Приложение № 2

к Техническому заданию

на оказание государственным и муниципальным образовательным организациям, реализующим образовательные программы общего образования и среднего профессионального образования**,** избирательным комиссиям субъектов Российской Федерации и территориальным избирательным комиссиям (с учетом потребностей пользователей)

услуг по предоставлению с использованием единой сети передачи данных доступа к государственным, муниципальным, иным информационным системам и к информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»); по передаче данных при осуществлении доступа к государственным, муниципальным, иным информационным системам и к сети «Интернет»; по защите данных, обрабатываемых и передаваемых при осуществлении доступа к государственным, муниципальным, иным информационным системам и к сети «Интернет»; по обеспечению ограничения доступа к информации, распространение которой в Российской Федерации запрещено, и к информации, причиняющей вред здоровью и (или) развитию детей, содержащейся в сети «Интернет» (для указанных образовательных организаций); по мониторингу и обеспечению безопасности связи при предоставлении доступа к государственным, муниципальным, иным информационным системам и к сети «Интернет»; по организации подключения к единой сети передачи данных указанных образовательных организаций и избирательных комиссий, по передаче данных при осуществлении доступа к этой сети

**Программа и методика испытаний**

1. Процедура проведения испытаний
   1. Заказчик осуществляет проверку наличия у представителя Исполнителя следующих документов:

* копия Государственного контракта с приложениями.
  1. В случае отсутствия документов указных в пункте 1 главы I Заказчик проводит мероприятия, указанные в п. 3 главы I. Акт проверки оказания Услуг (Приложение № 3 к Техническому заданию) не подписывается до устранения замечаний.
  2. Заказчик проверяет компоненты Услуг согласно главы II на соответствии требованиям Технического задания. Проверки проводятся согласно главе IV.
  3. В случае отсутствия замечаний или после их устранения подписывается Акт проверки оказания Услуг (приложение № 3 к Техническому заданию).

1. Цель проведения испытаний

Целью проведения испытаний является проверка соответствия предоставляемых Услуг связи и её компонентов требованиям Технического задания.

Состав проверяемых компонентов Услуг связи:

* Компонент Услуг связи «Передача данных L2»;
* Компонент Услуг связи «Передача данных»;
* Компонент Услуг «Защита данных»;
* Компонент Услуг «Ограничение доступа к информации»;
* Компонент Услуг «Мониторинг и обеспечение безопасности связи».

1. Объём испытаний

Перечень проверок компонентов Услуг приведен ниже:

|  |  |  |
| --- | --- | --- |
| № | Проверяемый компонент | Что проверяется |
|  | Компонент Услуг «Передача данных» (за исключением Услуги передачи данных в ВЧС для ГАС «Выборы») | Обеспечение передачи данных СЗО в единой сети передачи данных |
|  | Компонент Услуг «Защита данных» | Обеспечение защиты данных, обрабатываемых и передаваемых при осуществлении доступа для СЗО |
|  | Компонент Услуг «Ограничение доступа к информации» | Обеспечение и контроль доступа пользователей в сеть «Интернет» с фильтрацией входящего и исходящего Интернет-трафика по протоколам HTTP/HTTPS |
|  | Компонент Услуг «Мониторинг и обеспечение безопасности связи» | Блокировка запрещенных типов взаимодействий, мониторинг качества предоставляемых услуг и защита от DDoS атак |
|  | Компонент Услуг связи «Передача данных L2» | Обеспечение передачи данных от СЗО до Точки присоединения ЕСПД |

1. Методики тестирования
   1. **Проведение испытаний компонента Услуги «Передача данных»**

- элемент «Передача данных» в ВЧС с заданными параметрами качества

- элемент «Передача данных» в сеть Интернет

1. Введение
   1. Настоящий раздел определяет порядок проведения испытаний при проверке Услуг Исполнителем в его зоне ответственности по предоставлению доступа СЗО к сети Интернет/ЕСПД, определенных Государственным контрактом на объекте.
   2. Контролируемыми параметрами подключения являются:

* пропускная способность канала по направлениям от и к СЗО, единица измерения – Мбит/с;
* время задержки IP-пакетов, единица измерения – мс;
* вариация времени задержки IP-пакетов (далее – джиттер), единица измерения – мс;
* потери IP-пакетов, единица измерения – процент.
  1. Контроль проводится с использованием исключительно передачи и приема цифровой информации, в связи с чем показатели точности измерений не устанавливаются.
  2. Результаты проведения инструментального контроля вносятся в Протокол проведения тестирования Услуг (далее – Протокол проведения тестирования) (Приложение № 6 к Техническому заданию).

1. Методика проверки элемента «Передача данных» в ВЧС с заданными параметрами качества
   1. Значения показателей пропускной способности проверяются согласно Техническому заданию:
      1. Требования к средствам измерений, вспомогательным устройствам, материалам.
      2. При выполнении проверки применяют следующие средства измерений, вспомогательные устройства, материалы:

* переносной компьютер (ноутбук) с тактовой частотой не менее 1 ГГц, объемом памяти не менее 4 Гбайт, наличием не менее 1 порта Gigabit Ethernet, наличием операционной системы MS Windows версии 7 и выше или FreeBSD/Linux (далее – Ноутбук);
* интернет-обозреватель Firefox, Chrome, Opera и их аналоги (Спутник, Яндекс) в версии не ранее 2019 года, установленные на Ноутбуке;
* ПО (утилита) *cmd*, установленное на Ноутбуке в составе ОС.
  + 1. При проведении инструментального контроля на Ноутбуке должны быть отключены антивирусные, межсетевые экраны и прочие программы, которые могут привести к повышению загрузки центрального процессора, либо передаче данных по сети, а также препятствию передачи данных по сетевым портам (блокирование).
    2. IP-адрес, шлюз по умолчанию и маска подсети для проведения проверки, планы IP-адресации для СЗО, параметры подключения (в том, числе порт на оборудовании Исполнителя) предоставляются Исполнителем при проведении проверки.
  1. Метод и порядок проведения проверки.
     1. Проверка осуществляются с помощью команды *ping* утилиты *cmd*.

Порядок проведения проверки:

* + - * Подключить Ноутбук к оборудованию Исполнителя в Точке присоединения к ЕСПД того субъекта РФ, в котором проводится проверка
      * Запустить утилиту *cmd* на Ноутбуке;
      * Ввести команду *ping X.X.X.X,* где *X.X.X.X* – IP-адрес выделенный для СЗО согласно плана IP-адресации;
      * Запустить тест;
      * Прервать проведение теста по истечении 30 секунд;
      * Зафиксировать результат проверки в Протоколе проведения тестирования Услуг. Положительным результатом является наличие отклика на ICMP-запрос, что подтверждает сетевую доступность СЗО.
  1. **Методика проверки элемента «Передача данных» в сеть Интернет.**
  2. Установленные требования к контролируемым параметрам подключения Услуги в СЗО:
* скорость передачи данных – согласно требований ТЗ;
* процент потерянных пакетов – не более 5%;
* задержка передачи пакетов:
* по проводным каналам – не более 250 мс;
* на составных каналах с учетом наличия одного беспроводного участка (одного спутникового скачка) – не более 1000 мс.
  1. Требования к средствам измерений, вспомогательным устройствам, материалам:
     1. При выполнении инструментального контроля применяют следующие средства измерений, вспомогательные устройства, материалы:
* 1 переносной компьютер (ноутбук) с тактовой частотой не менее 1 ГГц, объемом памяти не менее 4 Гбайт, наличием не менее 1 порта Gigabit Ethernet, наличием операционной системы (далее – ОС) Linux или FreeBSD или MS Windows версии 7 и выше (далее – Ноутбук);
* интернет-обозреватель Firefox, Chrome, Opera или их аналоги (Спутник, Яндекс) в версии не ранее 2019 года;
* ПО (утилита) *cmd* (командная строка) установленное на каждом Ноутбуке в составе ОС.
  + 1. При проведении инструментального контроля на Ноутбуке должны быть отключены антивирусные и прочие программы, которые могут привести к повышению загрузки центрального процессора, либо передаче данных по сети передачи данных.
  1. Метод и порядок измерений
     1. Измерение пропускной способности канала связи и времени задержки IP‑пакетов осуществляется посредством сервиса для контроля скорости доступа в Интернет (далее – СКСДИ) по адресу <http://speedtest.rt.ru> с Ноутбука, подключенного к порту оборудования Исполнителя на объекте согласно схемы организации Услуг (рис.3).
     2. Настройки сетевого подключения на ноутбуке (IP-адрес, шлюз по умолчанию и маска подсети за проверяемый СЗО), планы IP-адресации для СЗО, параметры подключения (в том, числе порт на оборудовании Исполнителя) предоставляются Исполнителем при проведении проверки.
     3. Проверка проводиться в следующем порядке:
* Открыть в интернет-обозревателе на Ноутбуке электронный адрес клиента СКСДИ (<http://speedtest.rt.ru>);
* На открывшейся в окне интернет-обозревателя (странице) нажать на кнопку «Начать тестирование»;
* Дождаться окончания измерений (примерно 60 секунд) и зафиксировать результат измерений в Протоколе проведения тестирования Услуг. В качестве значения времени задержки IP-пакетов принимается половина от измеренной круговой задержки;
* Скриншот результатов измерений внести в Протокол проведения тестирования Услуг.
  + 1. Измерение потерь IP-пакетов осуществляется с использованием утилиты *cmd* в следующем порядке (порядок приведен для операционной системы MS Windows):

Алгоритм измерения процента потерь IP-пакетов:

* Запустить утилиту *cmd* на Ноутбуке;
* Ввести команду *ping* [*test.ip.rt.ru*](http://test.ip.rt.ru)*,*  где http://test.ip.rt.ru – электронный адрес в сети «Интернет» в зоне ответственности Исполнителя.Резервный электронный адрес *speedtest.rt.ru;*
* Провести тест в течении 60 секунд, прервать проведение теста по истечении 60 секунд и зафиксировать результаты измерения – процент потерянных пакетов;
* Результаты инструментального контроля оформить в Протокол проведения тестирования Услуг;
* Скриншот результатов измерений внести в Протокол проведения тестирования Услуг.

**3. Проведение приемочных испытаний компонента Услуг «Защита данных»**

- элемент « Криптографическая защита каналов связи»

* + - 1. Введение
  1. Целью испытания является проверка возможности передачи пакетов данных в рамках закрытого (защищенного) контура сети и отсутствии возможности передачи данных в другие сети.
     + 1. Требования к средствам измерений, вспомогательным устройствам, материалам:
  2. При выполнении инструментального контроля применяют следующие средства измерений, вспомогательные устройства, материалы:
* 1 переносной компьютер (ноутбук) с тактовой частотой не менее 1 ГГц, объемом памяти не менее 4 Гбайт, наличием не менее 1 порта Gigabit Ethernet, наличием операционной системы (далее – ОС) Linux или FreeBSD или MS Windows версии 7 и выше (далее – Ноутбук);
* интернет-обозреватель Firefox, Chrome, Opera или их аналоги (Спутник, Яндекс) в версии не ранее 2019 года;
* ПО (утилита) cmd (командная строка) установленное на каждом Ноутбуке в составе ОС.

3 Метод и порядок измерений

3.1 Для проверки следует подключить Ноутбук к порту оборудования Исполнителя на объекте (криптомаршрутизатора) и настроить сетевое подключение согласно параметров таблицы адресации в общей подсети для выбранного (выбранных) СЗО (план IP-адресации) - адрес, маска и шлюз по умолчанию. План IP—адресации и параметры подключения, определяемые в соответствии с планом IP-адресации СЗО в закрытом контуре сети, предоставляется Исполнителем Заказчику при проведении проверки.

Алгоритм проверки:

* + - * + Запустить утилиту *cmd* на Ноутбуке;
        + Ввести команду ping test.ip.rt.ru, где test.ip.rt.ru – электронный адрес в открытой сети (сети «Интернет») в зоне ответственности Исполнителя. Данный адрес должен быть недоступен для взаимодействия;
        + Ввести команду ping X.X.X.X, где X.X.X.X - адрес криптомаршрутизатора в СЗО. Данный адрес должен быть доступен в рамках взаимодействия внутри закрытого контура;
        + Результаты проведения инструментального контроля вносятся в Протокол проведения тестирования Услуг.
      1. **Проведение приемочных испытаний компонента Услуг «Ограничение доступа к информации**
* элемент «Контентная фильтрация»

1. Введение
   1. Настоящий документ описывает методику проведения тестирования компонента Услуг «Ограничение доступа к информации».
   2. Целью проведения тестирования является проверка соответствия компонента Услуг «Ограничение доступа к информации» требованиям Технического задания (далее – ТЗ). Состав проверяемых элементов компонентов Услуг «Информационная безопасность» (далее - Услуги):

- Компонент услуг «Ограничение доступа к информации» обеспечивает ограничение доступа к информации, распространение которой в Российской Федерации запрещено, и к информации, наносящей вред здоровью и развитию детей, содержащейся в сети Интернет:

* проверяемый элемент «Контентная фильтрация».

1. Объём испытаний.
   1. В состав испытаний элемента «Контентная фильтрация» входит проверка по обеспечению и контролю доступа пользователей в сеть Интернет с фильтрацией входящего и исходящего Интернет-трафика.
2. Условия и порядок проведения испытаний.
   1. Проведение испытаний компонента Услуг проводится на объекте, на котором оказывается Услуга.
   2. Приемочные испытания компонента Услуг «Ограничение доступа к информации» начинаются при подтверждении готовности программно‑аппаратных средств Исполнителя, используемых в составе проверяемых компонентов Услуг.
   3. Во время проведения тестирования функциональных возможностей Системы ни одна из сторон не должна проводить работы, которые каким-либо образом могут повлиять на результаты испытаний. В случае каких-либо отклонений от настоящей Программы стороны должны утвердить такие отклонения.
3. Требования к средствам измерений, вспомогательным устройствам, материалам:
   * При выполнении инструментального контроля применяют следующие средства измерений, вспомогательные устройства, материалы:

* 1 переносной компьютер (ноутбук) с тактовой частотой не менее 1 ГГц, объемом памяти не менее 4 Гбайт, наличием не менее 1 порта Gigabit Ethernet, наличием операционной системы (далее – ОС) Linux или FreeBSD или MS Windows версии 7 и выше (далее – Ноутбук);
* интернет-обозреватель Firefox, Chrome, Opera или их аналоги (Спутник, Яндекс) в версии не ранее 2019 года;
* Методика тестирования;
  + Проверка обеспечения и контроля доступа пользователей в сеть Интернет с фильтрацией входящего и исходящего Интернет-трафика компонента Услуг «Ограничение доступа к информации», элемент «Контентная фильтрация».
  1. В качестве проверки проводится тестирование фильтрации доменов согласно базе данных ресурсов, относящихся к запрещенным категориям (наркотики, порнография, терроризм, экстремизм, насилие, социальные сети, анонимайзеры и т.д.) в соответствии с требованиями нормативной документацией Российской Федерации:

- Блокировка URL ресурсов, относящихся к запрещенным категориям, по протоколам HTTP/HTTPS, внесенных в реестры Роскомнадзора, такие как «Единый Реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено», внесенных в «Федеральный список экстремистских материалов» Министерства юстиции Российской Федерации;

- Блокировка ресурсов, относящихся к запрещенным категориям, по вводимому IP-адресу.

Алгоритм проверки:

* + - * + Настроить на Ноутбуке IP-адрес, шлюз по умолчанию и маску подсети, назначенные для проверяемого СЗО;
        + Подключить Ноутбук к оборудованию Исполнителя на объекте;
        + Настроить на Ноутбуке IP-адрес, IP-адрес шлюза по умолчанию и маску подсети в соответствии с планом IP-адресации. Дополнительно на ноутбуке настроить IP-адрес прокси-сервера в соответствии с планом IP-адресации и установить файл сертификата прокси-сервера. План IP—адресации и параметры подключения для проведения проверки предоставляется Исполнителем Заказчику при проведении проверки;
* Запустить на Ноутбуке интернет-браузер;
* Ввести в адресную строку URL ресурса, относящегося к запрещённой категории (приложение №1). Убедиться, что доступ к запрещенному ресурсу заблокирован;
* Ввести в адресную строку URL ресурса, относящегося к разрешённой категории (приложение №1). Убедиться, что доступ к ресурсу разрешён;
* Ввести в адресную строку IP-адрес ресурса, относящегося к запрещённой категории (приложение №1). Убедиться, что доступ к запрещенному ресурсу заблокирован;
* Ввести в адресную строку IP-адрес ресурса, относящегося к разрешённой категории (приложение №1). Убедиться, что доступ к ресурсу разрешён;
* Результат проверки отразить в Протоколе проведения тестирования Услуги (приложение № 6 к Техническому заданию).

Приложение № 1

Перечни URL ресурсов и разрешенных и запрещенных IP-адресов:

1. Перечень запрещённых и разрешённых URL ресурсов (протокол HTTP/HTTPS)

|  |  |  |  |
| --- | --- | --- | --- |
| URL ресурса (пример списка) | IP-адрес Ноутбука с которого проводится проверка (открытая ЛВС): | Результат блокировки | Категория |
| <https://yandex.ru> | 10.x.x.x | Не заблокирован | Разрешенный ресурс |
| <https://vk.com> | 10.x.x.x | Заблокирован | Социальная сеть |
| <https://www.facebook.com> | 10.x.x.x | Заблокирован | Социальная сеть |
| <http://pornhub.com> | 10.x.x.x | Заблокирован | Порнография |
| <http://worldoftanks.ru> | 10.x.x.x | Заблокирован | Комп. игры |
| <http://3rm.info/?newsid=26584> | 10.x.x.x | Заблокирован | - |
| <http://upyachka.ru> | 10.x.x.x | Заблокирован | Досуг |

2. Перечень запрещённых и разрешённых URL ресурсов (Блокировка по IP-адресам ресурса)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ip-адрес ресурса | Сайт | IP-адрес Ноутбука с которого проводится проверка (открытая ЛВС): | Результат блокировки | Категория |
| 87.240.131.99 | [vk.com](https://vk.com) | Заблокирован | Заблокирован | Социальная сеть |
| 31.13.64.97 | [www.facebook.com](http://www.facebook.com) | Заблокирован | Заблокирован | Социальная сеть |
| 62.240.84.135 | [3rm.info/?newsid=26584](http://3rm.info/?newsid=26584) | Заблокирован | Заблокирован | - |
| 185.12.241.151 | [worldoftanks.ru](http://worldoftanks.ru) | Заблокирован | Заблокирован | Комп. игры |

* + - 1. **Проведение приемочных испытаний компонента Услуг «Мониторинг и обеспечение безопасности связи»**

- элемент « Межсетевое экранирование»;

- элемент « Мониторинг качества предоставляемых услуг»;

- элемент «Защита от DDoS атак».

1. Проверка блокировки запрещенных типов взаимодействий элемента услуг «Межсетевое экранирование».

* 1. Условия и порядок проведения испытаний
     1. В качестве проверки проводится тестирование блокировки запрещенных типов взаимодействий в соответствии с настроенными политиками информационной безопасности.
     2. Требования к средствам измерений, вспомогательным устройствам, материалам:
        1. При выполнении инструментального контроля применяют следующие средства измерений, вспомогательные устройства, материалы:
* 1 переносной компьютер (ноутбук) с тактовой частотой не менее 1 ГГц, объемом памяти не менее 4 Гбайт, наличием не менее 1 порта Gigabit Ethernet, наличием операционной системы (далее – ОС) Linux или FreeBSD или MS Windows версии 7 и выше (далее – Ноутбук);
* интернет-обозреватель Firefox, Chrome, Opera или их аналоги (Спутник, Яндекс) в версии не ранее 2019 года;
* ПО (утилита) *cmd* (командная строка) установленное на каждом Ноутбуке в составе ОС.

1.1.3 Для проведения проверки Ноутбук необходимо подключить к порту криптомаршрутизатора для открытой сети или напрямую к коммутатору доступа.

Алгоритм проведения проверки

* + - * Настроить на Ноутбуке IP-адрес, IP-адрес шлюза по умолчанию и маску подсети в соответствии с планом IP-адресации. План IP—адресации и параметры подключения для проведения проверки предоставляется Исполнителем Заказчику при проведении проверки;
      * Запустить утилиту *cmd;*
      * Ввести команду *ping* [*192.168.1.1*](http://test.ip.rt.ru)*, где 192.168.1.1 –* IP-адрес частной сети класса С (не используемой в Плане IP-адресации СЗО);
      * Убедиться, что доступ к сторонней сети заблокирован;
      * Зафиксировать результат проверки.

1.2 Проверка элементов услуги «Мониторинг качества предоставляемых услуг» и «Защита от DDoS атак».

1.2.1. В ходе оказания Услуги «Мониторинг и обеспечение безопасности связи» Исполнитель обеспечивает оказание Услуг «Мониторинг качества предоставляемых услуг» и «Защита от DDoS атак» в соответствии с условиями государственного контракта в ходе предоставления Услуг посредством ЕСПД в соответствии с действующими техническими политиками в части обеспечения мониторинга и безопасности связи.

1.2.2. Достаточными факторами для подтверждения факта оказания услуг являются:

- отсутствие влияний на передачу данных, в том числе и на доступность ресурсов, в том числе вследствие осуществления DDoS атак.

1.3. Результаты проверки отразить в Протоколе проведения тестирования Услуги (приложение № 6 к Техническому заданию).

|  |  |  |
| --- | --- | --- |
| **от Заказчика:**  **Заместитель Министра**  **цифрового развития, связи и массовых коммуникаций Российской Федерации**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /Д.К.Угнивенко / |  | **от Исполнителя:**  **Старший Вице-Президент по работе с корпоративным и государственным сегментами ПАО «Ростелеком»**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/В.В.Ермаков/ |