



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

Е-MAIL office@selectel.ru

САЙТ selectel.ru

Информационная система «Облачная платформа Selectel»

Акт оценки эффективности принимаемых мер по обеспечению безопасности персональных данных для 1-го уровня защищенности

1. ООО «Селектел» проведена оценка эффективности принимаемых мер и соответствия системы защиты информационной системы «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».
2. Информационная система «Облачная платформа Selectel» включает следующие сервисы:
 - Группа услуг «Облачная платформа», включая:
 - Виртуальные машины, Виртуальные диски, Виртуальные сети;
 - Бэкапы
 - Кластер Kubernetes;
 - Кластер базы данных;
 - Отказоустойчивый балансировщик нагрузки;
 - Реестр контейнеров;
 - Облачное объектное хранилище.
3. Технические средства информационной системы «Облачная платформа Selectel» располагаются на следующих территориальных площадках:
 - Санкт-Петербург, ул. Цветочная, д. 21, лит. А;
 - Санкт-Петербург, ул. Коли Томчака, д. 28, лит. К, помещение 1-Н;
 - Ленинградская обл., Всеволожский р-н, пгт Дубровка, ул. Советская, д 1, лит. А;
 - Ленинградская обл., Всеволожский р-н, пгт Дубровка, ул. Советская, д 1, лит. Б;
 - Ленинградская обл., Всеволожский р-н, пгт Дубровка, ул. Советская, уч. 1/1, лит. И;
 - Москва, ул. Берзарина, д. 36, стр. 3;
 - Новосибирск, ул. Серебренниковская, д. 14, лит. А.
4. Оценка эффективности принимаемых мер проведена в форме приемочных испытаний системы защиты информационной системы «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 информационной системы «Облачная платформа Selectel» соответствует требованиям к составу и содержанию мер по обеспечению безопасности персональных данных для 1-го уровня защищенности (УЗ-1) персональных данных, а также обеспечивает защиту от актуальных угроз безопасности информации.
6. Результаты оценки действуют в течение 3 (трех) лет. При изменении структурно-функциональных характеристик информационной системы «Облачная платформа Selectel», условий ее эксплуатации, изменения требований, на соответствие которым проводилась оценка, появлении новых актуальных угроз безопасности информации проводится повторная оценка.
7. Обеспечение безопасности информации, обрабатываемой с использованием информационной системы «Облачная платформа Selectel» и размещаемых на ее базе информационных систем, выполнение требований законодательства – совместная ответственность ООО «Селектел» и клиентов. Разграничение зон ответственности приведено в Приложении 1.

8. Перечень мер, на соответствие которым проводилась оценка, приведен в Приложении 2. Также указанное приложение содержит сведения о мерах, которые необходимо реализовать в клиентских информационных системах, размещаемых на базе информационной системы «Облачная платформа Selectel», для обеспечения безопасности персональных данных 1-го уровня защищенности (УЗ-1).

Заместитель генерального директора по разработке и эксплуатации продуктов



С.А. Пимков

30 декабря 2022 г.

Разграничение зон ответственности в части обеспечения безопасности

Информационная система «Облачная платформа Selectel»

Информационная система «Облачная платформа Selectel» представляет собой распределенную вычислительную инфраструктуру, состоящую из набора инфраструктурных сервисов, предназначенную для размещения на ее базе клиентских информационных систем, в том числе информационных систем персональных данных. до 1-го уровня защищенности (УЗ-1) включительно.

Обеспечение безопасности информации, обрабатываемой с использованием информационной системы «Облачная платформа Selectel» и размещаемых на ее базе информационных систем клиентов, а также выполнение требований законодательства – совместная ответственность ООО «Селектел» и клиентов.

Разграничение ответственности между ООО «Селектел» и клиентами при пользовании сервисами, указанными в п. 2, реализуется следующим образом:

1. ООО «Селектел» в общем случае отвечает за обеспечение информационной безопасности служебной инфраструктуры информационной системы «Облачная платформа Selectel» - обеспечивает физическую безопасность и отказоустойчивость оборудования, сетевую безопасность служебных сетей, безопасность платформы виртуализации и служебных серверов.
2. Клиент отвечает за обеспечение информационной безопасности размещаемых на базе информационной системы «Облачная платформа Selectel» собственных информационных систем - обеспечивает безопасность виртуальных серверов (включая операционные системы и приложения), сетевую безопасность клиентских сетей, организует управление доступом к обрабатываемым данным.
3. В зависимости от инфраструктурных особенностей отдельных сервисов и условий их предоставления за обеспечение безопасности:
 - master-нод и служебной сети кластера Kubernetes при использовании сервиса Managed Kubernetes отвечает ООО «Селектел», worker-нод - клиент;
 - нод и служебной сети кластера баз данных при использовании сервиса Облачные базы данных отвечает ООО «Селектел».

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

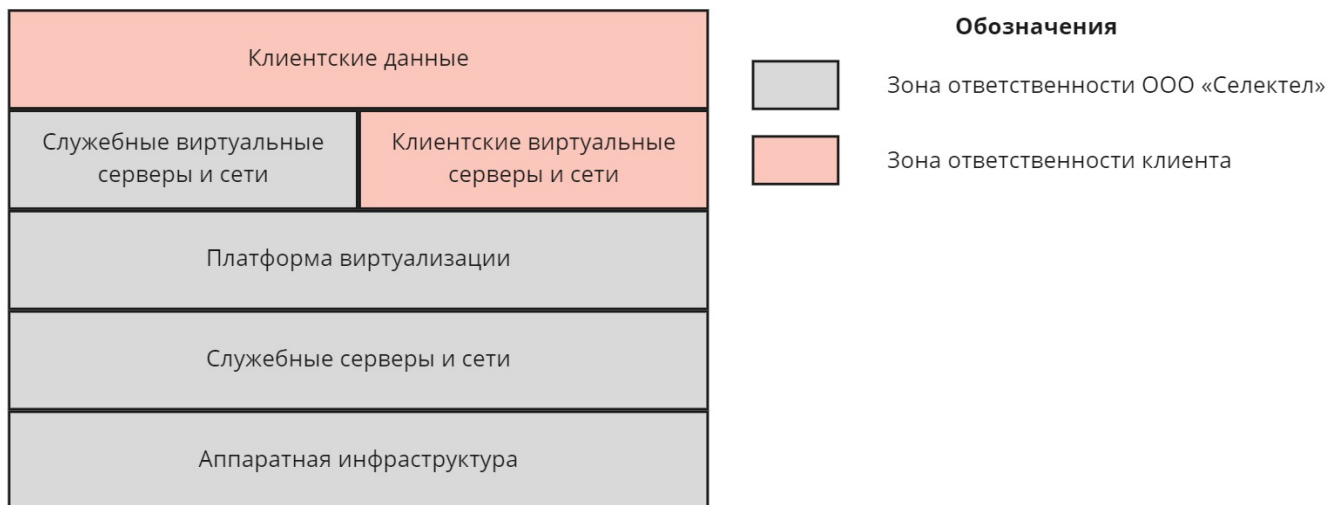


Рисунок 1 - Разграничение зон ответственности между ООО «Селектел» и клиентом

Выполнение мер по обеспечению безопасности информации

Информационная система «Облачная платформа Selectel»

Выполнение мер, необходимых для обеспечения безопасности персональных данных 1-го уровня защищенности (УЗ-1), а также для защиты от актуальных угроз безопасности, осуществляется за счет использования штатного функционала системного и прикладного программного обеспечения, входящего в состав информационной системы «Облачная платформа Selectel», а также применяемых средств защиты информации и комплекса организационных мер.

Перечень реализуемых ООО «Селектел» мер, сформированный с учетом требований Приказа ФСТЭК России № 21 от 18.02.2013 и Постановления Правительства РФ от 01.11.2012 № 1119, приведен в таблице ниже. Кроме того, указанная таблица содержит перечень мер, которые необходимо реализовать в клиентских информационных системах, размещаемых на базе информационной системы «Облачная платформа Selectel», для обеспечения безопасности персональных данных 1-го уровня защищенности (УЗ-1).

Обозначение меры	Описание меры	Реализация ООО «Селектел»	Реализация клиентом
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками	Реализуется на уровне сетевого оборудования, служебных серверов и платформы виртуализации (далее при совместном упоминании - служебная инфраструктура)	Необходимо реализовать на уровне клиентских виртуальных серверов, приложений, функционирующих на базе кластера Kubernetes (далее при совместном упоминании - клиентские серверы и приложения)
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	Реализуется на уровне технических средств	Не применимо, т.к. технические средства не входят в зону ответственности клиента
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов и приложений
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 на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов и приложений
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов и приложений
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	Не применимо, т.к. внешние пользователи служебной инфраструктуры отсутствуют	Необходимо реализовать на уровне клиентских серверов и приложений

Обозначение меры	Описание меры	Реализация ООО «Селектел»	Реализация клиентом
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов и приложений
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов и приложений
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами объекта информатизации	Реализуется для служебных сетей	Необходимо реализовать для клиентских сетей
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование объекта информатизации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов и приложений
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование объекта информатизации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов и приложений
УПД.6	Ограничение неуспешных попыток входа в объект информатизации (доступа к объекту информатизации)	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов и приложений

Обозначение меры	Описание меры	Реализация ООО «Селектел»	Реализация клиентом
УПД.10	Блокирование сеанса доступа в объект информатизации после установленного времени бездействия (неактивности) пользователя или по его запросу	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов и приложений
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов и приложений
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов и приложений
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	Не применимо, т.к. технология не используется	Не применимо, т.к. технология не используется
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	Не применимо, т.к. технология не используется	Не применимо, т.к. технология не используется
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов и приложений
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники	Реализуется на уровне технических средств	Не применимо, т.к. технические средства не входят в зону ответственности клиента

Обозначение меры	Описание меры	Реализация ООО «Селектел»	Реализация клиентом
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения	Реализуется на уровне служебных серверов и платформы виртуализации	Необходимо реализовать на уровне виртуальных серверов
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	Реализуется на уровне служебных серверов и платформы виртуализации	Необходимо реализовать на уровне виртуальных серверов
ЗНИ.1	Учет машинных носителей персональных данных	Реализуется на уровне технических средств	Не применимо, т.к. технические средства не входят в зону ответственности клиента
ЗНИ.2	Управление доступом к машинным носителям персональных данных	Реализуется на уровне технических средств	Не применимо, т.к. технические средства не входят в зону ответственности клиента
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 на уровне технических средств	Не применимо, т.к. технические средства не входят в зону ответственности клиента
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов и приложений

Обозначение меры	Описание меры	Реализация ООО «Селектел»	Реализация клиентом
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов и приложений
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов и приложений
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов и приложений
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов и приложений
РСБ.7	Защита информации о событиях безопасности	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов и приложений
АВЗ.1	Реализация антивирусной защиты	Реализуется на уровне служебных серверов	Необходимо реализовать на уровне клиентских серверов и приложений
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	Реализуется на уровне служебных серверов	Необходимо реализовать на уровне клиентских серверов и приложений
СОВ.1	Обнаружение вторжений	Реализуется на уровне служебной сети и служебных серверов	Необходимо реализовать на уровне клиентских сетей и/или виртуальных серверов

Обозначение меры	Описание меры	Реализация ООО «Селектел»	Реализация клиентом
СОВ.2	Обновление базы решающих правил	Реализуется на уровне служебной сети и служебных серверов	Необходимо реализовать на уровне клиентских сетей и/или виртуальных серверов
АНЗ.1	Выявление, анализ уязвимостей объекта информатизации и оперативное устранение вновь выявленных уязвимостей	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов и приложений
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов

Обозначение меры	Описание меры	Реализация ООО «Селектел»	Реализация клиентом
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)	Не применимо, т.к. технология не используется	Необходимо реализовать на уровне клиентских серверов и приложений
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование	Реализуется на уровне технических средств	Не применимо, т.к. технические средства не входят в зону ответственности клиента
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных	Реализуется на уровне служебных серверов и платформы виртуализации Также реализуется на уровне нод Облачных баз данных и системы хранения в составе Объектного хранилища	Необходимо реализовать на уровне клиентских серверов и приложений
ОДТ.5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала	Реализуется на уровне служебных серверов и платформы виртуализации Также реализуется на уровне нод Облачных баз данных и системы хранения в составе Объектного хранилища	Необходимо реализовать на уровне клиентских серверов и приложений
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	Реализуется на уровне служебных серверов и платформы виртуализации	Необходимо реализовать на уровне клиентских серверов и приложений

Обозначение меры	Описание меры	Реализация ООО «Селектел»	Реализация клиентом
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	Реализуется на уровне служебных серверов и платформы виртуализации	Необходимо реализовать на уровне клиентских серверов и приложений
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре	Реализуется на уровне служебных серверов и платформы виртуализации	Необходимо реализовать на уровне клиентских серверов и приложений
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	Реализуется на уровне платформы виртуализации	Необходимо реализовать на уровне клиентских серверов и приложений
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций	Реализуется на уровне служебных серверов и платформы виртуализации	Необходимо реализовать на уровне клиентских серверов и приложений
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры	Реализуется на уровне служебных серверов и платформы виртуализации Также реализуется на уровне нод Облачных баз данных и системы хранения в составе Объектного хранилища	Необходимо реализовать на уровне клиентских серверов и приложений
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	Реализуется на уровне служебных серверов и платформы виртуализации	Необходимо реализовать на уровне клиентских серверов
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей	Реализуется на уровне служебной сети	Необходимо реализовать на уровне клиентских сетей

Обозначение меры	Описание меры	Реализация ООО «Селектел»	Реализация клиентом
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, исключая 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 на уровне технических средств	Не применимо, т.к. технические средства не входят в зону ответственности клиента
ЗТС.4	Размещение устройств вывода (отображения) информации, исключая ее несанкционированный просмотр	Не применимо, т.к. устройства вывода не входят в состав информационной системы	Не применимо, т.к. устройства вывода не входят в состав информационной системы
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов и приложений
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	Реализуется на уровне служебной сети	Необходимо реализовать на уровне клиентских сетей

Обозначение меры	Описание меры	Реализация ООО «Селектел»	Реализация клиентом
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов	Реализуется на уровне служебной сети	Необходимо реализовать на уровне клиентских сетей
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов и приложений
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе	Не применимо, т.к.технология не используется	Не применимо, т.к.технология не используется
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них	Реализуется в отношении инцидентов, возникающих на уровне дата-центра, служебных сетей и инфраструктуры	Необходимо реализовать в отношении инцидентов, возникающих на уровне клиентских серверов, приложений и данных
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов	Реализуется в отношении инцидентов, возникающих на уровне дата-центра, служебных сетей и инфраструктуры	Необходимо реализовать в отношении инцидентов, возникающих на уровне клиентских серверов, приложений и данных

Обозначение меры	Описание меры	Реализация ООО «Селектел»	Реализация клиентом
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами	Реализуется в отношении инцидентов, возникающих на уровне дата-центра, служебных сетей и инфраструктуры	Необходимо реализовать в отношении инцидентов, возникающих на уровне клиентских серверов, приложений и данных
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий	Реализуется в отношении инцидентов, возникающих на уровне дата-центра, служебных сетей и инфраструктуры	Необходимо реализовать в отношении инцидентов, возникающих на уровне клиентских серверов, приложений и данных
ИНЦ.5	Принятие мер по устранению последствий инцидентов	Реализуется в отношении инцидентов, возникающих на уровне дата-центра, служебных сетей и инфраструктуры	Необходимо реализовать в отношении инцидентов, возникающих на уровне клиентских серверов, приложений и данных
ИНЦ.6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов	Реализуется в отношении инцидентов, возникающих на уровне дата-центра, служебных сетей и инфраструктуры	Необходимо реализовать в отношении инцидентов, возникающих на уровне клиентских серверов, приложений и данных
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию объекта информатизации и системы защиты информации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов
УКФ.2	Управление изменениями конфигурации объекта информатизации и системы защиты информации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов

Обозначение меры	Описание меры	Реализация ООО «Селектел»	Реализация клиентом
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 на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов
УКФ.4	Документирование информации (данных) об изменениях в конфигурации объекта информатизации и системы защиты информации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских серверов

Лист регистрации изменений

Номер редакции	Дата	Описание
1	30 декабря 2022 г.	Исходный документ