Selectel

Выписка из документа «Модель угроз и нарушителя безопасности информации инженерной инфраструктуры центров обработки данных, предоставляемой в рамках услуги «Аттестованный сегмент ЦОД» Акционерного общества «Селектел»

Обратите внимание!	Это шаблон документа, размещен на сайте selectel.ru. Для получения заполненного документа с указанием адресов инфраструктуры, перечня актуальных угроз и мер, принимаемых для их нейтрализации, создайте Тикет в панели управления my.selectel.ru

В настоящем документе представлена информация о перечне угроз безопасности информации, признанных актуальными по результатам оценки угроз безопасности для инженерной инфраструктуры центров обработки данных (далее - Инфраструктура), владельцем которых является Акционерное общество «Сеть дата-центров «Селектел» (далее – Общество).

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 No 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 (У31) включительно в соответствии с Постановлением Правительства No 1119 и приказом ФСТЭК России No 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».

Selectel

Инфраструктура расположена на территориальных площадках:

- ...
- ...
- ...

Определение актуальности угроз безопасности информации для Инфраструктуры осуществлялось с учетом положений Методики оценки угроз безопасности информации (утверждена ФСТЭК России 05.02.2021 г.) и для компонентов, находящихся в зоне ответственности Общества.
Более подробная информация о разделении зон ответственности представлена в **Приложении 1**.

Результаты оценки могут быть использованы для моделирования угроз безопасности информации, обрабатываемой в информационных системах, функционирующих на базе Инфраструктуры.

Для Инфраструктуры реализована система защиты, включающая набор организационных и технических мер, направленных на минимизацию вероятности возникновения угроз безопасности информации.

Меры выбраны с учетом требований следующих документов:

- Постановление Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» № 1119 от 01.11.2012 г.;
- Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- Руководящий документ Автоматизированные системы. Защита

от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации (утв. решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.).

Эффективность принимаемых Обществом мер по обеспечению безопасности информации для следующих стоек, входящих в состав Инфраструктуры:

- ...
- ...
- ...

подтверждена посредством проведения аттестационных испытаний...

Для остальных стоек, входящих в состав Инфраструктуры, реализованы аналогичные меры по обеспечению безопасности информации.

Сведения о мерах защиты информации, реализованных в отношении Инфраструктуры, а также информация об особенностях их реализации представлена в **Приложении 2**.

В **Таблице 1** представлен перечень актуальных для Инфраструктуры угроз безопасности информации, а также сведения о мерах защиты, принимаемых для их блокирования (нейтрализации).

Таблица 1 - Перечень актуальных угроз и сведения о мерах, принимаемых для их блокирования (нейтрализации)

Идентификатор угрозы	Наименование угрозы	Меры, принимаемые для нейтрализации угрозы
...	...	...
...	...	...
...	...	...

Selectel

Приложение 1. Разграничение зон ответственности

Разграничение ответственности между АО «Селектел» и клиентами реализуется следующим образом:

1. АО «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.

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

Приложение 2. Реализованные меры защиты информации

Система защиты Инфраструктуры состоит из набора организационных и технических мер защиты информации, обеспечивающих блокирование (нейтрализацию) угроз безопасности информации, указанных в **Таблице 1**.

Перечень мер защиты информации составлен на основе базового набора мера защиты для класса защищенности К1, адаптирован, уточнен и дополнен с учетом структурно-функциональных характеристик Инфраструктуры, используемых информационных технологий, особенностей функционирования, применимого законодательства и актуальных угроз безопасности информации. Перечень мер и особенности их реализации представлены в **Таблице 2**.

Таблица 2 - Перечень реализуемых мер защиты информации

Обозначение меры	Описание меры	Реализация мер
...	...	...
...	...	...
...	...	...