

# Выписка из модели угроз и нарушителя безопасности информации информационной системы «Инфраструктура» аттестованного сегмента центра обработки данных ООО «Селектел»

Общее описание	<b>2</b>
Аттестованный сегмент центра обработки данных	2
Информационная система «Инфраструктура»	3
Классификация	3
Разделение зон ответственности	3
Оценка актуальности угроз безопасности	<b>4</b>
Угрозы, не подлежащие рассмотрению в качестве актуальных	4
Угрозы, признанные актуальными	5
Меры для нейтрализации актуальных угроз	<b>5</b>

## Общее описание

Моделирование угроз безопасности информации осуществляется с учетом требований «Методики оценки угроз безопасности информации», разработанной и утвержденной ФСТЭК России 05.02.2021 года. Результаты оценки угроз, приведенные в данной выписке, могут использоваться для оценки угроз в отношении систем клиента согласно п. 2.10–2.13 Методики в качестве определенных актуальных угроз информационно-телекоммуникационной инфраструктуры, на базе которой система или сеть клиента функционирует.

...

## Аттестованный сегмент центра обработки данных

Услуга «Аттестованный сегмент центра обработки данных» предназначена для размещения систем и приложений с повышенными требованиями к обеспечению информационной безопасности и состоит из набора аттестованных информационных систем:

- «Инфраструктура» — клиенту в полное управление предоставляются выделенные и виртуальные серверы произвольной конфигурации, сетевое оборудование и дополнительные средства защиты информации, расположенные в дата-центрах Селектел. Информационно-телекоммуникационная инфраструктура обеспечивает техническую и организационную возможность размещения информационных систем клиентов, предъявляющих требования к классу защищенности информации до первого класса (К1) защищенности включительно в соответствии с приказом ФСТЭК России № 17 от 11.02.2013 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», а также к уровню защищенности персональных данных до первого (УЗ1) включительно в соответствии с Постановлением Правительства № 1119 и приказом ФСТЭК России № 21 от 18.02.2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
- «Управляемые сервисы безопасности» — набор сервисов информационной безопасности, предназначенных для оказания услуг клиентам, а также централизованного управления средствами защиты информации. Использование сервисов позволяет выполнять требования приказов ФСТЭК России № 21 и № 17, а также требованиям международных стандартов, предъявляемых к информационным системам клиентов по сервисной модели с ежемесячной оплатой без капитальных вложений на закупку средств защиты.
- «Администрирование» — выделенные рабочие места сотрудников с усиленными мерами безопасности для оказания услуг администрирования средств и систем защиты информации. Клиентам доступны как разовые работы, так и полное сопровождение систем, включая реагирование на инциденты информационной безопасности. Наличие аттестата по требованиям безопасности информации позволяет клиентам передавать на

администрирование собственные аттестованные системы, не нарушая требований законодательства.

- «Мониторинг информационной безопасности» — система, предназначенная для мониторинга событий информационной безопасности, регистрации и реагирования на инциденты информационной безопасности. Инфраструктура удовлетворяет требованиям ФСТЭК России в части лицензии на услуги по мониторингу информационной безопасности средств и систем информатизации.

## Информационная система «Инфраструктура»

В рамках информационной системы «Инфраструктура» клиенту в полное управление предоставляются выделенные и виртуальные серверы произвольной конфигурации, сетевое оборудование и дополнительные средства защиты информации, расположенные в дата-центрах ООО «Селектел» ...

### Классификация

В соответствии с «Актом классификации информационной системы «Инфраструктура» присвоены:

- Первый класс защищенности (К1) информационной системы в соответствии с приказом ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»
- Первый уровень защищенности (У31) персональных данных в соответствии с Постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Соответствие требованиям безопасности информации подтверждается аттестатом №3479.00001.2022 от 10 марта 2022 г.

### Разделение зон ответственности

ООО «Селектел» обеспечивает непрерывное функционирование инфраструктуры, размещает оборудования клиентов в телекоммуникационных стойках, подключенных к инженерным системам, обеспечивающим электропитание и заземление, соблюдение температурного режима (вентиляцию и кондиционирование), а также обеспечивает физическую безопасность, включая видеонаблюдение и контроль физического доступа.

Клиент отвечает за безопасность системного и прикладного программного обеспечения, а также сетевого периметра размещаемой информационной системы.

...

## Оценка актуальности угроз безопасности

Определение актуальных угроз безопасности информации при ее обработке в ИС «Инфраструктура» осуществляется с учетом требований «Методики оценки угроз безопасности информации», разработанной и утвержденной ФСТЭК России 05.02.2021 года.

Перечень актуальных для объекта информатизации «Информационная система «Инфраструктура» угроз безопасности представлен в Таблице 1.

Таблица 1 - Перечень актуальных угроз

<b>Идентификатор угрозы</b>	<b>Наименование угрозы</b>
...	...
...	...

## Меры для нейтрализации угроз безопасности

Нейтрализация (минимизация вероятности возникновения) актуальных угроз безопасности информации осуществляется за счет использования подсистем защиты информации

...

Описание способов реализации защитных мер приведено в Таблице 2.

Таблица 2 - Нейтрализация угроз

<b>Подсистема (группа мер) защиты</b>	<b>Идентификатор угрозы</b>
...	...
...	...

Таблица 3 - Реализация защитных мер

<b>Мера защиты</b>	<b>Реализация</b>
...	...
...	...