронизация системного времени с периодичностью, определенной оператором;
- РСБ.7 – В информационной системе должна обеспечиваться защита информации о событиях безопасности;
- РСБ.7 (Усиление 1) – В информационной системе обеспечивается резервное копирование записей регистрации (аудита);
- РСБ.8 – Сведения о действиях отдельных пользователей в информационной системе должны предоставляться уполномоченным должностным лицам для просмотра и анализа с целью расследования причин возникновения инцидентов в информационной системе в соответствии с законодательством Российской Федерации с использованием средств информационной системы (Журнала аудита);
- АНЗ.5 – Оператором должен проводиться контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе;
- АНЗ.5 (Усиление 1) – В информационной системе должна обеспечиваться регистрация событий, связанных со сменой паролей пользователей, заведением и удалением учетных записей пользователей, изменением правил разграничения доступом и полномочий пользователей;
- ОЦЛ.3 – Оператором должна быть предусмотрена возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций;
- ОЦЛ.3 (Усиление 1) – Оператором обеспечивается восстановление отдельных функциональных возможностей информационной системы с применением

резервированного программного обеспечения зеркальной информационной системы (сегмента информационной системы, технического средства, устройства);

- ОЦЛ.4 – Оператором должно обеспечиваться обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама);
- ОЦЛ.7 – В информационной системе должен осуществляться контроль точности, полноты и правильности данных, вводимых в информационную систему путем установления и проверки соблюдения форматов ввода данных, синтаксических, семантических и (или) иных правил ввода информации в информационную систему (допустимые наборы символов, размерность, область числовых значений, допустимые значения, количество символов) для подтверждения того, что ввод информации соответствует заданному оператором формату и содержанию;
- ОЦЛ.8 – В информационной системе должен обеспечиваться контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях;
- ОДТ.3 – Оператором должен осуществляться контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование;
- ОДТ.3 (Усиление 1) – В информационной системе должна быть обеспечена сигнализация (уведомление) о неисправностях, сбоях и отказах в функционировании программно-технических средств информационной системы;
- ОДТ.4 – Оператором должно обеспечиваться периодическое резервное копирование персональных данных на резервные машинные носители персональных данных;
- ОДТ.4 (Усиление 1) – Оператором должна осуществляться с установленной им периодичностью проверка работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий (периодичность проверки работоспособности определяется оператором);

- ОДТ.4 (Усиление 3) – оператором должно осуществляться резервное копирование информации на зеркальную информационную систему (сегмент информационной системы, техническое средство, устройство);
- ОДТ.5 – Оператором должна быть обеспечена возможность восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала;
- ОДТ.5 (Усиление 1) – Оператором должна обеспечиваться возможность восстановления информации с учетом нагруженного ("горячего") резервирования технических средств;
- ЗИС.7 – В информационной системе должны обеспечиваться контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологии мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологии мобильного кода;
- ЗИС.7 (Усиление 1) – В информационной системе должны быть реализованы механизмы обнаружения и анализа мобильного кода для выявления фактов несанкционированного использования мобильного кода и выполнения действий по реагированию (оповещение администраторов, изоляция мобильного кода (перемещение в карантин), блокирование мобильного кода, удаление мобильного кода) и иные действия, определяемые оператором;
- ЗИС.7 (Усиление 2) – В информационной системе должен осуществляться запрет загрузки и выполнения запрещенного мобильного кода;
- ЗИС.10 – В информационной системе должно обеспечиваться подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам;
- ЗИС.11 – В информационной системе должно обеспечиваться признание идентификатора сеанса связи недействительным после окончания сетевого соединения;
- ЗИС.11 (Усиление 1) – В информационной системе должно обеспечиваться признание идентификатора сеанса связи недействительным после окончания сетевого соединения.

2 УСЛОВИЯ ПРИМЕНЕНИЯ

ПО «Mailion» функционирует в среде операционной системы Astra Linux Special Edition 1.7.

Штатная работа серверных компонентов изделия должна быть обеспечена на оборудовании, удовлетворяющем требованиям, приведенным в таблице 1 и таблице 2.

Таблица 1 – Минимальные требования к оборудованию для работы серверных компонентов

Имя группы сервера	**VCPU**	**RAM, Gb**	**HDD, Gb (без учёта ОС)**	**SSD, Gb**	**Количество виртуальных машин**	**VCPU**	**RAM, Gb**	**HDD, Gb**	**SSD, Gb**
	на каждую роль					**итого на группу**			
ucs_frontend	6	6	10	10	2	12	12	20	20
ucs_mail									
ucs_apps	8	8	10		2	16	16	20	
ucs_catalog									
ucs_calendar									
ucs_balancers									
ucs_converter									
ucs_search	16	18	10	15	3	48	54	30	45
ucs_etcd									
ucs_arangodb_agency									
ucs_mongodb									
ucs_arangodb									
ucs_redis_cache									
ucs_mq									
ucs_redis_data									
dispersed_object_store	3	3	20	4	4	12	12	80	16
ucs_infrastructure	4	8	100		1	4	8	100	
				ИТОГО:	12	92	102	250	81

Таблица 2 – Рекомендуемые требования к оборудованию для работы серверных компонентов

Имя роли сервера	**VCPU**	**RAM, Gb**	**HDD, Gb (без учёта ОС)**	**SSD, Gb**	**Количество виртуальных машин**	**VCPU**	**RAM, Gb**	**HDD, Gb**	**SSD, Gb**
	на каждую роль					**итого на группу**			
ucs_frontend	4	4	10		2	8	8	20	
ucs_mail	4	4		10	4	16	16		40
ucs_catalog	8	8	10		2	16	16	20	
ucs_apps	8	8	10		2	16	16	20	
ucs_calendar									
ucs_balancers									
ucs_search	4	8		30	3	12	24		90
ucs_converter	4	8		30	3				
ucs_etcd	8	16		30	3	24	48		90
ucs_arangodb_agency									
ucs_mongodb									
ucs_arangodb									
ucs_mq									
dispersed_object_store	4	4	60	10	4	16	16	240	40
ucs_redis_data	8	8		10	3	24	24		30
ucs_redis_cache									
ucs_infrastructure	4	8	200		1	4	8	200	
				ИТОГО:	26	144	184	510	290

3 ОПИСАНИЕ ЗАДАЧИ

Общая логическая схема «Mailion» приведена на рисунке 1.

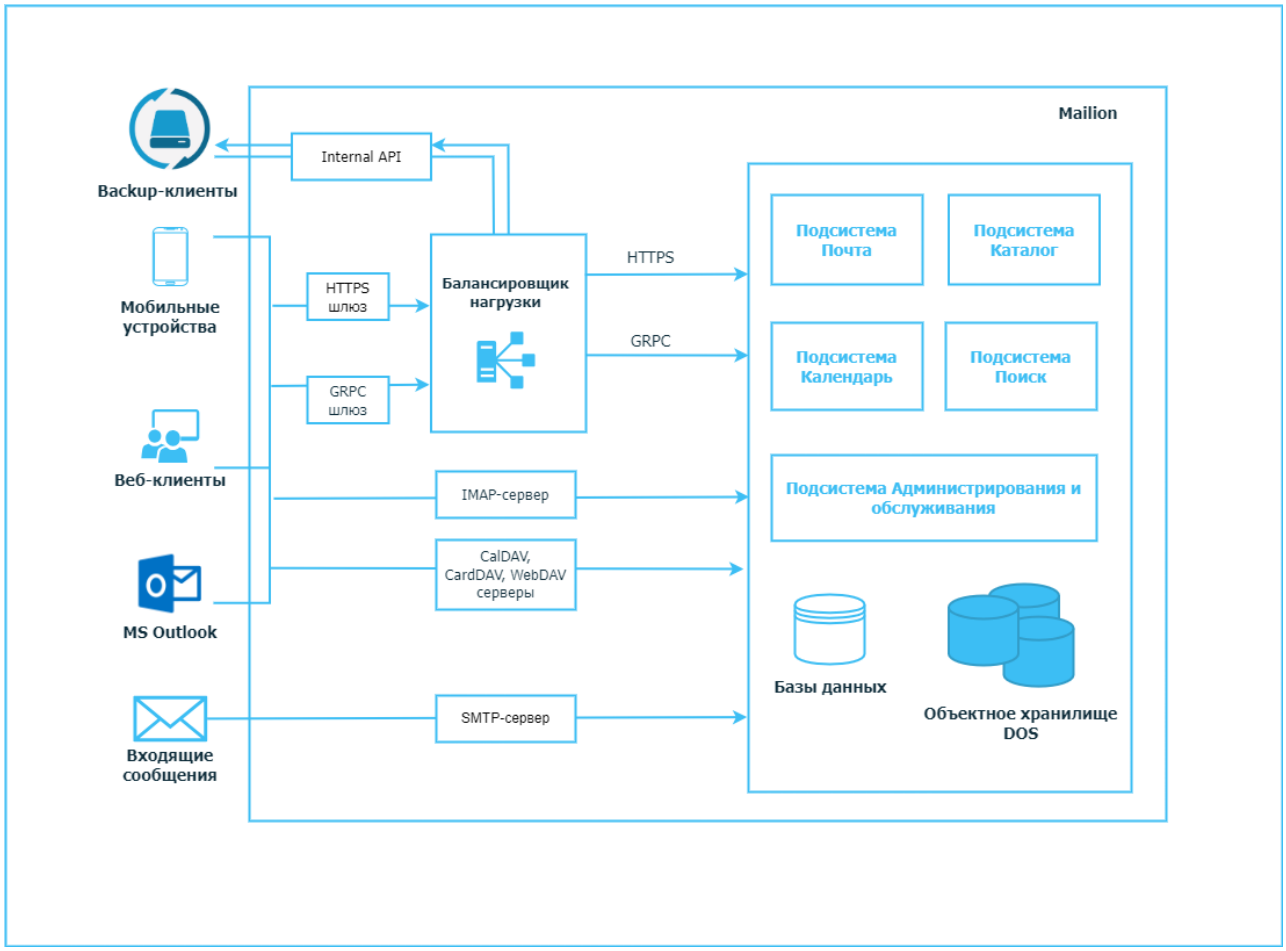

Рисунок 1 – Общая логическая схема «Mailion»

После ввода учетных данных в сервис протокола, они передаются в подсистему «Каталог», которая, обращаясь к подсистеме «Базы данных», сначала проверяет существование учетной записи с указанным логином, её статус, далее проверяет пароль на соответствие хранимому хешу по алгоритму Argon2ID, если все шаги успешны, то происходит создание идентификатора сессии и запись его в базу. Далее этот идентификатор сессии возвращается в вызывающую подсистему, которая использует его для дальнейшей работы.

Все последующие запросы снабжаются этим идентификатором, проверка которого происходит с помощью обращения к подсистеме «Каталог», которая, в свою очередь, обращается в подсистему «Базы данных» для проверки наличия и срока действия идентификатора.

Запросы Администратора тенанта для управления могут быть следующими: создание пользователя, создание e-mail, создание логина, создание пароля, создание профиля, удаление логина, удаление e-mail, изменение статуса пользователя, добавить пользователя в группу, удалить пользователя из группы. Подсистема «Платформа» этот запрос передаёт далее в подсистему «Каталог», который для выполнения соответствующего действия обращается в подсистему «Базы данных».

Каждый запрос пользователя, проходящий в любой сервис, доступный по публичному адресу, проверяет настройки политики хранения информации о событиях безопасности. Это сервисы протоколов HTTP, GRPC, IMAP, SMTP, Card/CalDAV, LDAP. Для проверки настроек политики сервис обращается в подсистему «Каталог», которая с помощью подсистемы «Баз данных» получает настройки, относящиеся к пользователю и тенанту. Если политика настроена на сохранение этого запроса от этого пользователя, то через подсистему «Каталог» информация о совершении указанного запроса происходит запись в лог событий безопасности в подсистеме «Базы данных».

Вся информация об интерфейсах подсистем описана в документе «Программное обеспечение «Mailion». Функциональная спецификация» RU.29144487.506900.001 ФС.

4 ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

4.1 Входные данные ПО «Mailion»

Входными данными ПО «Mailion» являются:

- данные по протоколу IMAP;
- HTTP-передача логина и пароля от учетной записи, а также одноразовый пароль второго фактора;
- LDAP логин и пароль в Bind-запросе;
- SMTP логин и пароль в команде AUTH;
- CardDAV/CalDAV-запросы;
- HTTP-запросы Администратора;
- запросы Администратора через консольную утилиту по протоколу GRPC.

4.2 Выходные данные ПО «Mailion»

Выходными данными ПО «Mailion» являются:

- данные по протоколу SMTP в формате MIME текстовых сообщений с кодировкой UTF-8;
- данные по протоколу IMAP в формате MIME текстовых сообщений с кодировкой UTF-8, Windows-1251, KOI8-R.