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 «Облачная платформа Selectel»

Система защиты информации

Акт оценки эффективности принимаемых мер по обеспечению безопасности персональных данных

На 11 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 «Облачная платформа 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». В объем работ по оценке эффективности входят следующие инфраструктурные сервисы, предоставляющие ресурсы: **виртуальные машины, виртуальные диски, виртуальные сети**.

2. Технические средства располагаются на следующих территориальных площадках:
   - Регион **ru-1** – Ленинградская область, пгт. Дубровка, ул. Советская, д. 1;
   - Регион **ru-2** – Москва, ул. Берзарина, д. 36, стр. 3;
   - Регион **ru-3** – Санкт-Петербург, ул. Коли Томчака, д. 28, лит. К;
   - Регион **ru-7** – Москва, ул. Берзарина, д. 36, стр. 3;
   - Регион **ru-8** – Новосибирск, ул. Серебренниковская, д. 14, лит. А;
   - Регион **ru-9** – Ленинградская область, пгт. Дубровка, ул. Советская, д. 1.

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

4. Оценка эффективности принимаемых мер проведена в форме приемочных испытаний системы защиты объекта информатизации «Облачная платформа Selectel».

5. По результатам проведения оценки эффективности принимаемых мер и соответствия системы защиты требованиям по обеспечению безопасности персональных данных установлено, что система защиты объекта информатизации «Облачная платформа Selectel» соответствует требованиям к составу и содержанию мер по обеспечению безопасности персональных данных для 3-го уровня защищенности (УЗ-3) персональных данных.

6. Результаты оценки действуют в течение 3 (трех) лет.
   При изменении структурно-функциональных характеристик производится повторная оценка.

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

8. Перечень мер, реализованных для инфраструктуры «Облачной платформы Selectel» и мер, реализация которых позволит заказчику выполнить требования для 3-го уровня защищенности персональных данных, предъявляемых к его информационной системе, приведен в Приложении 2.

Заместитель генерального директора
по разработке и эксплуатации продуктов

М.П

«СЕТЬ ДАТА-ЦЕНТРОВ «СЕЛЕКТЕЛ» selectel.ru Selectel САНКТ-ПЕТЕРБУРГ ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ

С.А. Пимков

31 августа 2020 г.

Приложение 1

Разграничение зон ответственности в «Облачной платформе Selectel»

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

ООО «Селектел» отвечает за обеспечение безопасности и выполнение требований законодательства для вычислительной инфраструктуры, состоящей из набора инфраструктурных сервисов, предназначенной для размещения набора изолированных информационных систем заказчиков, в том числе информационных систем персональных данных с уровнем защищенности не более УЗ-3, в рамках оказания услуг, которая управляет и на которой функционирует «Облачная платформа Selectel».

Она включает в себя аппаратное и программное обеспечение вычислительной и сетевой инфраструктуры, среду виртуализации, средства управления, а также рабочие места сотрудников, с которых осуществляется управление.

Заказчик, размещающий изолированную информационную систему, является оператором персональных данных и отвечает за обеспечение безопасности и выполнение требований законодательства внутри размещаемой информационной системы, включая управление доступом, безопасность системного и прикладного программного обеспечения, функционирующего внутри виртуальных машин, резервное копирование, сетевое взаимодействие и обеспечение сетевой безопасности.

Разделение зон ответственности приведено ниже.

Область	**Ответственность**
Данные и резервное копирование	Заказчик
Операционная система и прикладное ПО	Заказчик
Сеть внутри Проекта	Заказчик
Управление доступом к Проекту и его ресурсам	Заказчик
Технологическая сеть	ООО «Селектел»
Среда виртуализации	ООО «Селектел»
Аппаратное обеспечение	ООО «Селектел»
Рабочие места сотрудников ООО «Селектел»	ООО «Селектел»
Безопасность дата-центров	ООО «Селектел»

Приложение 2

Реализация мер Приказа ФСТЭК России № 21 в «Облачной платформе Selectel»

Реализация мер выполняется с помощью компонентов инфраструктуры, реализующих функции безопасности, на всех уровнях инфраструктуры, находящихся в зоне ответственности ООО «Селектел», приведенных в Приложении 1.

Реализация мер заказчиком в виртуальной инфраструктуре, находящейся в его зоне ответственности, приведенной в Приложении 1, может осуществляться как на уровне Проекта в целом, так и на уровне отдельных его компонентов.

Реализация мер приведена ниже.

Мера	ООО «Селектел»	Заказчик
ИАФ.1 Идентификация и аутентификация пользователей, являющихся работниками	Реализуется для физической и виртуальной инфраструктуры, средств управления, рабочих мест	Необходимо реализовать для Проекта и входящих в него ресурсов
ИАФ.3 Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	Реализуется для физической и виртуальной инфраструктуры, средств управления, рабочих мест	Необходимо реализовать для Проекта и входящих в него ресурсов
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	Реализуется для физической и виртуальной инфраструктуры, средств управления, рабочих мест	Необходимо реализовать для Проекта и входящих в него ресурсов
ИАФ.5 Защита обратной связи при вводе аутентификационной информации	Реализуется для физической и виртуальной инфраструктуры, средств управления, рабочих мест	Необходимо реализовать для Проекта и входящих в него ресурсов

УПД.1 Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	Реализуется для физической и виртуальной инфраструктуры, средств управления, рабочих мест	Необходимо реализовать для Проекта и входящих в него ресурсов
УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	Реализуется для физической и виртуальной инфраструктуры, средств управления, рабочих мест	Необходимо реализовать для Проекта и входящих в него ресурсов
УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами объекта информатизации	Реализуется для физической и виртуальной инфраструктуры, средств управления, рабочих мест	Необходимо реализовать для Проекта и входящих в него ресурсов
УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование объекта информатизации	Реализуется для физической и виртуальной инфраструктуры, средств управления, рабочих мест	Необходимо реализовать для Проекта и входящих в него ресурсов
УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование объекта информатизации	Реализуется для физической и виртуальной инфраструктуры, средств управления, рабочих мест	Необходимо реализовать для Проекта и входящих в него ресурсов
УПД.6 Ограничение неуспешных попыток входа в объект информатизации (доступа к объекту информатизации)	Реализуется для физической и виртуальной инфраструктуры, средств управления, рабочих мест	Необходимо реализовать для Проекта и входящих в него ресурсов
УПД.10 Блокирование сеанса доступа в объект информатизации после установленного времени бездействия (неактивности) пользователя или по его запросу	Реализуется для физической и виртуальной инфраструктуры, средств управления, рабочих мест	Необходимо реализовать для Проекта и входящих в него ресурсов

УПД.11 Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	Реализуется для физической и виртуальной инфраструктуры, средств управления, рабочих мест	Необходимо реализовать для Проекта и входящих в него ресурсов
УПД.13 Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	Для административного доступа используются выделенные защищенные каналы связи	Необходимо реализовать для Проекта и входящих в него ресурсов
УПД.14 Регламентация и контроль использования технологий беспроводного доступа	Реализуется для рабочих мест	Неприменимо
УПД.15 Регламентация и контроль использования мобильных технических средств	К мобильным техническим средствам относятся, в том числе, ноутбуки и съемные носители информации В физической и виртуальной инфраструктуре, средствах управления мобильные технические средства не используются Реализуется для рабочих мест	Неприменимо
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	Реализуется для виртуальной инфраструктуры Осуществляется их физическое уничтожение дисков.	Необходимо реализовать для Проекта и входящих в него ресурсов
РСБ.1 Определение событий безопасности, подлежащих регистрации, и сроков их хранения	Реализуется для физической и виртуальной инфраструктуры, средств управления, рабочих мест	Необходимо реализовать для Проекта и входящих в него ресурсов

РСБ.2 Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	Реализуется для физической и виртуальной инфраструктуры, средств управления, рабочих мест	Необходимо реализовать для Проекта и входящих в него ресурсов
РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	Реализуется для физической и виртуальной инфраструктуры, средств управления, рабочих мест	Необходимо реализовать для Проекта и входящих в него ресурсов
РСБ.7 Защита информации о событиях безопасности	Реализуется для физической и виртуальной инфраструктуры, средств управления, рабочих мест	Необходимо реализовать для Проекта и входящих в него ресурсов
АВЗ.1 Реализация антивирусной защиты	Реализуется для рабочих мест	Необходимо реализовать для Проекта и входящих в него ресурсов
АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	Реализуется для рабочих мест	Необходимо реализовать для Проекта и входящих в него ресурсов
АНЗ.1 Выявление, анализ уязвимостей объекта информатизации и оперативное устранение вновь выявленных уязвимостей	Осуществляется сканирование образов, пакетов и зависимостей на наличие уязвимостей; сканирование инфраструктуры для обнаружения несанкционированных опубликованных служб	Необходимо реализовать для Проекта и входящих в него ресурсов
АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	Реализуется для физической и виртуальной инфраструктуры, средств управления, рабочих мест	Необходимо реализовать для Проекта и входящих в него ресурсов

АН3.3 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	Реализуется для физической и виртуальной инфраструктуры, средств управления, рабочих мест	Необходимо реализовать для Проекта и входящих в него ресурсов
АН3.4 Контроль состава технических средств, программного обеспечения и средств защиты информации	Реализуется для физической и виртуальной инфраструктуры, средств управления, рабочих мест	Необходимо реализовать для Проекта и входящих в него ресурсов
ЗСВ.1 Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	Реализуется для виртуальной инфраструктуры и средств управления	Необходимо реализовать для Проекта и входящих в него ресурсов
ЗСВ.2 Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	Реализуется для виртуальной инфраструктуры и средств управления	Необходимо реализовать для Проекта и входящих в него ресурсов
ЗСВ.3 Регистрация событий безопасности в виртуальной инфраструктуре	Реализуется для виртуальной инфраструктуры и средств управления	Необходимо реализовать для Проекта и входящих в него ресурсов
ЗСВ.10 Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей	Реализуется для виртуальной инфраструктуры и средств управления	Необходимо реализовать для Проекта и входящих в него ресурсов
ЗТС.2 Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования	Реализуется для центров обработки данных, физической инфраструктуры, рабочих мест	Неприменимо

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	Реализуется для центров обработки данных, физической инфраструктуры, рабочих мест	Неприменимо
ЗТС.4 Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	Реализуется для рабочих мест	Неприменимо
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	Для административного доступа используются выделенные защищенные каналы связи	Необходимо реализовать для Проекта и входящих в него ресурсов
ЗИС.20 Защита беспроводных соединений, применяемых в объекте информатизации	Реализуется для рабочих мест Реализация беспроводных соединений возможна только через контролируемые интерфейсы	Неприменимо
ЗИС.22 Защита от угроз безопасности информации, направленных на отказ в обслуживании	Реализуется сервисами и средствами защиты информации	Возможно реализовать для Проекта и входящих в него ресурсов
УКФ.1 Определение лиц, которым разрешены действия по внесению изменений в конфигурацию объекта информатизации и системы защиты информации	Реализуется для физической и виртуальной инфраструктуры, средств управления, рабочих мест	Необходимо реализовать для Проекта и входящих в него ресурсов

УКФ.2 Управление изменениями конфигурации объекта информатизации и системы защиты информации	Реализуется для физической и виртуальной инфраструктуры, средств управления, рабочих мест	Необходимо реализовать для Проекта и входящих в него ресурсов
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	Реализуется для физической и виртуальной инфраструктуры, средств управления, рабочих мест	Необходимо реализовать для Проекта и входящих в него ресурсов
УКФ.4 Документирование информации (данных) об изменениях в конфигурации объекта информатизации и системы защиты информации	Реализуется для физической и виртуальной инфраструктуры, средств управления, рабочих мест	Необходимо реализовать для Проекта и входящих в него ресурсов

Лист регистрации изменений

Номер редакции	Дата	Описание
1	31 августа 2020 г.	Исходный документ. Проведена оценка эффективности принимаемых мер.