ООО «Селектел»
196084, Санкт-Петербург,
ул. Цветочная, д. 21, литера А

ТЕЛ./ФАКС +7 (812) 667-80-36 / 677-80-86

ИНН / ОГРН 7842393933 / 1089847357126

E-MAIL office@selectel.ru

САЙТ selectel.ru

Объект информатизации «Облачное хранилище Selectel»

Акт оценки эффективности принимаемых мер по обеспечению безопасности персональных данных для 3-го уровня защищенности

На 7 страницах

1. ООО «Селектел» (Лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации № 3449 от 20 февраля 2018 г.) проведена оценка эффективности принимаемых мер и соответствия системы защиты вычислительной инфраструктуры объекта информатизации «Облачное хранилище Selectel» требованиям по обеспечению безопасности персональных данных, определенным в Приказе ФСТЭК России № 21 от 18 февраля 2013 г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

2. В объем работ по оценке эффективности входят следующие компоненты информационной инфраструктуры ООО «Селектел»:
   — кластеры серверов распределенной системы хранения Ceph, используемые для хранения данных клиентов Selectel;
   — сервисные компоненты, используемые для управления системой хранения Ceph.

3. Технические средства располагаются на следующих территориальных площадках:
   — Ленинградская обл., Всеволжский р-н, пгт Дубровка, ул. Советская, д 1, лит. Б;
   — Ленинградская обл., Всеволжский р-н, пгт Дубровка, ул. Советская, уч. 1/1, лит. И..

4. Для инфраструктуры объекта информатизации «Облачное хранилище Selectel» признаны актуальными угрозы 3-го типа, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении.

5. Оценка эффективности принимаемых мер проведена в форме приемочных испытаний системы защиты объекта информатизации «Облачное хранилище Selectel».

6. По результатам проведения оценки эффективности принимаемых мер и соответствия системы защиты требованиям по обеспечению безопасности персональных данных установлено, что система защиты объекта информатизации «Облачное хранилище Selectel» соответствует требованиям к составу и содержанию мер по обеспечению безопасности персональных данных для 3-го уровня защищенности (УЗ-3) персональных данных, а также обеспечивает защиту от актуальных угроз безопасности.

7. Результаты оценки действуют в течение 3 (трех) лет. При изменении структурно-функциональных характеристик, актуальных угроз безопасности информации проводится повторная оценка.

8. Обеспечение безопасности и выполнение требований законодательства – совместная ответственность ООО «Селектел» и заказчика. Разграничение зон ответственности приведено в Приложении 1.

9. Перечень мер, реализованных для объекта информатизации «Облачное хранилище Selectel» приведен в Приложении 2.

Заместитель генерального директора
по разработке и эксплуатации продуктов М.П. С.А. Пимков

06 июня 2022 г.

Приложение 1

Разграничение зон ответственности

«Облачное хранилище Selectel»

Обеспечение безопасности и выполнение требований законодательства – совместная ответственность ООО «Селектел» и клиентов.

Разграничение ответственности между ООО «Селектел» и клиентами при использовании услуги «Облачное хранилище» реализуется следующим образом:

1. ООО «Селектел» отвечает за обеспечение информационной безопасности в отношении всей информационной инфраструктуры, используемой для предоставления услуги «Облачное хранилище», включая используемое программное обеспечение.

2. Клиент отвечает за управление доступом к обрабатываемым им данным в рамках использования услуги «Облачное хранилище», а именно за создание пользователей и предоставление прав доступа к контейнерам. Все стороннее программное обеспечение, эксплуатируемое клиентом по своему желанию в процессе использования услуги «Облачное хранилище» (такое как API-клиенты, CLI, SDK и иное) не является частью «Облачного хранилища Selectel» и находится в зоне ответственности клиента.

Схематично разграничение зон ответственности между ООО «Селектел» и клиентами представлено на схеме ниже:

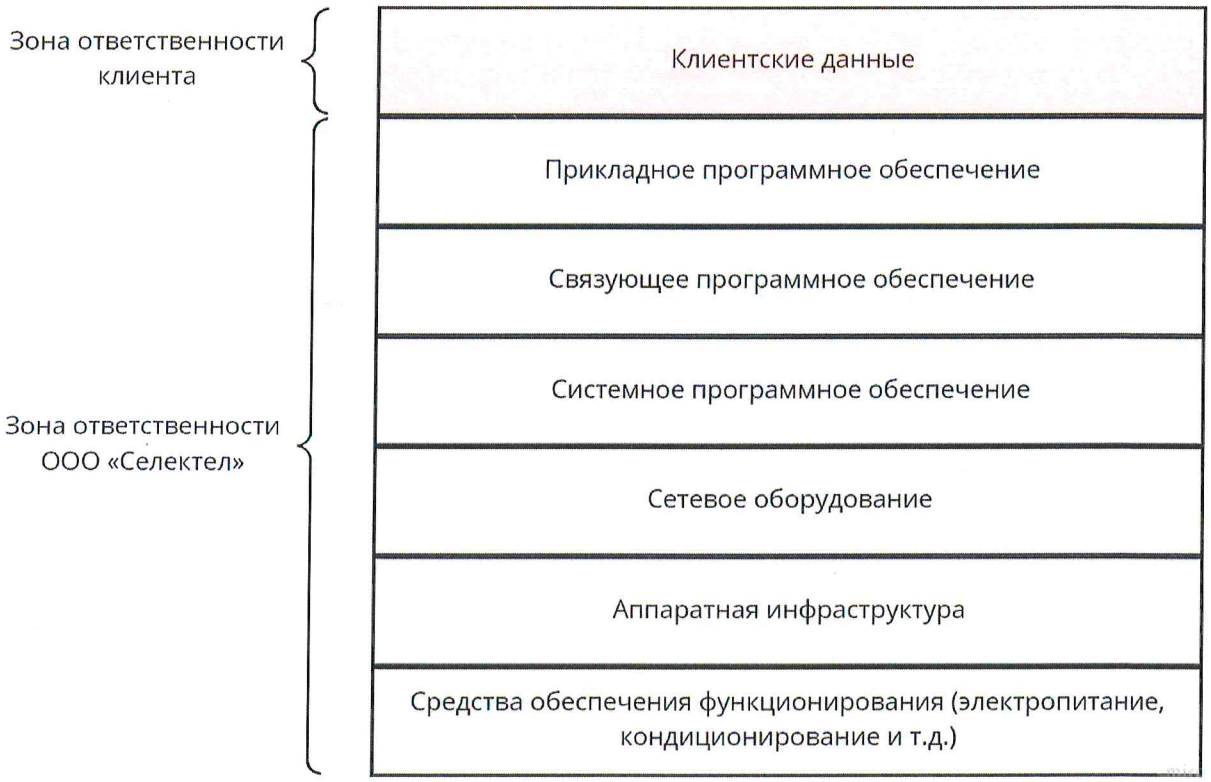

Рисунок 1 - Разграничение зон ответственности между ООО «Селектел» и клиентами

Приложение 2

Выполнение мер по защите информации

«Облачное хранилище Selectel»

Выполнение мер по защите информации, направленных на выполнение требований к составу и содержанию мер по обеспечению безопасности персональных данных для 3-го уровня защищенности (УЗ-3) персональных данных, а также на защиту от актуальных угроз безопасности, осуществляется за счет использования штатного функционала системного и прикладного программного обеспечения, средств защиты информации, а также организационных мер.

Клиент, с использованием функционала клиентской панели Selectel осуществляет управление учетными записями для доступа к контейнерам «Облачного хранилища», а также управление правами доступа.

В зону ответственности ООО «Селектел» входит реализация мер на уровне всей информационной инфраструктуры, используемой для предоставления услуги «Облачное хранилище», а именно:

- физическая безопасность технических устройств;
- сетевая безопасность;
- безопасность операционных систем и используемого программного обеспечения.

В таблице ниже представлена информация по реализуемым ООО «Селектел» мерам по защите информации.

Обозначение меры	Мера
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами объекта информатизации
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование объекта информатизации

Обозначение меры	Мера
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование объекта информатизации
УПД.6	Ограничение неуспешных попыток входа в объект информатизации (доступа к объекту информатизации)
УПД.10	Блокирование сеанса доступа в объект информатизации после установленного времени бездействия (неактивности) пользователя или по его запросу
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе
РСБ.7	Защита информации о событиях безопасности
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
АНЗ.1	Выявление, анализ уязвимостей объекта информатизации и оперативное устранение вновь выявленных уязвимостей
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации

Обозначение меры	Мера
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации
ОЦЛ.2	Контроль целостности персональных данных, содержащихся в базах данных информационной системы
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных
ОДТ.5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала
ЗТС.3	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 объекта информатизации, в помещения и сооружения, в которых они установлены
ЗИС.3	Обеспечение защиты информации 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
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию объекта информатизации и системы защиты информации
УКФ.2	Управление изменениями конфигурации объекта информатизации и системы защиты информации
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации объекта информатизации и системы защиты информации на обеспечение защиты информации и согласование изменений в конфигурации объекта информатизации с должностным лицом (работником), ответственным за обеспечение безопасности информации
УКФ.4	Документирование информации (данных) об изменениях в конфигурации объекта информатизации и системы защиты информации

Лист регистрации изменений

Номер редакции	Дата	Описание
1	06 июня 2022 г.	Исходный документ. Проведена оценка эффективности принимаемых мер.