Общество с ограниченной ответственностью
«Центр Безопасности Информационных Систем»
Лицензия Федеральной службы по техническому и экспортному контролю
на деятельность по технической защите конфиденциальной информации
Регистрационный номер 2446 от 30 сентября 2014 года

Выписка из заключения по результатам аттестационных испытаний системы защиты персональных данных по требованиям ФЗ-152 «О персональных данных»

Заявитель: Общество с ограниченной ответственностью «Мэйл.Ру» (ООО «Мэйл.Ру»), ИНН 7743001840.

Полное и сокращенное наименование заявителя, ИНН заявителя

Аттестационный центр: Общество с ограниченной ответственностью «Центр Безопасности информационных Систем» (ООО «ЦБИС»), ИНН 7715981266, лицензия ФСТЭК России на техническую защиту конфиденциальной информации № 2446 от 30 сентября 2014 года.

Полное и сокращенное наименование аттестационного центра, ИНН, реквизиты лицензии на осуществление деятельности

Объект оценки: информационная система персональных данных «Сервиса Mail.ru Cloud Solution Infra» (ИСПДн «MCS»).

Тип, полное и сокращенное наименование объекта оценки

Уровень защищенности: для объекта оценки установлен 3 (третий) уровень защищенности персональных данных при их обработке в ИСПДн «MCS».

Уровень защищенности персональных данных

Результат оценки: объект оценки соответствует требованиям ФЗ-152 «О персональных данных» и 3 (третьему) уровню защищенности персональных данных в соответствии с нормативно-правовыми актами:

- Постановление Правительства РФ № 1119 от 01 ноября 2012 года «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Приказ ФСТЭК России № 21 от 18 февраля 2013 года «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- Приказ ФСБ России № 378 от 10 июля 2014 года «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

Вывод по результатам оценки соответствия и перечень нормативно-правовых актов которым объект соответствует

Приложение:

1. Краткое описание мер защиты ИСПДн «MCS», которые позволят конечным заказчикам (клиентам) ООО «Мэйл.Ру» соответствовать 3 (третьему) уровню защищенности.

Генеральный директор ООО «ЦБИС» _____ Поспелов Н.С.

15 марта 2019 года

Приложение 1. К выписке из заключения по результатам аттестационных испытаний системы защиты персональных данных по требованиям ФЗ-152 «О персональных данных» от 15.03.2019

Краткое описание мер защиты ИСПДн «MCS», которые позволят конечным заказчикам ООО «Мэйл.Ру» соответствовать 3 (третьему) уровню защищенности

<table>
<tr><th>Меры защиты по Приказу ФСТЭК № 21 от 18.02.2013</th><th>Реализация на стороне ИСПДн «MCS» ООО «Мэйл.Ру»</th><th>Реализация на стороне конечного заказчика (клиента)</th></tr>
<tr><td colspan="3">Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)</td></tr>
<tr><td>Идентификация и аутентификация пользователей, являющихся работниками оператора. (ИАФ.1)</td><td rowspan="5">Меры защиты реализованы:
1) на уровне операционных систем:
- используется специализированное сертифицированное средство защиты от несанкционированного доступа (СЗИ от НСД).
2) на уровне платформы облачных сервисов Mail.ru Group (далее «Платформа»):
- штатными функциями Платформы.

Описание реализации мер защиты на уровне среды виртуализации (гипервизора) и в виртуальных машинах смотрите ниже в категории мер «Защита среды виртуализации» (ЗСВ).</td><td rowspan="5">Внимание: меры защиты ИАФ связаны только с защитой физических серверов и физических рабочих станций, так как для сред виртуализации (гипервизоров) и виртуальных машин в Приказе ФСТЭК № 21 существует отдельная категория мер «Защита среды виртуализации (ЗСВ)» (см. ниже).

Меры нужно реализовывать:
если со стороны клиента к приобретенным клиентом облачным ресурсам Платформы подключаются офисные рабочие станции сотрудников/подрядчиков, то их необходимо защитить СЗИ от НСД или на них должна стоять операционная система прошедшая оценку соответствия (сертифицированная или с декларацией соответствия).

Меры не нужно реализовывать:
если приобретенные клиентом облачные ресурсы Платформы, функционируют без подключения офисных рабочих станций сотрудников/подрядчиков клиента.</td></tr>
<tr><td>Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов (ИАФ.3)</td></tr>
<tr><td>Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации. (ИАФ.4)</td></tr>
<tr><td>Защита обратной связи при вводе аутентификационной информации. (ИАФ.5)</td></tr>
<tr><td>Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей). (ИАФ.6)</td></tr>
<tr><td colspan="3">Управление доступом субъектов доступа к объектам доступа (УПД)</td></tr>
<tr><td>Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей. (УПД.1)</td><td rowspan="3">Меры защиты реализованы:
1) на уровне сети:
- используется специализированное сертифицированное средство межсетевого экранирования (МЭ).
2) на уровне операционных систем:
- используется специализированное сертифицированное средство защиты от несанкционированного доступа (СЗИ от НСД).
3) на уровне Платформы:
- штатными функциями Платформы.

Описание реализации мер защиты на уровне среды виртуализации</td><td rowspan="3">Внимание: меры защиты УПД в целом связаны с защитой физических серверов и рабочих станций, так как для сред виртуализации (гипервизоров) и виртуальных машин в Приказе ФСТЭК № 21 существует отдельная категория мер «Защита среды виртуализации (ЗСВ)» (см. ниже).

Меры нужно реализовывать:</td></tr>
<tr><td>Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа. (УПД.2)</td></tr>
<tr><td>Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы</td></tr>
</table>

Меры защиты по Приказу ФСТЭК № 21 от 18.02.2013	Реализация на стороне ИСПДн «MCS» ООО «Мэйл.Ру»	Реализация на стороне конечного заказчика (клиента)
управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами. (УПД.3)	(гипервизора) и в виртуальных машинах смотрите ниже в категории мер «Защита среды виртуализации» (ЗСВ).	**Меры нужно реализовывать:** если со стороны клиента к приобретенным клиентом облачным ресурсам Платформы подключаются офисные рабочие станции сотрудников/подрядчиков, то их необходимо защитить СЗИ от НСД или на них должна стоять операционная система прошедшая оценку соответствия (сертифицированная или с декларацией соответствия). Также рабочие станции должны быть защищены МЭ с оценкой соответствия (сертифицированным или с декларацией соответствия). **Меры не нужно реализовывать:** если приобретенные клиентом облачные ресурсы Платформы, функционируют без подключения офисных рабочих станций сотрудников/подрядчиков клиента.
Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы. (УПД.4)		
Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы. (УПД.5)		
Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе). (УПД.6)		
Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу (УПД.10).		
Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации (УПД.11)		
Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети. (УПД.13)		
Регламентация и контроль использования в информационной системе технологий беспроводного доступа. (УПД.14)	Не используется	**Меру нужно реализовывать:** если клиент включит в состав ИСПДн, созданной на базе виртуальных ресурсов Платформы, офисные рабочие станции сотрудников/подрядчиков и со стороны клиента будут использоваться средства беспроводного доступа, то необходимо будет использовать специализированное средство защиты беспроводных соединений, прошедшее оценку соответствия (сертифицированное или с декларацией соответствия).
Регламентация и контроль использования в информационной системе мобильных технических средств. (УПД.15)	Не используется	**Меру нужно реализовывать:** если клиент включит в состав ИСПДн, созданной на базе виртуальных ресурсов Платформы, офисные рабочие станции

Меры защиты по Приказу ФСТЭК № 21 от 18.02.2013	Реализация на стороне ИСПДн «MCS» ООО «Мэйл.Ру»	Реализация на стороне конечного заказчика (клиента)
		сотрудников/подрядчиков и со стороны клиента будут использоваться мобильные технические средства, то необходимо будет установить на них СЗИ от НСД или на них должна стоять операционная система прошедшая оценку соответствия (сертифицированная или с декларацией соответствия), а также САВЗ.
Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы). (УПД.16)	Аналогично УПД.3 (см. выше).	Аналогично УПД.3 (см. выше).
Защита машинных носителей персональных данных (ЗНИ)		
Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания (ЗНИ.8).	**Мера защиты реализована:** на уровне операционных систем: - используется специализированное сертифицированное средство защиты от несанкционированного доступа (СЗИ от НСД).	**Меры нужно реализовывать:** если клиент включит в состав ИСПДн, созданной на базе виртуальных ресурсов Платформы, офисные рабочие станции сотрудников/подрядчиков, то такие рабочие места должны быть защищены СЗИ от НСД или на них должна стоять операционная система прошедшая оценку соответствия (сертифицированная или с декларацией соответствия).
Регистрация событий безопасности (РСБ)		
Определение событий безопасности, подлежащих регистрации, и сроков их хранения. (РСБ.1) Определение состава и содержания информации о событиях безопасности, подлежащих регистрации. (РСБ.2) Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения. (РСБ.3) Защита информации о событиях безопасности. (РСБ.7)	**Меры защиты реализованы:** 1) на уровне сети: - используется специализированное сертифицированное средство межсетевого экранирования (МЭ). 2) на уровне операционных систем: - используется специализированное сертифицированное средство защиты от несанкционированного доступа (СЗИ от НСД). 3) на уровне Платформы: - штатными функциями Платформы. Описание реализации мер защиты на уровне среды виртуализации (гипервизора) и в виртуальных машинах смотрите ниже в категории мер «Защита среды виртуализации» (ЗСВ).	**Внимание:** меры защиты РСБ связаны только с защитой физических серверов и физических рабочих станций, так как для сред виртуализации (гипервизоров) и виртуальных машин в Приказе ФСТЭК № 21 существует отдельная категория мер «Защита среды виртуализации (ЗСВ)» (см. ниже). **Меры нужно реализовывать:** если со стороны клиента к приобретенным клиентом облачным ресурсам Платформы подключаются офисные рабочие станции сотрудников/подрядчиков, то их необходимо защитить СЗИ от НСД или на них должна стоять операционная система прошедшая оценку соответствия (сертифицированная или с декларацией соответствия). **Меры не нужно реализовывать:** если приобретенные клиентом облачные ресурсы Платформы,

Меры защиты по Приказу ФСТЭК № 21 от 18.02.2013	Реализация на стороне ИСПДн «MCS» ООО «Мэйл.Ру»	Реализация на стороне конечного заказчика (клиента)
		функционируют без подключения офисных рабочих станций сотрудников/подрядчиков клиента.
Антивирусная защита (АВЗ)		
Реализация антивирусной защиты. (АВЗ.1) Обновление базы данных признаков вредоносных компьютерных программ (вирусов). (АВЗ.2)	**Меры защиты реализованы:** на уровне операционных систем: - используется специализированное сертифицированное средство антивирусной защиты (САВЗ).	**Внимание:** меры защиты АВЗ связаны только с защитой физических серверов и физических рабочих станций, так как для сред виртуализации (гипервизоров) и виртуальных машин в Приказе ФСТЭК № 21 существует отдельная категория мер «Защита среды виртуализации (ЗСВ)» (см. ниже). **Меры нужно реализовывать:** если со стороны клиента к приобретенным клиентом облачным ресурсам Платформы подключаются офисные рабочие станции сотрудников/подрядчиков, то их необходимо защитить САВЗ с оценкой соответствия (сертифицированное или с декларацией соответствия). **Меры не нужно реализовывать:** если приобретенные клиентом облачные ресурсы Платформы, функционируют без подключения офисных рабочих станций сотрудников/подрядчиков клиента.
Контроль (анализ) защищенности персональных данных (АНЗ)		
Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей (АНЗ.1). Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации. (АНЗ.2) Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации (АНЗ.3). Контроль состава технических средств, программного обеспечения и средств защиты информации (АНЗ.4).	**Меры защиты реализованы:** на уровне операционных систем и сети: - используется специализированное сертифицированное средство анализа защищенности (САЗ).	**Внимание:** меры защиты АНЗ в целом связаны только с защитой физических серверов и физических рабочих станций, так как для сред виртуализации (гипервизоров) и виртуальных машин в Приказе ФСТЭК № 21 существует отдельная категория мер «Защита среды виртуализации (ЗСВ)» (см. ниже). **Меры нужно реализовывать:** если со стороны клиента к приобретенным клиентом облачным ресурсам Платформы подключаются офисные рабочие станции сотрудников/подрядчиков, то необходимо использовать САЗ с оценкой соответствия (сертифицированное или с декларацией соответствия). **Меры не нужно реализовывать:** если приобретенные клиентом

Меры защиты по Приказу ФСТЭК № 21 от 18.02.2013	Реализация на стороне ИСПДн «MCS» ООО «Мэйл.Ру»	Реализация на стороне конечного заказчика (клиента)
		облачные ресурсы Платформы, функционируют без подключения офисных рабочих станций сотрудников/подрядчиков клиента.
Защита среды виртуализации (ЗСВ)		
Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации. (ЗСВ.1).	**Меры защиты реализованы:** на уровне операционных систем гипервизоров: - используются штатные компоненты виртуализации операционных систем, прошедшие оценку соответствия в форме декларирования соответствия в соответствии с ФЗ-184 «О техническом регулировании».	**Меры нужно реализовывать:** в обязательном порядке в каждую виртуальную машину необходимо устанавливать сертифицированное СЗИ от НСД или виртуальные машины должны быть развернуты на базе операционных систем прошедших оценку соответствия (сертифицированных или с декларацией соответствия).
Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин. (ЗСВ.2).		
Регистрация событий безопасности в виртуальной инфраструктуре (ЗСВ.3).		
Реализация и управление антивирусной защитой в виртуальной инфраструктуре (ЗСВ.9).	**Мера защиты реализована:** на уровне операционных систем гипервизоров: - используется специализированное сертифицированное средство антивирусной защиты (САВЗ).	**Меру нужно реализовать:** в обязательном порядке в каждую виртуальную машину необходимо устанавливать САВЗ с оценкой соответствия (сертифицированное или с декларацией соответствия).
Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей. (ЗСВ.10).	Аналогично ЗСВ.2	Аналогично ЗСВ.2
Защита технических средств (ЗТС)		
Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены. (ЗТС.3)	**Мера защиты реализована:** на уровне центра обработки данных (ЦОД): - имеется постоянная охрана входа на территорию ЦОД; - имеется система контроля и управления доступом на территорию ЦОД и в помещение с ИСПДн Платформы.	**Меру нужно реализовывать:** если клиент включит в состав ИСПДн, созданной на базе виртуальных ресурсов Платформы, офисные рабочие станции сотрудников/подрядчиков, то для таких рабочих мест должна быть реализована указанная мера защиты в полном объеме. Под контролем и управлением физическим доступом понимается одно или все из перечисленных одновременно: - наличие системы контроля и управления доступом в помещение с ИСПДн; - наличие постоянной охраны помещения с ИСПДн.

Меры защиты по Приказу ФСТЭК № 21 от 18.02.2013	Реализация на стороне ИСПДн «MCS» ООО «Мэйл.Ру»	Реализация на стороне конечного заказчика (клиента)
Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр. (ЗТС.4)	**Мера защиты реализована:** 1) на уровне ЦОД: - при работе инженеров ООО «Мэйл.Ру» в ЦОД применяются организационные меры. 2) на уровне офисных помещений ООО «Мэйл.Ру»: - применяются организационные меры.	**Меру нужно реализовывать:** если клиент включит в состав ИСПДн, созданной на базе виртуальных ресурсов Платформы, офисные рабочие станции сотрудников/подрядчиков, то для таких рабочих мест должна быть реализована указанная мера защиты в полном объеме.
Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)		
Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи (ЗИС.3).	**Мера защиты реализована:** 1) на уровне каналов связи между ИСПДн Платформы и администраторами ООО «Мэйл.Ру»: - используется сертифицированное средство криптографической защиты информации (СКЗИ). 2) на уровне каналов связи между ИСПДн Платформы и клиентами: - используется сертифицированное средство криптографической защиты информации (СКЗИ).	**Меру нужно реализовывать:** если клиент включит в состав ИСПДн, созданной на базе виртуальных ресурсов Платформы, офисные рабочие станции сотрудников/подрядчиков, то связь рабочих мест с ИСПДн на Платформе должна осуществляться с использованием СКЗИ с оценкой соответствия (сертифицированное или с декларацией соответствия).
Защита беспроводных соединений, применяемых в информационной системе (ЗИС.20).	Не используется	**Меру нужно реализовывать:** если клиент включит в состав ИСПДн, созданной на базе виртуальных ресурсов Платформы, офисные рабочие станции сотрудников/подрядчиков и со стороны клиента будут использоваться средства беспроводного доступа, то необходимо будет использовать специализированное средство защиты беспроводных соединений, прошедшее оценку соответствия (сертифицированное или с декларацией соответствия).
Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)		
Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных (УКФ.1).	**Меры защиты реализованы:** 1) на уровне сети: - используется специализированное сертифицированное средство межсетевого экранирования (МЭ). 2) на уровне операционных систем: - используется специализированное сертифицированное средство защиты от несанкционированного доступа (СЗИ от НСД). 3) на уровне операционных систем и сети: - используется специализированное сертифицированное средство анализа защищенности (САЗ). 4) на уровне Платформы:	**Внимание:** меры защиты УКФ в целом связаны только с защитой физических серверов и физических рабочих станций, так как для сред виртуализации (гипервизоров) и виртуальных машин в Приказе ФСТЭК № 21 существует отдельная категория мер «Защита среды виртуализации (ЗСВ)» (см. выше). **Меру нужно реализовывать:** если клиент включит в состав ИСПДн, созданной на базе виртуальных ресурсов Платформы, офисные рабочие места сотрудников/подрядчиков, то для
Управление изменениями конфигурации информационной системы и системы защиты персональных данных (УКФ.2).		
Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты		

Меры защиты по Приказу ФСТЭК № 21 от 18.02.2013	Реализация на стороне ИСПДн «MCS» ООО «Мэйл.Ру»	Реализация на стороне конечного заказчика (клиента)
персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных (УКФ.3).	- штатными функциями Платформы. Описание реализации мер защиты на уровне среды виртуализации (гипервизора) и в виртуальных машинах смотрите выше в категории мер «Защита среды виртуализации» (ЗСВ).	таких рабочих мест должна быть реализована указанная мера защиты в полном объеме (см. подпункты 1) - 3) в столбце слева). **Примечание:** для реализации указанных мер могут применяться средства защиты не только с оценкой соответствия в форме сертификации, но и в форме декларирования соответствия.
Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных (УКФ.4).		