Разделение ответственности при использовании программного обеспечения «Облачная платформа Cloud.ru Evolution Public» в контексте выполнения требований ГОСТ Р 57580.1-2017

Москва 2026

Содержание

Перечень сокращений и терминов 4
Предупреждение об исключительных правах и конфиденциальной информации 5
Введение 6
1 Функциональные характеристики ПО Evolution 7
1.1 Портал самообслуживания 7
1.2 Зона доступности 9
1.3 Функциональность, предоставляемая ПО Evolution 10
2 Последовательность действий Клиента для достижения соответствия требованиям ГОСТ Р 57580 12
3 Разделение ответственности 13
3.1 Выполнение требований ПО Evolution 13
3.2 Выполнение требований Клиентом 14
3.3 Общее разделение ответственности 14
4 Разделение ответственности при выполнении требований к системе защиты информации 16
4.1 Процесс 1 «Обеспечение защиты информации при управлении доступом» (меры групп УЗП, РД, ФД и ИУ) 16
4.1.1 Подпроцесс «Управление учетными записями и правами субъектов логического доступа» (УЗП.1 – УЗП.29) 16
4.1.2 Подпроцесс «Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа» (РД.1 – РД.44) 17
4.1.3 Подпроцесс «Защита информации при осуществлении физического доступа» (ФД.1 – ФД.21) 19
4.1.4 Подпроцесс «Идентификация и учет ресурсов и объектов доступа» (ИУ.1 – ИУ.8) 19
4.2 Процесс 2 «Обеспечение защиты вычислительных сетей» (меры групп СМЭ, ВСА, ЗВС и ЗБС) 19
4.2.1 Подпроцесс «Сегментация и межсетевое экранирование вычислительных сетей» (СМЭ.1 – СМЭ.21) 19
4.2.2 Подпроцесс «Выявление вторжений и сетевых атак» (ВСА.1 – ВСА.14) 20
4.2.3 Подпроцесс «Защита информации, передаваемой по вычислительным сетям» (ЗВС.1, ЗВС.2) 20
4.2.4 Подпроцесс «Защита беспроводных сетей» (ЗБС.1 – ЗБС.10) 20
4.3 Процесс 3 «Контроль целостности и защищенности информационной инфраструктуры» (меры группы ЦЗИ) 20
4.4 Процесс 4 «Защита от вредоносного кода» (мера группы ЗВК) 20
4.5 Процесс 5 «Предотвращение утечек информации» (мера группы ПУИ) 20
4.6 Процесс 6 «Управление инцидентами защиты информации» (меры групп МАС и РИ) 20
4.6.1 Подпроцесс «Мониторинг и анализ событий защиты информации» (МАС.1 – МАС.23) 21
4.6.2 Подпроцесс «Обнаружение инцидентов защиты информации и реагирование на них» (РИ.1 – 19) 21
4.7 Процесс 7 «Защита среды виртуализации» (меры группы ЗСВ) 21
4.8 Процесс 8 «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств» (меры группы ЗУД) 23

5 Разделение ответственности при выполнении требований к организации и управлению защитой информации 24
5.1 Направление 1 «Планирование процесса системы защиты информации» (мера группы ПЗИ) 24
5.2 Направление 2 «Реализация процесса системы защиты информации» (мера группы РЗИ) ...24
5.3 Направление 3 «Контроль процесса системы защиты информации» (мера группы КЗИ).....24
5.4 Направление 4 «Совершенствование процесса системы защиты информации» (мера группы СЗИ) 24
6 Разделение ответственности при выполнении требований к защите информации на этапах жизненного цикла автоматизированных систем и приложений 25
6.1 Этап «Создание (модернизация) автоматизированной системы» (ЖЦ.1 – ЖЦ.11) 25
6.2 Этап «Ввод в эксплуатацию автоматизированной системы» (ЖЦ.12 – ЖЦ.14) 25
6.3 Этап «Эксплуатация (сопровождение) автоматизированной системы» (ЖЦ.15 – ЖЦ.25) 25
6.4 Этап «Эксплуатация (сопровождение) и снятие с эксплуатации автоматизированной системы» (ЖЦ.26 – ЖЦ.28).....25

Перечень сокращений и терминов

АС – Автоматизированная система

АРМ – Автоматизированное рабочее место

ПО – Программное обеспечение

ЦОД – Центр обработки данных

API – от англ. Application Programming Interface – интерфейс программирования приложения

IaaS – от англ. Infrastructure as a Service – инфраструктура как услуга

PaaS – от англ. Platform as a Service – платформа как услуга

RAG – от англ. Retrieval Augmented Generation генерация с дополненной выборкой

API – это набор правил и протоколов, который позволяет разным программным приложениям обмениваться данными и взаимодействовать друг с другом, работая как посредник или переводчик между ними без необходимости знать внутреннюю реализацию каждого сервиса.

IaaS – модель облачных вычислений, где поставщик предоставляет клиентам доступ к базовым IT-ресурсам (виртуальным серверам, хранилищам, сетям) через интернет по подписке, оплачиваемой по факту использования, что позволяет компаниям арендовать и масштабировать IT-инфраструктуру без покупки физического оборудования, сохраняя при этом контроль над операционными системами и приложениями.

PaaS – модель облачных вычислений, предоставляющая разработчикам готовую среду для создания, тестирования, развертывания и управления приложениями, включая операционные системы, базы данных, серверы и инструменты, при этом провайдер управляет всей базовой инфраструктурой, позволяя разработчикам сосредоточиться на коде. Это избавляет от забот о покупке, настройке и поддержке оборудования, снижая затраты и ускоряя разработку.

Virtual Private Cloud – сервис сетевой изоляции виртуальных частных облаков ("доменов" внутри пользовательской инфраструктуры.

RAG – соединяет языковую модель с внешней базой знаний. AI-помощник на базе RAG сначала находит релевантные документы во внешних источниках с помощью, например, векторного поиска, ранжирует найденную информацию, а затем генерирует ответ на запрос пользователя на основе этих данных.

Representational State Transfer Application Programming Interface (REST API) – архитектурный стиль для создания веб-сервисов, который использует стандартные методы HTTP (GET, POST, PUT, DELETE) для взаимодействия между клиентскими приложениями (сайтами, мобильными приложениями) и сервером, обеспечивая эффективный и стандартизированный обмен данными и ресурсами через интернет, обычно в формате JSON или XML.

Software-Defined Storage (SDS) – программно-определяемое хранилище, где управление ресурсами абстрагировано от базового физического оборудования.

Предупреждение об исключительных правах и конфиденциальной информации

Исключительные права на все результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий, которым предоставляется правовая охрана (интеллектуальная собственность), используемые при разработке, поддержке и эксплуатации программного обеспечения «Облачная платформа Cloud.ru Evolution Public» (далее – ПО Evolution), включая, но не ограничиваясь, программы для электронной вычислительной машины, базы данных, изображения, тексты, другие произведения, а также изобретения, полезные модели, товарные знаки, знаки обслуживания, коммерческие обозначения и фирменные наименования, принадлежат ООО «Облачные технологии».

Использование результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации в целях, не связанных с разработкой, поддержкой и эксплуатацией ПО Evolution, не допускается без получения предварительного согласия правообладателя.

Отношения ООО «Облачные технологии» с лицами, привлекаемыми для разработки, поддержки и эксплуатации ПО Evolution, регулируются законодательством Российской Федерации и заключаемыми в соответствии с ним трудовыми и/или гражданско-правовыми договорами (соглашениями). Нарушение требований об охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации, а равно как и конфиденциальной информации, влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Контактная информация ООО «Облачные технологии»

Техническая поддержка:

Тел. 8-800-444-24-99

E-mail: support@cloud.ru

Офис:

Тел. 8 495 260-10-82

Адрес: 117312, Москва, ул. Вавилова, д. 23, стр. 1 комната № 1.207

Введение

ПО Evolution является собственной разработкой ООО «Облачные технологии» и представляет собой платформу виртуализации, состоящую из множества компонент и подсистем, позволяющую использовать набор сервисов по моделям Infrastructure as a Service (далее – IaaS) и Platform as a Service (далее – PaaS) в целях выполнения задач коммерческого публичного и частного облака.

Для создания и управления облачными ресурсами пользователь использует Личный кабинет как единую точку доступа к сервисам, контролю затрат, управлению доступами и поддержке.

Настоящий документ рекомендуется использовать, если инфраструктура клиента ООО «Облачные технологии» (далее – Клиент), которая реализуется на базе компонентов ПО Evolution, попадает под действие документа «ГОСТ Р 57580.1-2017. Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утв. и введен в действие Приказом Росстандарта от 08.08.2017 № 822-ст (далее – ГОСТ Р 57580).

Документ описывает разделение ответственности за выполнение требований ГОСТ Р 57580. Часть требований выполняет ПО Evolution, часть должна выполняться самостоятельно Клиента, а часть является обоюдной ответственностью сторон.

ПО Evolution имеет заключение об оценке соответствии требованиям ГОСТ Р 57580 по усиленному уровню защиты информации. На момент окончания аудита итоговая оценка составила R=0,88 (четвертый уровень соответствия).

1 Функциональные характеристики ПО Evolution

Укрупненно, ПО Evolution можно представить в виде функциональных блоков (Рисунок 1). Каждый блок отвечает за определенную функцию(ии).

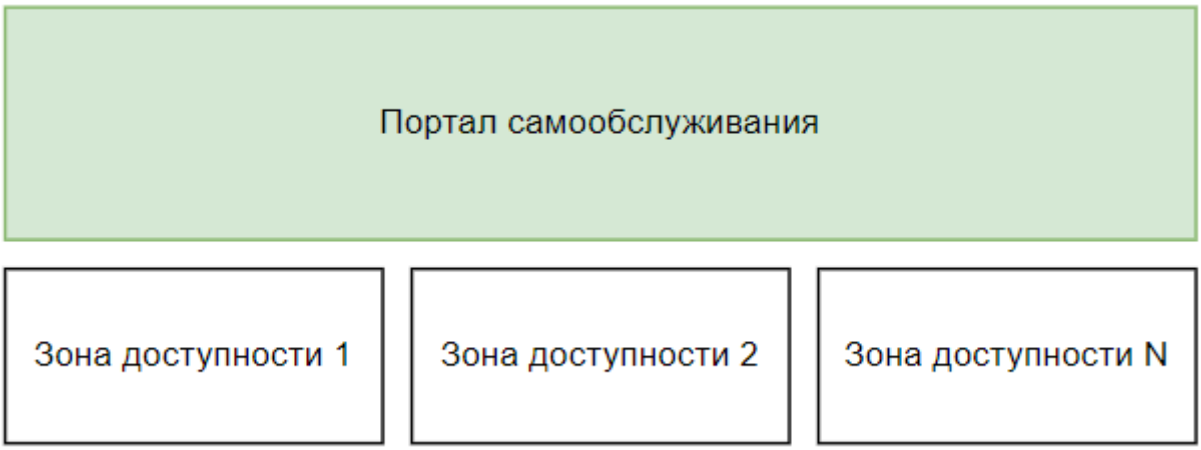

Рисунок 1 – Укрупненная схема ПО Evolution

1.1 Портал самообслуживания

Портал самообслуживания состоит из подсистем, которые выполняют различные функции. Таблица 1 содержит наименование подсистем и их функции.

Таблица 1 – Функции подсистем

Наименование	Функция
Cloud-Platform	Функциональное ядро Личного кабинета и Административной консоли. Позволяет управлять инфраструктурой, ресурсами, предоставлять услуги внутренним подразделениям компании
IAM	Сервис управления пользователями, группами пользователей, ролями и политиками, с помощью которых администратор контролирует доступ к облачным ресурсам
MONaaS	Сервис, позволяющий собирать и хранить метрики ресурсов облачной инфраструктуры. С помощью мониторинга можно отслеживать ключевые показатели производительности и поддерживать стабильную работу приложений
Notifications	Сервис уведомлений и оповещений
Audit (AUDaaS)	Сервис, производящий запись о событиях в системе, инициаторах и времени этих событий. Как следствие позволяет проверять работу системы на соответствие стандартам безопасности, требованиям законодательства и корпоративным политикам
LogaaS	Сервис для сбора событий с других платформенных сервисов личного кабинета, не поддерживающих интеграцию через шину данных Ebus
Ebus	Шина данных для получения, агрегации, корреляции и фильтра событий

evolution-iaas-vpc	Backend-for-Frontend сервис для представления информации по Virtual Private Cloud в личном кабинете пользователей
api-gw	Высокопроизводительный, доступный и безопасный сервис размещения Application Programming Interface (далее – API), который помогает создавать, разворачивать программные интерфейсы приложения в любом масштабе и управлять ими
Evolution Artifact Registry	Сервис для версионирования, хранения и распространения Docker-образов
Автоматизированная система расчетов «Модуль тарификации Cloud.ru», версия ПО 1.0	Сервис для учета и контроля затрат
evolution-s3-sc	Отказоустойчивый (распределенный) сервис хранения объектов (файлов) на базе Software-Defined Storage (далее – SDS), в т.ч. для использования резервного копирования
Evolution Managed Kubernetes (MK8S)	Сервис управления кластерами Kubernetes. Позволяет автоматически развертывать контейнеризированные приложения и создавать кластеры Kubernetes
Evolution IaaS Service Controller	Набор приложений, предоставляющий API для управления платформой Evolution IaaS
DBaaS	Сервис управления базами данных
Evolution Compute	Сервис для управление виртуальными машинами в облачной инфраструктуре. Виртуальная машина эмулирует поведение реального компьютера и позволяет запускать приложения в различных окружениях
Evolution Managed PostgreSQL	Сервис для создания кластеров реляционной СУБД PostgreSQL® и управления ими
Evolution Pangolin	Сервис для развертывания и управления кластерами Pangolin в инфраструктуре ПО Evolution. Pangolin — специальная сборка открытой СУБД PostgreSQL с повышенной защищенностью
Evolution Magic Router	Инструмент управления сетевыми связями между ресурсами внутри облачной инфраструктуры, а также между ресурсами облачной инфраструктуры ПО Evolution и внешними сетями
Evolution Load Balancer	Сервис, позволяющий управлять сетевыми балансировщиками нагрузки в ПО Evolution
Evolution DirectConnect	Выделенный канал связи с гарантированной пропускной способностью между корпоративной сетью Клиента и ПО Evolution
Evolution Container Apps	Сервис для запуска контейнерных приложений в облаке, без знаний Kubernetes и создания виртуальных машин
Evolution Bare Metal	Сервис аренды физических серверов для систем, которым требуется доступ к аппаратной части
Evolution Managed ArenadataDB	Предназначена для хранения и обработки больших объемов структурированных и полуструктурированных данных. неограниченного роста компании

Evolution DNS	Управляемый сервис обслуживания DNS-зон, который позволяет создавать и управлять приватными или публичными доменными зонами и их ресурсными записями без необходимости развертывания собственных DNS-серверов
Evolution Foundation models	Сервис для запуска ML-моделей из платформы Hugging Face на облачных мощностях с графическим процессором, в том числе в пользовательских Docker-образах
Evolution ML Inference	Решение, позволяющее запустить ML-модель в облаке
Evolution AI Agents	Автономные программные системы на основе искусственного интеллекта
Evolution Managed RAG	Сервис для создания управляемых Retrieval Augmented Generation (RAG) систем на основе пользовательских данных
Evolution ML Finetuning	Сервис для тонкой настройки больших языковых моделей под необходимые задачи.
Evolution Notebooks	Сервис для работы и экспериментов с машинным обучением в облаке
Managed Metastore	Сервис для хранения метаданных
Managed Trino	Сервис, который предоставляет массивно-параллельный аналитический SQL-движок для обработки больших объемов данных из разных источников
Managed Redis	Сервис для создания и управления кластерами Redis® в инфраструктуре ПО Evolution

1.2 Зона доступности

Таблица 2 содержит состав зоны доступности.

Таблица 2 – Состав зоны доступности

Наименование	Назначение
Evolution OverCloud	
Compute	Управляет виртуализацией — взаимодействует с другими службами для создания экземпляров виртуальных машин. Инкапсулирует клиентские виртуальные машины для рабочей нагрузки, а также виртуальных машин для работы Managed Kubernetes
Network	Реализует работу сетей
SDS	Сервис создания логического уровня управления ресурсами хранения. Позволяет программно объединять диски в единое хранилище, которое оптимизировано для хранения больших объемов данных, обеспечивает их репликацию и высокую доступность
S3	Объектное хранилище
Evolution Undercloud	
Compute Node undercloud	Инкапсулирует ноды рабочей нагрузки Managed Kubernetes
Control Node undercloud	Управление гипервизорами

SDS undercloud	Сервис создания логического уровня управления ресурсами хранения. Позволяет программно объединять диски в единое хранилище, которое оптимизировано для хранения больших объемов данных, обеспечивает их репликацию и высокую доступность
Общее	
ulf	Реализации динамической сетевой маршрутизации

1.3 Функциональность, предоставляемая ПО Evolution

ПО Evolution функционирует на физических серверах в ЦОДах и предоставляет возможность создавать множество виртуальных машин, которые могут работать одновременно.

Каждая виртуальная машина эмулирует работу реального компьютера, в том числе работу компонентов аппаратного обеспечения: процессоров, оперативной памяти, сетевых средств, хранилища и BIOS, поэтому в виртуальной среде можно запускать операционные системы без каких-либо модификаций.

Благодаря реализованной в ПО Evolution поддержке технологий аппаратной виртуализации и низким затратам ресурсов на функционирование системных сервисов, обеспечивается производительность виртуальных машин практически на уровне аппаратных аналогов.

Пользователю доступны сервисы по:

– автоматическому разворачиванию контейнеризированных приложений и созданию кластеров Kubernetes;

– просмотру событий в системе, инициаторах и времени этих событий. Как следствие позволяет проверять работу системы на соответствие стандартам безопасности, требованиям законодательства и корпоративным политикам;

– сбору и хранению метрики ресурсов. С помощью мониторинга можно отслеживать ключевые показатели производительности и поддерживать стабильную работу приложений;

– созданию логического уровня управления ресурсами хранения. Позволяет программно объединять диски в единое хранилище, которое оптимизировано для хранения больших объемов данных, обеспечивает их репликацию и высокую доступность;

– созданию виртуальных сетей и управлению ими.

Управление ПО Evolution происходит через Личный кабинет и Административную консоль.

Личный кабинет предназначен для сотрудников компании, которые используют инфраструктурные и платформенные сервисы. Гибкая ролевая модель личного кабинета позволяет настраивать для сотрудников роли и права, чтобы обеспечить нужные уровни доступа и безопасность при управлении сервисами.

Административную консоль используют системные администраторы — сотрудники организации, которые отвечают за доступ к облаку и его настройку. Через административную консоль можно создавать подразделения для организации, распределять облачные ресурсы между задачами и командами.

На основе ПО Evolution, за счет возможности расширения базового функционала и предоставления API-интерфейсов всех модулей, возможно предоставлять широкий спектр услуг.

Для управления инфраструктурой ПО Evolution предоставляет как Representational State Transfer Application Programming Interface (REST-API) интерфейсы, так и графический web-портал.

2 Последовательность действий Клиента для достижения соответствия требованиям ГОСТ Р 57580

При возникновении потребности в соответствии ПО Evolution требованиям ГОСТ Р 57580, Клиенту необходимо выполнить следующие действия:

1. Изучить настоящий документ.

2. Построить инфраструктуру с использованием ПО Evolution, учетом требований ГОСТ Р 57580 и настоящего документа.

3. Выполнить требования ГОСТ Р 57580 в своей зоне ответственности.

4. Выбрать аудитора (с учетом требований соответствующих актуальных положений, например, п. 9 Положения 683-П или 757-П) и провести аудит инфраструктуры, развернутой на базе ПО Evolution, на соответствие требованиям ГОСТ Р 57580.

3 Разделение ответственности

3.1 Выполнение требований ПО Evolution

ПО Evolution предоставляет сервисы, которые можно использовать для обработки и хранения информации Клиента. ПО Evolution обеспечивает выполнение требований ГОСТ Р 57580 в части обслуживаемой инфраструктуры, на базе которой функционируют сервисы IaaS, а также в части сервисов PaaS, размещаемых поверх инфраструктуры IaaS. Для инфраструктурных элементов реализованы технические и организационные меры защиты информации, а именно:

- идентификация и аутентификация пользователей, являющихся работниками Клиента;
- управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;
- управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;
- защита обратной связи при вводе аутентификационной информации;
- идентификация и аутентификация пользователей, не являющихся работниками Клиента (внешних пользователей);
- управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;
- реализация ролевого метода доступа и правил разграничения доступа;
- назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ПО Evolution;
- ограничение неуспешных попыток входа в ПО Evolution;
- ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя ПО Evolution;
- блокирование сеанса доступа в ПО Evolution после установленного времени бездействия (неактивности) пользователя или по его запросу
- разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации;
- управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения;
- определение событий безопасности, подлежащих регистрации, и сроков их хранения;
- определение состава и содержания информации о событиях безопасности, подлежащих регистрации;
- сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения;
- генерирование временных меток и (или) синхронизация системного времени;
- защита информации о событиях безопасности;

– контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ПО Evolution;

– контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации;

– идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации;

– управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин;

– регистрация событий безопасности в виртуальной инфраструктуре;

– управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры;

– управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных;

– контроль целостности виртуальной инфраструктуры и ее конфигураций;

– резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры;

– разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей;

– изоляция процессов (выполнение программ) в выделенной области памяти;

– исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы ПО Evolution.

3.2 Выполнение требований Клиентом

Чтобы соответствовать требованиям ГОСТ Р 57580, Клиенту необходимо корректно:

– настроить параметры функционирования средств, которые размещаются в виртуальной инфраструктуре;

– при необходимости выполнить процедуры и процессы, связанных с обеспечением информационной безопасности, согласно актуальным требованиям регуляторов (ФСТЭК России, ФСБ России, ЦБ РФ и др.).

3.3 Общее разделение ответственности

ПО Evolution способствует реализации мер защиты информации, при этом нельзя исключать человеческий фактор или злой умысел. Соответственно, под обоюдной ответственностью в настоящем документе понимается процесс, когда в процессе реализации мер защиты информации участвуют одновременно и пользователь, и ПО Evolution.

Таблица 3 содержит обобщенную табличную форму разделения ответственности, указанной в ГОСТ Р 57580 (п.7 «Требования к системе защиты информации», п.8 «Требования к организации и управлению защитой информации» и п.9 «Требования к защите информации на этапах жизненного цикла автоматизированных систем и приложений»).

ПО Evolution способствует реализации мер защиты информации, при этом нельзя исключать человеческий фактор или злой умысел. Соответственно, под обоюдной ответственностью в настоящем документе понимается процесс, когда в процессе реализации мер защиты информации участвуют одновременно и пользователь, и ПО Evolution.

Таблица 3 – Разделение ответственности

Процесс/Направление/Этап	**Подпроцесс (при наличии)**	**Ответственность**
Требования к системе защиты информации (Процесс)		
Обеспечение защиты информации при управлении доступом	Управление учетными записями и правами субъектов логического доступа	Обоюдная
	Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа	Обоюдная
	Защита информации при осуществлении физического доступа	Обоюдная
	Идентификация, классификация и учет ресурсов и объектов доступа	Обоюдная
Обеспечение защиты вычислительных сетей	Сегментация и межсетевое экранирование вычислительных сетей	Клиент
	Выявление сетевых вторжений и атак	Клиент
	Защита информации, передаваемой по вычислительным сетям	Клиент
	Защита беспроводных сетей	Клиент
Контроль целостности и защищенности информационной инфраструктуры		Обоюдная
Защита от вредоносного кода		Обоюдная
Предотвращение утечек информации		Клиент
Управление инцидентами защиты информации	Мониторинг и анализ событий защиты информации	Обоюдная
	Обнаружение инцидентов защиты информации и реагирование на них	Обоюдная
Защита среды виртуализации		Обоюдная
Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств		Клиент
Требования к организации и управлению защитой информации (Направление)		
Планирование процесса системы защиты информации (Планирование)		Клиент
Реализация процесса системы защиты информации (Реализация)		Клиент
Контроль процесса системы защиты информации" (Контроль)		Обоюдная
Совершенствование процесса системы защиты информации (Совершенствование)		Клиент

Требования к защите информации на этапах жизненного цикла автоматизированных систем и приложений (Этап)	
Создание (модернизация) автоматизированной системы (далее – АС)	Обоюдная
Ввод в эксплуатацию АС	Клиент
Эксплуатация (сопровождение) АС	Клиент
Эксплуатация (сопровождение) и снятие с эксплуатации АС	Клиент

4 Разделение ответственности при выполнении требований к системе защиты информации

Раздел содержит описание разделения ответственности по процессам и подпроцессам в рамках выполнения требований, указанных в п.7 ГОСТ Р 57580. В разделе указаны только меры на ответственности ПО Evolution. Остальные меры должен выполнить Клиент самостоятельно.

4.1 Процесс 1 «Обеспечение защиты информации при управлении доступом» (меры групп УЗП, РД, ФД и ИУ)

Подраздел содержит перечень подпроцессов для обеспечения защиты информации при управлении доступом, согласно пп.7.2 ГОСТ Р 57580.

4.1.1 Подпроцесс «Управление учетными записями и правами субъектов логического доступа» (УЗП.1 – УЗП.29)

ПО Evolution способствует реализации следующих мер:

– УЗП.1 – Осуществление логического доступа пользователями и эксплуатационным персоналом под уникальными и персонифицированными учетными записями;

– УЗП.2 – Контроль соответствия фактического состава разблокированных учетных записей фактическому составу легальных субъектов логического доступа;

– УЗП.3 – Контроль отсутствия незаблокированных учетных записей;

– УЗП.4 – Контроль отсутствия незаблокированных учетных записей неопределенного целевого назначения;

– УЗП.5 – Документарное определение правил предоставления (отзыва) и блокирования логического доступа;

– УЗП.6 – Назначение для всех ресурсов доступа распорядителя логического доступа (владельца ресурса доступа);

– УЗП.7 – Предоставление прав логического доступа по решению распорядителя логического доступа (владельца ресурса доступа);

– УЗП.8 – Хранение эталонной информации о предоставленных правах логического доступа и обеспечение целостности указанной информации;

– УЗП.9 – Контроль соответствия фактических прав логического доступа эталонной информации о предоставленных правах логического доступа;

– УЗП.12 – Контроль необходимости отзыва прав субъектов логического доступа при изменении их должностных обязанностей;

– УЗП.13 – Контроль прекращения предоставления логического доступа и блокирование учетных записей при истечении периода (срока) предоставления логического доступа

– УЗП.14 – Установление фактов неиспользования субъектами логического доступа предоставленных им прав на осуществление логического доступа на протяжении периода времени, превышающего 90 дней;

– УЗП.15 – Установление фактов неиспользования субъектами логического доступа предоставленных им прав на осуществление логического доступа на протяжении периода времени, превышающего 45 дней;

– УЗП.16 – Реализация контроля со стороны распорядителя логического доступа целесообразности дальнейшего предоставления прав логического доступа, не использованных субъектами на протяжении периода времени, указанного в мерах УЗП.14, УЗП.15;

– УЗП.22 – Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего привилегированными правами логического доступа, позволяющими осуществить деструктивное воздействие, приводящие к нарушению выполнения бизнес-процессов или технологических процессов финансовой организации;

– УЗП.23 – Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала и пользователей, обладающих правами логического доступа, в том числе в АС, позволяющими осуществить операции (транзакции), приводящие к финансовым последствиям для финансовой организации, клиентов и контрагентов;

– УЗП.24 – Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по управлению логическим доступом;

– УЗП.25 – Регистрация событий защиты информации, связанных с действиями по управлению учетными записями и правами субъектов логического доступа;

– УЗП.26 – Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по управлению техническими мерами, реализующими многофакторную аутентификацию;

– УЗП.27 – Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по изменению параметров настроек средств и систем защиты информации, параметров настроек АС, связанных с защитой информации;

– УЗП.28 – Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по управлению криптографическими ключами.

4.1.2 Подпроцесс «Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа» (РД.1 – РД.44)

ПО Evolution способствует реализации следующих мер:

– РД.1 – Идентификация и однофакторная аутентификация пользователей;

– РД.2 – Идентификация и многофакторная аутентификация пользователей;

– РД.3 – Идентификация и однофакторная аутентификация эксплуатационного персонала;

– РД.4 – Идентификация и многофакторная аутентификация эксплуатационного персонала;

– РД.8 – Сокрытие (неотображение) паролей при их вводе субъектами доступа;

– РД.9 – Запрет использования учетных записей субъектов логического доступа с незаданными аутентификационными данными или заданными по умолчанию разработчиком ресурса доступа, в том числе разработчиком АС;

– РД.11 – Реализация необходимых типов (чтение, запись, выполнение или иной тип) и правил разграничения логического доступа к ресурсам доступа, в том числе АС;

– РД.12 – Запрет множественной аутентификации субъектов логического доступа с использованием одной учетной записи путем открытия параллельных сессий логического доступа с использованием разных автоматизированных рабочих мест (далее – АРМ), в том числе виртуальных;

– РД.13 – Обеспечение возможности выполнения субъектом логического доступа работниками финансовой организации процедуры принудительного прерывания сессии логического доступа и (или) приостановки осуществления логического доступа (с прекращением отображения на мониторе АРМ информации, доступ к которой получен в рамках сессии осуществления логического доступа);

– РД.14 – Автоматическое прерывание сессии логического доступа (приостановка осуществления логического доступа) по истечении установленного времени бездействия (неактивности) субъекта логического доступа, не превышающего 15 мин., с прекращением отображения на мониторе АРМ информации, доступ к которой получен в рамках сессии осуществления логического доступа;

– РД.17 – Запрет на использование технологии аутентификации с сохранением аутентификационных данных в открытом виде в средстве вычислительной техники;

– РД.19 – Смена паролей пользователей не реже одного раза в год;

– РД.20 – Смена паролей эксплуатационного персонала не реже одного раза в квартал;

– РД.21 – Использование пользователями паролей длиной не менее восьми символов;

– РД.22 – Использование эксплуатационным персоналом паролей длиной не менее шестнадцати символов;

– РД.23 – Использование при формировании паролей субъектов логического доступа символов, включающих буквы (в верхнем и нижнем регистрах) и цифры;

– РД.24 – Запрет использования в качестве паролей субъектов логического доступа легко вычисляемых сочетаний букв и цифр (например, имена, фамилии, наименования, общепринятые сокращения);

– РД.26 – Хранение копий аутентификационных данных эксплуатационного персонала на выделенных машинных носителях информации или на бумажных носителях;

– РД.27 – Реализация защиты копий аутентификационных данных эксплуатационного персонала от несанкционированного доступа при их хранении на машинных носителях информации или бумажных носителях;

– РД.28 – Регистрация персонификации, выдачи (передачи) и уничтожения персональных технических устройств аутентификации, реализующих многофакторную аутентификацию;

– РД.29 – Смена аутентификационных данных в случае их компрометации;

– РД.31 – Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод) при разграничении логического доступа к ресурсам доступа;

– РД.32 – Реализация ролевого метода (с определением для каждой роли прав доступа) при разграничении логического доступа в АС;

– РД.33 – Реализация необходимых типов (чтение, запись, выполнение или иной тип) и правил разграничения логического доступа к ресурсам доступа, в том числе АС;

– РД.37 – Контроль состава разрешенных действий в АС до выполнения идентификации и аутентификации;

– РД.39 – Регистрация выполнения субъектами логического доступа ряда неуспешных последовательных попыток аутентификации;

– РД.40 – Регистрация осуществления субъектами логического доступа идентификации и аутентификации;

– РД.41 – Регистрация авторизации, завершения и (или) прерывания (приостановки) осуществления эксплуатационным персоналом и пользователями логического доступа, в том числе в АС;

– РД.42 – Регистрация запуска программных сервисов, осуществляющих логический доступ;

– РД.43 – Регистрация изменений аутентификационных данных, используемых для осуществления логического доступа;

– РД.44 – Регистрация действий пользователей и эксплуатационного персонала, предусмотренных в случае компрометации их аутентификационных данных.

4.1.3 Подпроцесс «Защита информации при осуществлении физического доступа» (ФД.1 – ФД.21)

ПО Evolution способствует реализации мер ФД.14 – Хранение архивов информации средств (систем) контроля и управления доступом не менее трех лет.

4.1.4 Подпроцесс «Идентификация и учет ресурсов и объектов доступа» (ИУ.1 – ИУ.8)

ПО Evolution способствует реализации меру ИУ.5 – Контроль выполнения операций по созданию, удалению и резервному копированию ресурсов доступа (баз данных, сетевых файловых ресурсов, виртуальных машин).

4.2 Процесс 2 «Обеспечение защиты вычислительных сетей» (меры групп СМЭ, ВСА, ЗВС и ЗБС)

Подраздел содержит перечень подпроцессов для обеспечения защиты информации при управлении доступом, согласно пп. 7.3 ГОСТ Р 57580.

4.2.1 Подпроцесс «Сегментация и межсетевое экранирование вычислительных сетей» (СМЭ.1 – СМЭ.21)

ПО Evolution не способствует реализации мер группы СМЭ.

4.2.2 Подпроцесс «Выявление вторжений и сетевых атак» (ВСА.1 – ВСА.14)

ПО Evolution не способствует реализации мер группы ВСА.

4.2.3 Подпроцесс «Защита информации, передаваемой по вычислительным сетям» (ЗВС.1, ЗВС.2)

ПО Evolution не способствует реализации мер группы ЗВС.

4.2.4 Подпроцесс «Защита беспроводных сетей» (ЗБС.1 – ЗБС.10)

ПО Evolution не способствует реализации мер группы ЗБС.

4.3 Процесс 3 «Контроль целостности и защищенности информационной инфраструктуры» (меры группы ЦЗИ)

Подраздел содержит перечень подпроцессов для обеспечения защиты информации при управлении доступом, согласно пп. 7.4 ГОСТ Р 57580.

ПО Evolution способствует реализации следующих мер:

– ЦЗИ.20 – Контроль состава разрешенного для использования программного обеспечения АРМ пользователей и эксплуатационного персонала;

– ЦЗИ.21 – Исключение возможности установки и (или) запуска неразрешенного для использования программного обеспечения АРМ пользователей и эксплуатационного персонала;

– ЦЗИ.30 – Регистрация запуска программных сервисов;

– ЦЗИ.34 – Регистрация результатов выполнения операций контроля целостности запускаемых компонентов программного обеспечения АС;

– ЦЗИ.36 – Регистрация результатов выполнения операций по контролю целостности и достоверности источников получения при распространении и (или) обновлении программного обеспечения АС, программного обеспечения средств и систем защиты информации, системного программного обеспечения.

4.4 Процесс 4 «Защита от вредоносного кода» (мера группы ЗВК)

Подраздел содержит перечень подпроцессов для обеспечения защиты информации при управлении доступом, согласно пп. 7.5 ГОСТ Р 57580.

ПО Evolution способствует реализации меру ЗВК.28 – Регистрация нарушений целостности программных компонентов средств защиты от вредоносного кода.

4.5 Процесс 5 «Предотвращение утечек информации» (мера группы ПУИ)

Подраздел содержит перечень подпроцессов для обеспечения защиты информации при управлении доступом, согласно пп. 7.6 ГОСТ Р 57580.

ПО Evolution не способствует реализации мер группы ПУИ.

4.6 Процесс 6 «Управление инцидентами защиты информации» (меры групп МАС и РИ)

Подраздел содержит перечень подпроцессов для обеспечения защиты информации при управлении доступом, согласно пп. 7.7 ГОСТ Р 57580.

4.6.1 Подпроцесс «Мониторинг и анализ событий защиты информации» (МАС.1 – МАС.23)

ПО Evolution способствует реализации следующих мер:

– МАС.9 – Генерация временных меток для данных регистрации о событиях защиты информации и синхронизации системного времени объектов информатизации, используемых для формирования, сбора и анализа данных регистрации;

– МАС.14 – Реализация защиты данных регистрации о событиях защиты информации от несанкционированного доступа при их хранении, обеспечение целостности и доступности хранимых данных регистрации;

– МАС.15 – Обеспечение возможности доступа к данным регистрации о событиях защиты информации в течение трех лет;

– МАС.16 – Обеспечение возможности доступа к данным регистрации о событиях защиты информации в течение пяти лет.

4.6.2 Подпроцесс «Обнаружение инцидентов защиты информации и реагирование на них» (РИ.1 – 19)

ПО Evolution способствует реализации следующих мер:

– РИ.1 – Регистрация информации о событиях защиты информации, потенциально связанных с инцидентами защиты информации, в том числе НСД, выявленными в рамках мониторинга и анализа событий защиты информации;

– РИ.2 – Регистрация информации, потенциально связанной с инцидентами защиты информации, в том числе НСД, полученной от работников, клиентов и (или) контрагентов финансовой организации;

– РИ.14 – Установление и применение единых правил закрытия инцидентов защиты информации.

4.7 Процесс 7 «Защита среды виртуализации» (меры группы ЗСВ)

Подраздел содержит перечень подпроцессов для обеспечения защиты информации при управлении доступом, согласно пп. 7.8 ГОСТ Р 57580.

ПО Evolution способствует реализации следующих мер:

– ЗСВ.1 – Разграничение и контроль осуществления одновременного доступа к виртуальным машинам с АРМ пользователей и эксплуатационного персонала только в пределах одного контура безопасности;

– ЗСВ.2 – Разграничение и контроль осуществления одновременного доступа к виртуальным машинам с АРМ пользователей и эксплуатационного персонала только в пределах одного контура безопасности на уровне не выше третьего (сетевой) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1;

– ЗСВ.5 – Идентификация и аутентификация пользователей серверными компонентами виртуализации и (или) средствами централизованных сервисов аутентификации при предоставлении доступа к виртуальным машинам;

– ЗСВ.6 – Реализация необходимых методов предоставления доступа к виртуальным машинам, обеспечивающих возможность доступа с использованием одних аутентификационных данных только к одной виртуальной машине;

– ЗСВ.7 – Реализация необходимых методов предоставления доступа к виртуальным машинам, обеспечивающих возможность доступа с использованием одних аутентификационных данных только к одной виртуальной машине с одного АРМ пользователя или эксплуатационного персонала;

– ЗСВ.9 – Контроль и протоколирование доступа эксплуатационного персонала к серверным компонентам виртуализации и системе хранения данных с реализацией двухфакторной аутентификации;

– ЗСВ.13 – Выделение в вычислительных сетях финансовой организации отдельных сегментов (групп сегментов), в том числе виртуальных, используемых для размещения совокупности виртуальных машин, предназначенных для размещения серверных компонент АС, включенных в разные контуры безопасности;

– ЗСВ.14 – Выделение в вычислительных сетях финансовой организации отдельных сегментов (групп сегментов), в том числе виртуальных, используемых для размещения совокупности виртуальных машин, предназначенных для размещения АРМ пользователей и эксплуатационного персонала, включенных в разные контуры безопасности;

– ЗСВ.15 – Организация информационного обмена между сегментами (группами сегментов) вычислительных сетей, определенных мерами ЗСВ.13 и ЗСВ.14 настоящей таблицы, физическим оборудованием (программно-аппаратным комплексом) и (или) программными средствами межсетевого экранирования, функционирующими на уровне гипервизора среды виртуализации;

– ЗСВ.20 – Исключение возможности информационного взаимодействия и переноса информации между сегментами вычислительных сетей, входящими в разные контуры безопасности, с использованием АРМ пользователей и эксплуатационного персонала, эксплуатируемых для осуществления доступа к виртуальным машинам разных контуров безопасности;

– ЗСВ.22 – Выделение отдельных сегментов управления, в которых располагаются АРМ эксплуатационного персонала, используемые для выполнения задач администрирования серверных компонент виртуализации и системы хранения данных;

– ЗСВ.23 – Регламентация и контроль выполнения операций в рамках жизненного цикла базовых образов виртуальных машин и операций по копированию образов виртуальных машин;

– ЗСВ.26 – Контроль целостности, выполняемый при запуске (загрузке) виртуальной машины (базового образа виртуальной машины; ПО, включенного в пользовательский профиль виртуальной машины; параметров настроек ПО технических мер защиты информации, применяемых в пределах виртуальных машин);

– ЗСВ.32 – Регистрация операций, связанных с запуском (остановкой) виртуальных машин;

– ЗСВ.33 – Регистрация операций, связанных с изменением параметров настроек виртуальных сетевых сегментов, реализованных средствами гипервизора;

– ЗСВ.34 – Регистрация операций, связанных с созданием и удалением виртуальных машин;

– ЗСВ.35 – Регистрация операций, связанных с созданием, изменением, копированием, удалением базовых образов виртуальных машин;

– ЗСВ.36 – Регистрация операций, связанных с копированием текущих образов виртуальных машин;

– ЗСВ.37 – Регистрация операций, связанных с изменением прав логического доступа к серверным компонентам виртуализации;

– ЗСВ.38 – Регистрация операций, связанных с изменением параметров настроек серверных компонентов виртуализации;

– ЗСВ.39 – Регистрация операций, связанных с аутентификацией и авторизацией эксплуатационного персонала при осуществлении доступа к серверным компонентам виртуализации;

– ЗСВ.40 – Регистрация операций, связанных с аутентификацией и авторизацией пользователей при осуществлении доступа к виртуальным машинам;

– ЗСВ.41 – Регистрация операций, связанных с запуском (остановкой) ПО серверных компонент виртуализации;

– ЗСВ.42 – Регистрация операций, связанных с изменением параметров настроек технических мер защиты информации, используемых для реализации контроля доступа к серверным компонентам виртуализации;

– ЗСВ.43 – Регистрация операций, связанных с изменением настроек технических мер защиты информации, используемых для обеспечения защиты виртуальных машин.

4.8 Процесс 8 «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств» (меры группы ЗУД)

Подраздел содержит перечень подпроцессов для обеспечения защиты информации при управлении доступом, согласно пп. 7.9 ГОСТ Р 57580.

ПО Evolution не способствует реализации мер группы ЗУД.

5 Разделение ответственности при выполнении требований к организации и управлению защитой информации

Раздел содержит описание разделения ответственности по направлениям в рамках выполнения требований, указанных в п.8 ГОСТ Р 57580. В разделе указаны только меры на ответственности ПО Evolution. Остальные меры должен выполнить Клиент самостоятельно.

5.1 Направление 1 «Планирование процесса системы защиты информации» (мера группы ПЗИ)

Подраздел содержит перечень подпроцессов для обеспечения защиты информации при управлении доступом, согласно пп. 8.2 ГОСТ Р 57580.

ПО Evolution не способствует реализации мер группы ПЗИ.

5.2 Направление 2 «Реализация процесса системы защиты информации» (мера группы РЗИ)

Подраздел содержит перечень подпроцессов для обеспечения защиты информации при управлении доступом, согласно пп. 8.3 ГОСТ Р 57580.

ПО Evolution не способствует реализации мер группы РЗИ.

5.3 Направление 3 «Контроль процесса системы защиты информации» (мера группы КЗИ)

Подраздел содержит перечень подпроцессов для обеспечения защиты информации при управлении доступом, согласно пп. 8.4 ГОСТ Р 57580.

ПО Evolution способствует реализации меры КЗИ.12 – Регистрация сбоев (отказов) технических мер защиты информации.

5.4 Направление 4 «Совершенствование процесса системы защиты информации» (мера группы СЗИ)

Подраздел содержит перечень подпроцессов для обеспечения защиты информации при управлении доступом, согласно пп. 8.3 ГОСТ Р 57580.

ПО Evolution не способствует реализации мер группы СЗИ.

6 Разделение ответственности при выполнении требований к защите информации на этапах жизненного цикла автоматизированных систем и приложений

Раздел содержит описание разделения ответственности по этапам жизненного цикла в рамках выполнения требований, указанных в п.9 ГОСТ Р 57580. В разделе указаны только меры на ответственности ПО Evolution. Остальные меры должен выполнить Клиент самостоятельно.

6.1 Этап «Создание (модернизация) автоматизированной системы» (ЖЦ.1 – ЖЦ.11)

Подраздел содержит перечень подпроцессов для обеспечения защиты информации при управлении доступом, согласно пп. 9.5 ГОСТ Р 57580.

ПО Evolution способствует реализации меры ЖЦ.6 – Контроль предоставления и обеспечение разграничения доступа в сегментах разработки и тестирования.

6.2 Этап «Ввод в эксплуатацию автоматизированной системы» (ЖЦ.12 – ЖЦ.14)

Подраздел содержит перечень подпроцессов для обеспечения защиты информации при управлении доступом, согласно пп. 9.6 ГОСТ Р 57580.

ПО Evolution не способствует реализации меры ЖЦ.12 – ЖЦ.14.

6.3 Этап «Эксплуатация (сопровождение) автоматизированной системы» (ЖЦ.15 – ЖЦ.25)

Подраздел содержит перечень подпроцессов для обеспечения защиты информации при управлении доступом, согласно пп. 9.7 ГОСТ Р 57580.

ПО Evolution не способствует реализации меры ЖЦ.15 – ЖЦ.25.

6.4 Этап «Эксплуатация (сопровождение) и снятие с эксплуатации автоматизированной системы» (ЖЦ.26 – ЖЦ.28)

Подраздел содержит перечень подпроцессов для обеспечения защиты информации при управлении доступом, согласно пп. 9.8 ГОСТ Р 57580.

ПО Evolution не способствует реализации меры ЖЦ.26 – ЖЦ.28.