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

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

ИНН / ОГРН 7810962785 / 1247800067790

E-MAIL office@selectel.ru

САЙТ selectel.ru

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

На 20 страницах

1. АО «Селектел» (Лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации № Л024-00107-00/00583397 от 20 февраля 2018 г.) проведена оценка эффективности принимаемых мер и соответствия системы защиты вычислительной инфраструктуры центра обработки данных 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 компоненты информационной инфраструктуры АО «Селектел», используемые для предоставления следующих продуктов и услуг (далее - Инфраструктура):
   - Выделенные серверы, Сетевые диски для выделенных серверов;
   - Выделенная СХД, Предоставление LUN СХД;
   - Облачная платформа:
     - Облачные серверы;
     - Резервное копирование в облаке (Бэкапы);
     - Файловое хранилище Selectel;
   - Облачные базы данных (Managed Databases, DBaaS);
   - Объектное хранилище (S3);
   - Кластер Kubernetes (Managed Kubernetes);
   - Реестр контейнеров (Container Registry);
   - Размещение оборудования (Colocation), Серверный шкаф;
   - Глобальный роутер Selectel;
   - Сетевое оборудование.

3. Технические средства Инфраструктуры располагаются на следующих территориальных площадках:
   - г. Санкт-Петербург, улица Коли Томчака, дом 28, литера К;
   - г. Санкт-Петербург, улица Цветочная, д. 21, лит. А;
   - 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;
   - г. Москва, ул. Берзарина, д. 36, стр. 3;
   - г. Москва, ул. Авиамоторная, д. 69;
   - г. Москва, пр-д Юрловский, владение 18;
   - г. Москва, ул. Рябиновая, д. 53, стр. 4;
   - г. Москва, пл. Академика Курчатова, д. 1, стр. 301;
   - г. Москва, Алтуфьевское ш., д. 33Г, здания 1 и 2;
   - Новосибирский район, д.п. Кудряшовский, ул. Светлая, д. 21.

4. Для Инфраструктуры 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 инфраструктуры.

6. По результатам проведения оценки эффективности принимаемых мер и соответствия системы защиты требованиям по обеспечению безопасности персональных данных установлено, что система защиты Инфраструктуры 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.

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

8. Обеспечение безопасности информации, обрабатываемой в Инфраструктуре, и размещаемых на ее базе информационных систем, выполнение требований законодательства – совместная ответственность АО «Селектел» и Заказчика. Разграничение зон ответственности приведено в Приложении 1 к настоящему акту.

9. Перечень мер, на соответствие которым проводилась оценка, приведен в Приложении 2. Данное приложение также содержит базовый набор мер, по обеспечению безопасности персональных данных для 1-го уровня защищенности.

Заместитель генерального директора
по разработке и эксплуатации продуктов

М.П

С.А. Пимков

30 декабря 2025 г.

**Приложение 1**

**Разграничение зон ответственности**

Selectel обеспечивает защиту служебной инфраструктуры продуктов и услуги, а Заказчик — защиту инфраструктуры, развернутой с использованием продуктов и услуг Selectel. Границы зоны ответственности могут отличаться в зависимости для различных продуктов и услуг.

Для всех продуктов и услуг, попадающих в область оценки, Selectel обеспечивает физическую безопасность технических средств, а также функционирование инженерных систем, включая системы электропитания и заземление, соблюдение температурного режима (вентиляцию и кондиционирование), систем видеонаблюдения, контроля физического доступа. В свою очередь в зону ответственности Заказчика входит обеспечение безопасности обрабатываемых данных, включая управление доступом к данным и ресурсам их обрабатывающим.

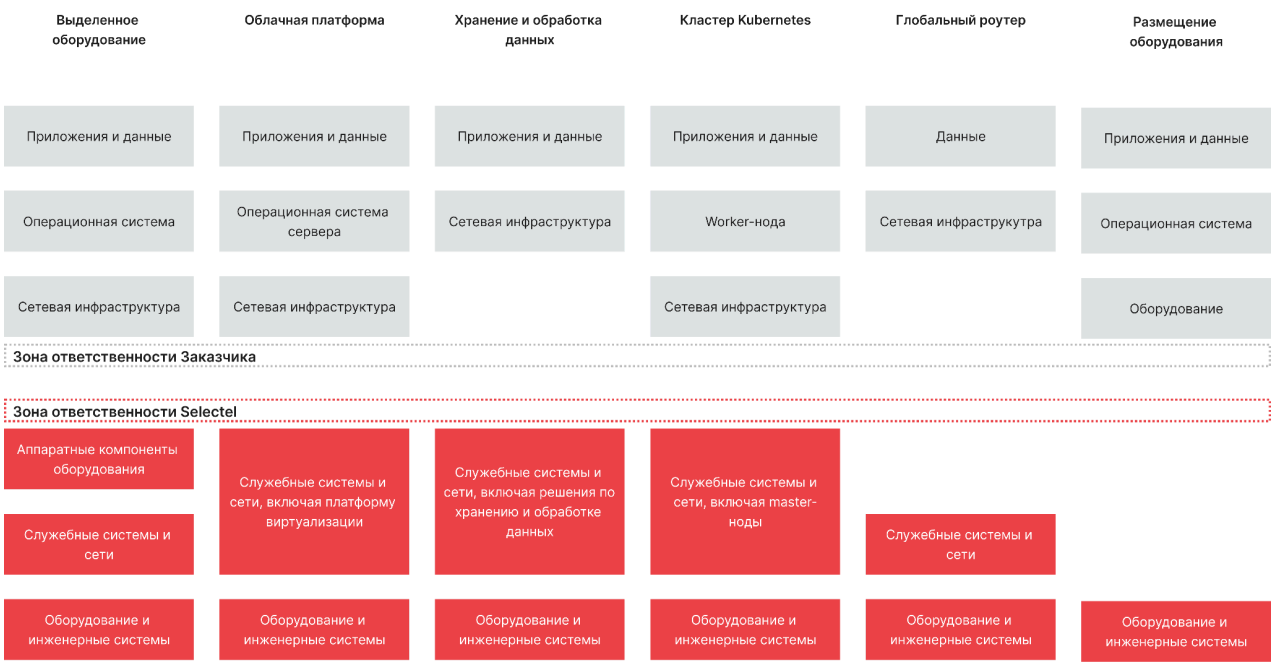
**Выделенные серверы, Сетевое оборудование, Выделенная СХД**. Selectel отвечает за безопасность служебных систем и сетей, а в отношении предоставляемого оборудования - за безопасность аппаратных компонентов. Заказчик отвечает за безопасность системного и прикладного программного обеспечения на оборудовании, безопасность сетевой инфраструктуры Заказчика, а также за безопасность обрабатываемых данных, включая управление доступом к ним.

**Облачная платформа**. Selectel отвечает за безопасность служебных систем и сетей, включая платформу виртуализации, решения, реализующее резервное копирование информации, хранение и обработку данных. Заказчик отвечает за безопасность системного и прикладного программного обеспечения, используемого на Облачных серверах, включая создание и управление резервными копиями, безопасность сетевой инфраструктуры Заказчика, а также за безопасность обрабатываемых данных, включая управление доступом к ним.

**Сетевые диски для выделенных серверов, Предоставление LUN СХД, Облачные базы данных (Managed Databases, DBaaS), Объектное хранилище (S3), Реестр контейнеров (Container Registry)**. Selectel отвечает за безопасность служебных систем и сетей, включая решения, реализующие хранение и обработку данных. Заказчик отвечает за безопасность сетевой инфраструктуры Заказчика, а также за безопасность обрабатываемых данных, включая управление доступом к ним.

**Кластер Kubernetes (Managed Kubernetes)**. Selectel отвечает за безопасность служебных систем и сетей, включая master-нод и служебной сети кластера Kubernetes. Заказчик отвечает за безопасность worker-нод, сетевой инфраструктуры Заказчика, а также за безопасность обрабатываемых данных, включая управление доступом к ним.

**Глобальный роутер**. Selectel отвечает за безопасность служебных систем и сетей, включая решение, непосредственно реализующие сетевую связность между разными продуктами и услугами Заказчика. Заказчик отвечает за безопасность сетевой инфраструктуры Заказчика, а также за безопасность обрабатываемых данных, включая управление доступом к ним.




Дополнительная информация по обеспечению безопасности при использовании продуктов и услуг Selectel представлена на сайте Selectel в разделе “Безопасность в Selectel” https://selectel.ru/about/security/ и в соответствующем разделе документации https://docs.selectel.ru/information-security/

**Приложение 2**

**Выполнение мер по защите информации**

Меры по защите информации, на соответствие которым проводилась оценка, выбраны с учетом требований Приказа ФСТЭК России № 21. В основе находится базовый состав мер, необходимый для обеспечения 1-го уровня защищенности (УЗ-1) персональных данных, который адаптирован, уточнен и дополнен с учетом:

- стека технологий, используемых в составе инфраструктуры продуктов и услуг Selectel;
- угроз безопасности, определенных в качестве актуальных;
- требований иных применимых требований в области защиты персональных данных.

Выполнение выбранных мер по защите информации осуществляется за счет использования Selectel штатного функционала системного и прикладного программного обеспечения, применения средств защиты информации, а также реализации организационных мер и внедрения соответствующих процессов.

Selectel реализует меры в соответствии с учетом разграничения зон ответственности, то есть в отношении инфраструктуры, используемой для предоставления продуктов и услуг. При этом меры в отношении ресурсов Заказчика, таких как выделенные серверы, виртуальные серверы, сетевая инфраструктура, образы контейнеров и обрабатываемых с их помощью данных должны быть выполнены Заказчиком. Для их реализации в числе прочего могут использоваться сервисы и решения, предоставляемые Selectel, информация о которых доступна на сайте https://selectel.ru/services/is/ и в соответствующем разделе документации https://docs.selectel.ru/security-guide/.

Итоговый перечень мер, реализуемый Заказчиком в отношении защищаемых им информационных систем, может отличаться от представленного в таблице ниже, с учетом его адаптации, уточнения и дополнения.

В зону ответственности АО «Селектел» входит реализация мер на уровне инфраструктурных компонентов на базе которых реализованы услуги:

- Размещение оборудования (Colocation), Серверный шкаф - физическая безопасность;
- Выделенные серверы, Сетевые диски для выделенных серверов, Сетевое оборудование, Выделенная СХД, Предоставление LUN СХД - физическая безопасность, безопасность аппаратных средств, сетевая безопасность служебной инфраструктуры;
- Облачная платформа (включая Облачные серверы, Резервное копирование в облаке (Бэкапы), Файловое хранилище Selectel) - физическая безопасность, безопасность аппаратных средств, сетевая безопасность служебной инфраструктуры и безопасность платформы виртуализации;
- Кластер Kubernetes (Managed Kubernetes) и Реестр контейнеров (Container Registry) - физическая безопасность, безопасность аппаратных средств, сетевая безопасность служебной инфраструктуры, безопасность платформы оркестрации и безопасность ОС;
- Облачные базы данных (Managed Databases, DBaaS) и Объектное хранилище (S3) - физическая безопасность, безопасность аппаратных средств, сетевая безопасность, безопасность платформы виртуализации оркестрации и безопасность ОС и прикладного ПО;

- Глобальный роутер - физическая безопасность, безопасность аппаратных средств, сетевая безопасность.

В зону ответственности заказчика входит обеспечение безопасности данных и управление доступом, а также для услуг:

- Размещение оборудования (Colocation), Серверный шкаф - безопасность аппаратных средств, сетей, ОС и прикладного ПО;
- Выделенные серверы, Сетевые диски для выделенных серверов, Сетевое оборудование, Выделенная СХД, Предоставление LUN СХД - безопасность ОС и прикладного ПО, клиентских сетей (безопасность сетевого оборудования, в случае если клиент берет его в аренду);
- Облачная платформа (включая Облачные серверы, Резервное копирование в облаке (Бэкапы), Файловое хранилище Selectel) - безопасность ОС и прикладного ПО, клиентских сетей;
- Кластер Kubernetes (Managed Kubernetes) и Реестр контейнеров (Container Registry) - безопасность сетей клиента и прикладного ПО.

В таблице ниже представлена информация о составе мер по обеспечению безопасности персональных данных, реализованных в зоне ответственности АО «Селектел». Заказчику также необходимо реализовать приведенные меры[1] в своей зоне ответственности (далее - ЗО заказчика) для обеспечения 1-го уровня защищенности персональных данных.

[1] В таблице приведен базовый состав мер для 1-го уровня защищенности персональных данных. Он может быть адаптирован, уточнен и дополнен с учетом особенностей информационной системы Заказчика

| Обозначение меры | Мера | АО «Селектел» | Заказчик |
|---|---|---|---|
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками | Реализуется на уровне служебных систем и сетей, используемых для предоставления продуктов и услуг (далее - Служебная инфраструктура) | Необходимо реализовать на уровне выделенного оборудования, клиентских серверов, виртуальных серверов, приложений, функционирующих на базе инфраструктуры продуктов и услуг Selectel (далее - Инфраструктура Заказчика) |
| ИАФ.2 | Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных | Реализуется на уровне технических средств | Необходимо реализовать на уровне используемого Заказчиком выделенного оборудования |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов | Реализуется на уровне Служебной инфраструктуры | Необходимо реализовать на уровне Инфраструктуры Заказчика |
| 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 Инфраструктуры Заказчика |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации | Реализуется на уровне Служебной инфраструктуры | Необходимо реализовать на уровне Инфраструктуры Заказчика |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) | Реализуется на уровне Служебной инфраструктуры | Необходимо реализовать на уровне Инфраструктуры Заказчика |

| Обозначение меры | Мера | АО «Селектел» | Заказчик |
|---|---|---|---|
| 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 Инфраструктуры Заказчика |
| 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 Инфраструктуры Заказчика |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами объекта информатизации | Реализуется на уровне служебных сетей | Необходимо реализовать для сетей Заказчика, функционирующих на базе инфраструктуры продуктов и услуг Selectel |
| УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование объекта информатизации | Реализуется на уровне Служебной инфраструктуры | Необходимо реализовать на уровне Инфраструктуры Заказчика |
| 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 Инфраструктуры Заказчика |

| Обозначение меры | Мера | АО «Селектел» | Заказчик |
|---|---|---|---|
| УПД.6 | Ограничение неуспешных попыток входа в объект информатизации (доступа к объекту информатизации) | Реализуется на уровне Служебной инфраструктуры | Необходимо реализовать на уровне Инфраструктуры Заказчика |
| 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 Инфраструктуры Заказчика |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации | Реализуется на уровне Служебной инфраструктуры | Необходимо реализовать на уровне Инфраструктуры Заказчика |
| 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 Инфраструктуры Заказчика |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа | Реализуется на уровне инфраструктуры Selectel | При необходимости - реализовать на уровне Инфраструктуры Заказчика |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств | Реализуется на уровне инфраструктуры Selectel | При необходимости - реализовать на уровне Инфраструктуры Заказчика |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) | Реализуется на уровне инфраструктуры Selectel | Необходимо реализовать на уровне Инфраструктуры Заказчика |

| Обозначение меры | Мера | АО «Селектел» | Заказчик |
|---|---|---|---|
| УПД.17 | Обеспечение доверенной загрузки средств вычислительной техники | Реализуется на уровне Служебной инфраструктуры | Необходимо реализовать на уровне размещаемого Заказчиком оборудования, используемого Заказчиком выделенного оборудования |
| 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 Служебной инфраструктуры | Необходимо реализовать на уровне Инфраструктуры Заказчика |
| ОПС.3 | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов | Реализуется на уровне Служебной инфраструктуры | Необходимо реализовать на уровне Инфраструктуры Заказчика |
| ЗНИ.1 | Учет машинных носителей персональных данных | Реализуется на уровне аппаратных компонентов | Необходимо реализовать на уровне размещаемого Заказчиком оборудования, используемого Заказчиком выделенного оборудования |
| ЗНИ.2 | Управление доступом к машинным носителям персональных данных | Реализуется на уровне аппаратных компонентов | Необходимо реализовать на уровне размещаемого Заказчиком оборудования |

| Обозначение меры | Мера | АО «Селектел» | Заказчик |
|---|---|---|---|
| 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 | Обеспечивается уничтожение и контроль уничтожения информации при передаче носителей между заказчиками, утилизации | Необходимо реализовать на уровне размещаемого Заказчиком оборудования, используемого Заказчиком выделенного оборудования[2] |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения | Реализуется на уровне Служебной инфраструктуры | Необходимо реализовать на уровне Инфраструктуры Заказчика |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации | Реализуется на уровне Служебной инфраструктуры | Необходимо реализовать на уровне Инфраструктуры Заказчика |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения | Реализуется на уровне Служебной инфраструктуры | Необходимо реализовать на уровне Инфраструктуры Заказчика |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них | Реализуется на уровне Служебной инфраструктуры | Необходимо реализовать на уровне Инфраструктуры Заказчика |
| РСБ.7 | Защита информации о событиях безопасности | Реализуется на уровне Служебной инфраструктуры | Необходимо реализовать на уровне Инфраструктуры Заказчика |
| АВЗ.1 | Реализация антивирусной защиты | Реализуется на уровне Служебной инфраструктуры | Необходимо реализовать на уровне Инфраструктуры Заказчика |

[2] Дополнительно рекомендуется самостоятельно обеспечить безопасность информации, обрабатываемой на арендуемом сервере, например, посредством ее шифрования

| Обозначение меры | Мера | АО «Селектел» | Заказчик |
|---|---|---|---|
| АВ3.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) | Реализуется на уровне Служебной инфраструктуры | Необходимо реализовать на уровне Инфраструктуры Заказчика |
| СОВ.1 | Обнаружение вторжений | Реализуется на уровне Служебной инфраструктуры | Необходимо реализовать на уровне Инфраструктуры Заказчика |
| СОВ.2 | Обновление базы решающих правил | Реализуется на уровне Служебной инфраструктуры | Необходимо реализовать на уровне Инфраструктуры Заказчика |
| АН3.1 | Выявление, анализ уязвимостей объекта информатизации и оперативное устранение вновь выявленных уязвимостей | Реализуется на уровнях ОС и прикладного ПО, служебной инфраструктуры | Необходимо реализовать на уровне Инфраструктуры Заказчика |
| АН3.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации | Реализуется на уровне Служебной инфраструктуры | Необходимо реализовать на уровне Инфраструктуры Заказчика |
| АН3.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации | Реализуется на уровне Служебной инфраструктуры | Необходимо реализовать на уровне Инфраструктуры Заказчика |
| АН3.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации | Реализуется на уровне Служебной инфраструктуры | Необходимо реализовать на уровне Инфраструктуры Заказчика |
| АН3.5 | Контроль правил генерации и смены паролей пользователей, заведения и | Реализуется на уровне Служебной инфраструктуры | Необходимо реализовать на уровне Инфраструктуры Заказчика |

| Обозначение меры | Мера | АО «Селектел» | Заказчик |
|---|---|---|---|
| | удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе | | |
| ОЦЛ.1 | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации | Реализуется на уровне Служебной инфраструктуры | Необходимо реализовать на уровне Инфраструктуры Заказчика |
| 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) | Реализуется на уровне инфраструктуры Selectel | При необходимости - реализовать на уровне Инфраструктуры Заказчика |
| ОДТ.3 | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование | Реализуется на уровне Служебной инфраструктуры, а также для выделенного оборудования на уровне инженерных систем | Необходимо реализовать на уровне Инфраструктуры Заказчика |
| ОДТ.4 | Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных | Реализуется на уровне Служебной инфраструктуры | Необходимо реализовать на уровне Инфраструктуры Заказчика |
| ОДТ.5 | Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных | Реализуется на уровне Служебной инфраструктуры | Необходимо реализовать на уровне Инфраструктуры Заказчика |

| Обозначение меры | Мера | АО «Селектел» | Заказчик |
|---|---|---|---|
| | данных (резервных копий) в течение установленного временного интервала | | |
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации | Реализуется на уровне платформ виртуализации и оркестрации | Необходимо реализовать на уровне виртуальных машин и контейнеров |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин | Реализуется на уровне платформ виртуализации и оркестрации | Необходимо реализовать на уровне виртуальных машин и контейнеров |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре | Реализуется на уровне платформ виртуализации и оркестрации | Необходимо реализовать на уровне виртуальных машин и контейнеров |
| ЗСВ.6 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных | Реализуется на уровне платформ виртуализации и оркестрации | Необходимо реализовать на уровне виртуальных машин и контейнеров |
| ЗСВ.7 | Контроль целостности виртуальной инфраструктуры и ее конфигураций | Реализуется на уровне платформ виртуализации и оркестрации | Необходимо реализовать на уровне виртуальных машин и контейнеров |
| ЗСВ.8 | Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры | Реализуется на уровне платформ виртуализации и оркестрации | Необходимо реализовать на уровне виртуальных машин и контейнеров |

| Обозначение меры | Мера | АО «Селектел» | Заказчик |
|---|---|---|---|
| ЗСВ.9 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре | Реализуется на уровне платформ виртуализации и оркестрации | Необходимо реализовать на уровне виртуальных машин и контейнеров |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей | Реализуется на уровне платформ виртуализации и оркестрации | Необходимо реализовать на уровне виртуальных машин и контейнеров |
| 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 на уровне технических средств | - |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр | Реализуется на уровне инфраструктуры Selectel | - |
| ЗИС.1 | Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению | Реализуется на уровне Служебной инфраструктуры | Необходимо реализовать на уровне Инфраструктуры Заказчика |

| Обозначение меры | Мера | АО «Селектел» | Заказчик |
|---|---|---|---|
| | (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы | | |
| 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 служебных сетей | Необходимо реализовать для сетей Заказчика, функционирующих на базе инфраструктуры продуктов и услуг Selectel |
| ЗИС.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов | Реализуется на уровне служебных сетей | Необходимо реализовать для сетей Заказчика, функционирующих на базе инфраструктуры продуктов и услуг Selectel |
| 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 Инфраструктуры Заказчика |
| 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 Инфраструктуры Заказчика |

| Обозначение меры | Мера | АО «Селектел» | Заказчик |
|---|---|---|---|
| ЗИС.20 | Защита беспроводных соединений, применяемых в информационной системе | Реализуется на уровне инфраструктуры Selectel | При необходимости - реализовать на уровне Инфраструктуры Заказчика |
| ИНЦ.1 | Определение лиц, ответственных за выявление инцидентов и реагирование на них | Реализуется для инцидентов, возникающих на уровне Служебной инфраструктуры | Необходимо реализовать для инцидентов в зоне ответственности Заказчика |
| ИНЦ.2 | Обнаружение, идентификация и регистрация инцидентов | Реализуется для инцидентов, возникающих на уровне Служебной инфраструктуры | Необходимо реализовать для инцидентов в зоне ответственности Заказчика |
| ИНЦ.3 | Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами | Реализуется для инцидентов, возникающих на уровне Служебной инфраструктуры | Необходимо реализовать для инцидентов в зоне ответственности Заказчика |
| ИНЦ.4 | Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий | Реализуется для инцидентов, возникающих на уровне Служебной инфраструктуры | Необходимо реализовать для инцидентов в зоне ответственности Заказчика |
| ИНЦ.5 | Принятие мер по устранению последствий инцидентов | Реализуется для инцидентов, возникающих на уровне Служебной инфраструктуры | Необходимо реализовать для инцидентов в зоне ответственности Заказчика |
| ИНЦ.6 | Планирование и принятие мер по предотвращению повторного возникновения инцидентов | Реализуется для инцидентов, возникающих на уровне Служебной инфраструктуры | Необходимо реализовать для инцидентов в зоне ответственности Заказчика |

| Обозначение меры | Мера | АО «Селектел» | Заказчик |
|---|---|---|---|
| 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 Инфраструктуры Заказчика |
| УКФ.2 | Управление изменениями конфигурации объекта информатизации и системы защиты информации | Реализуется на уровне Служебной инфраструктуры | Необходимо реализовать на уровне Инфраструктуры Заказчика |
| 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 Инфраструктуры Заказчика |
| УКФ.4 | Документирование информации (данных) об изменениях в конфигурации объекта информатизации и системы защиты информации | Реализуется на уровне Служебной инфраструктуры | Необходимо реализовать на уровне Инфраструктуры Заказчика |

## Лист регистрации изменений

| Номер редакции | Дата | Описание |
|---|---|---|
| 1 | 25 декабря 2025 г. | Исходный документ.<br>Проведена оценка эффективности принимаемых мер. |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |