ДОГОВОР № 5-2025

г. Южно-Сахалинск «24» 01 2025 года.

Федеральное государственное бюджетное образовательное учреждение высшего образования «Сахалинский государственный университет» (далее - СахГУ), именуемое в дальнейшем «АБОНЕНТ», в лице временно исполняющего обязанности ректора Шмерецкого Александра Андреевича, действующего на основании Приказа № 7-пр от 15.01.2025 г., и **Публичное Акционерное общество «Мобильные Телесистемы» (ПАО «МТС»)**, именуемое в дальнейшем «ПРОВАЙДЕР», в лице начальника отдела по работе с корпоративными клиентами Борисенко Ольги Игоревны, действующего на основании доверенности от 21.02.2023 г., зарегистрированной нотариусом г. Москвы Семеновой А.Н. в реестре № 77/509-н/77-2023-3-350 (номер бланка 77АД2159968), вместе именуемые «Стороны», и каждый в отдельности «Сторона», в соответствии с Федеральным законом от 18.07.2011 г. № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц», пп.12, п.2, раздела 2 Положения о закупке товаров, работ, услуг для нужд ФГБОУ ВО «СахГУ», заключили настоящий Договор (далее-Договор) о нижеследующем:

1. ПРЕДМЕТ ДОГОВОРА

1.1. Настоящий договор регулирует взаимоотношения между ПРОВАЙДЕРОМ и АБОНЕНТОМ по **предоставлению услуг телематических служб** далее - Услуг.

1.2. Предметом договора является предоставление АБОНЕНТУ услуг телематических служб сети Интернет по выделенной линии, в соответствии с Приложением № 1 к договору.

1.3. Приложение № 1 к договору на предоставление услуг является неотъемлемой частью настоящего договора и обязательным для ПРОВАЙДЕРА и АБОНЕНТА.

1.4. Услуги оказываются с момента заключения договора по 31 декабря 2025 г.

2. ЦЕНА ДОГОВОРА

2.1. Общая цена Договора, составляет **рублей 00 копеек**, в т. ч. НДС (20%).

2.2. Оплата по настоящему Договору осуществляется ежемесячно в размере тысяч) рублей, на основании выставленного счета, счет-фактуры, акта об оказанных услугах и не может превышать сумму, указанную в п. 2.1 настоящего Договора.

2.3. Цена Договора является твердой, не может изменяться в ходе заключения и исполнения Договора, за исключением случаев, установленных настоящим Договором и (или) предусмотренных законодательством Российской Федерации.

2.4. Цена Договора включает в себя все расходы ПРОВАЙДЕРА, связанные с оказанием услуг в полном объеме и надлежащего качества, в том числе страхование, уплату пошлин, налогов, сборов и иных обязательных платежей.

3. ОБЯЗАННОСТИ СТОРОН

3.1. ПРОВАЙДЕР обязуется с момента заключения договора:

3.1.1. Предоставить Абоненту при заключении Договора необходимую и достоверную информацию об Услугах, их перечне и правилах оказания, о реквизитах действующих лицензий, на основании которых оказываются Услуги, Тарифных планах, порядке и условиях оплаты Услуг, порядке и сроке доставки счетов, а также иную информацию, предусмотренную действующим законодательством РФ.

3.1.2. Организовать бесплатное и круглосуточное консультирование по вопросам пользования Услугой в объеме, предусмотренном действующим законодательством Российской Федерации.

3.1.3. ПРОВАЙДЕР гарантирует качество предоставляемых Услуг в соответствии с условиями лицензии (Л030-00114-77/00076706, на услуги передачи данных и телематических служб, выданных ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ)

3.1.4. Начать оказывать Абоненту Услуги в течение срока, предусмотренного Договором.

3.1.5. Соблюдать установленные Оператором сроки и порядок устранения неисправностей, препятствующих пользованию телематическими услугами связи и услугами по передаче данных.

3.2. АБОНЕНТ с момента заключения договора обязуется:

3.2.1. АБОНЕНТ обязуется принять УСЛУГИ в пользование по завершении подключения/инсталляции УСЛУГ и подписать соответствующий акт или направить письменно мотивированный отказ в принятии.

3.2.2. Оплачивать услуги, предоставляемые ПРОВАЙДЕРОМ в сроки, предусмотренные настоящим договором.

3.2.3. Читать и принимать к сведению информацию о технологических и организационных изменениях, рассылаемую посредством электронной почты ПРОВАЙДЕРОМ.

3.2.4. Соблюдать авторские права на предоставляемые ПРОВАЙДЕРОМ документацию, программные средства и на информацию, полученную по информационным каналам ПРОВАЙДЕРА.

3.2.5. Ответственность за ущерб любого рода, понесенный АБОНЕНТОМ или третьей Стороной в ходе использования АБОНЕНТОМ услуг ПРОВАЙДЕРА, несет АБОНЕНТ. АБОНЕНТ персонально отвечает за вред, причиненный его противоправными действиями (лично или иным лицом под его сетевыми реквизитами) интересам и имуществу физических и юридических лиц, нравственным принципам общества и государства.

3.2.6. Использовать Услуги для передачи через сеть информации, не противоречащей действующему российскому или международному законодательству;

3.2.7. Не осуществлять попытки несанкционированного доступа к ресурсам ПРОВАЙДЕРА и к другим системам, доступным через сеть Интернет.

3.2.8. Не использовать Услуги для распространения материалов, носящих оскорбительный характер для других участников сетевого сообщества.

4. ПОРЯДОК РАСЧЕТОВ

4.1. ПРОВАЙДЕР выставляет АБОНЕНТУ счета-фактуры к оплате в течение первых 7 дней следующего месяца. Ежемесячные счета-фактуры за услуги передачи данных и услуг телематических служб сети «Интернет» выписываются в рублях. Счета-фактуры доставляются ПРОВАЙДЕРОМ АБОНЕНТУ по адресу: 693000, г. Южно-Сахалинск, пр-т Коммунистический, д. 33, канцелярия, тел./факс: 8(4242) 45-23-00, E-mail: office@sakhgu.ru.

ПРОВАЙДЕР ежемесячно дублирует АБОНЕНТУ счет-фактуру на оплату Услуг и расшифровку к нему в электронном виде на e-mail sas@sakhgu.ru.

4.2. АБОНЕНТ должен оплатить счет-фактуру в течение 15 (календарных) дней со дня его получения или направить в адрес Провайдера мотивированный отказ от принятия услуги. При оформлении платежного поручения в графе «назначение платежа» обязательна ссылка на номер счет-фактуры, выписанной ПРОВАЙДЕРОМ.

4.3. АБОНЕНТ имеет право вносить авансовые платежи за услуги передачи данных и услуг телематических служб сети «Интернет».

5. ОТВЕТСТВЕННОСТЬ СТОРОН

5.1. За неисполнение или ненадлежащее исполнение обязательств, предусмотренных Договором, Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации.

5.2. За каждый факт неисполнения или ненадлежащего исполнения ПРОВАЙДЕРОМ обязательств, предусмотренных договором, за исключением просрочки исполнения обязательств (в том числе гарантийного обязательства), предусмотренных договором, размер штрафа устанавливается в виде фиксированной суммы – 10% цены договора (Постановление № 1042 от 30.08.2017).

5.3. Пеня начисляется за каждый день просрочки исполнения ПРОВАЙДЕРОМ обязательства, предусмотренного договором, в размере одной трехсотой действующей на дату уплаты пени ставки рефинансирования Центрального банка Российской Федерации от цены договора, уменьшенной на сумму, пропорциональную объему обязательств, предусмотренных договором и фактически исполненных ПРОВАЙДЕРОМ.

5.4. Общая сумма начисленной неустойки (штрафов, пени) за неисполнение или ненадлежащее исполнение ПРОВАЙДЕРОМ обязательств, предусмотренных договором, не может превышать цену договора.

5.5. За каждый факт неисполнения АБОНЕНТОМ обязательств, предусмотренных договором, за исключением просрочки исполнения обязательств, предусмотренных договором, размер штрафа устанавливается в виде фиксированной суммы – 1000 (одна тысяча) рублей (Постановление № 1042 от 30.08.2017).

5.6. Общая сумма начисленной неустойки (штрафов, пени) за ненадлежащее исполнение АБОНЕНТОМ обязательств, предусмотренных договором, не может превышать цену договора.

5.7. Сторона освобождается от уплаты неустойки (штрафа, пени), если докажет, что неисполнение или ненадлежащее исполнение обязательства, предусмотренного Договором, произошло вследствие непреодолимой силы или по вине другой стороны.

6.АНТИКОРРУПЦИОННАЯ ОГОВОРКА

6.1.Стороны в рамках исполнения настоящего соглашения обязуются соблюдать требования применимого антикоррупционного законодательства и не предпринимать никаких действий, которые могут нарушить нормы антикоррупционного законодательства или стать причиной такого нарушения другой Стороной, в том числе не требовать, не получать, не предлагать, не санкционировать, не обещать и не совершать незаконные платежи напрямую, через третьих лиц или в качестве посредника, включая (но не ограничиваясь) взятки в денежной или любой иной форме, каким-либо физическим или юридическим лицам, включая (но не ограничиваясь) коммерческим организациям, органам власти и самоуправления, государственным служащим, частным компаниям и их представителям.

6.2.В случае нарушения одной из Сторон изложенных выше антикоррупционных обязательств, другая Сторона вправе в одностороннем порядке приостановить исполнение своих обязательств по настоящему Договору до устранения причин такого нарушения или отказаться от исполнения Договора, направив об этом письменное уведомление.

7. КОНФИДЕНЦИАЛЬНОСТЬ И БЕЗОПАСНОСТЬ

7.1. ПРОВАЙДЕР принимает стандартные в сети Интернет технические и организационные меры по обеспечению конфиденциальности получаемой и отправляемой АБОНЕНТОМ информации. Доступ сотрудников ПРОВАЙДЕРА к такой информации разрешается исключительно с целью технического обеспечения предоставляемых услуг, либо в случаях получения претензий со стороны третьих лиц о злонамеренных действиях АБОНЕНТА (распространение программных вирусов, рекламных писем, материалов оскорбительного характера, использование сети Интернет с целью мошенничества и т.п.). Техническую возможность доступа к информации имеют только специально подготовленные сотрудники ПРОВАЙДЕРА, которые несут персональную ответственность за разглашение информации Абонента.

7.2. Информация о передаваемых сообщениях по сети связи ПРОВАЙДЕРА, а также сами эти сообщения могут выдаваться только отправителям и адресатам или их законным представителям. Ознакомление с сообщениями,

получение сведений о них, а также иные ограничения тайны связи допускаются только на основании действующего законодательства Российской Федерации.

8. ОБСТОЯТЕЛЬСТВА, ИСКЛЮЧАЮЩИЕ ОТВЕТСТВЕННОСТЬ

8.1. Ни одна из сторон не несет ответственности за задержку или невыполнение обязательств по настоящему Договору, если они вызваны обстоятельствами, исключающими ответственность.

8.2. Обстоятельствами, исключающими ответственность, являются: Указы, Постановления или письменные указания правительственного органа, комитета или организации, под юрисдикцией которого находится деятельность договаривающихся сторон; любое восстание, мятеж, пожар, наводнение или другие стихийные бедствия; или любая другая причина, неподвластная воздействию Стороны, затронутой этими обстоятельствами.

8.3. Сторона, подвергшаяся воздействию обстоятельств, исключающих ответственность должна немедленно сообщить об этом другой стороне в письменной форме.

8.4. Если воздействие обстоятельств, исключающих ответственность продлится более трех месяцев, любая из сторон имеет право расторгнуть настоящий Договор в одностороннем порядке без возмещения ущерба другой Стороне.

9. СРОК ДЕЙСТВИЯ ДОГОВОРА

9.1. Настоящий Договор вступает в законную силу с момента подписания и распространяет свои правоотношения возникшие с 01.01.2025 и действует по «31» декабря 2025 г. В части расчётов – до полного исполнения Сторонами своих обязательств.

10. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

10.1. Права и обязанности по настоящему Договору не подлежат передаче третьим лицам.

10.2. Все дополнения и изменения настоящего Договора действительны лишь при условии, если они совершены в письменной форме и подписаны уполномоченными на, то лицами.

10.3. Настоящий Договор составлен в форме электронного документа и подписывается электронной цифровой подписью.

10.4. Расторжение настоящего Договора допускается по соглашению сторон, по решению суда, в случае одностороннего отказа стороны Договора от исполнения Договора в соответствии с гражданским законодательством. АБОНЕНТ вправе принять решение об одностороннем расторжении Договора по основаниям, предусмотренным гражданским законодательством для одностороннего отказа от исполнения отдельных видов обязательств.

10.5. Во всем остальном, что не урегулировано настоящим Договором, стороны руководствуются действующим законодательством РФ.

10.6. К Договору прилагаются и являются его неотъемлемой частью следующие документы:

Приложение № 1 – Техническое задание.

11. ЮРИДИЧЕСКИЕ АДРЕСА СТОРОН

АБОНЕНТ
ФГБОУ ВО «СахГУ»
Юридический адрес: 693008, г. Южно-Сахалинск,
ул. Ленина, д.290, тел./факс: 8(4242) 45-23-50
Почтовый адрес: 693000 г. Южно-Сахалинск,
пр. Коммунистический, д.33, тел./факс: 8(4242) 45-23-00
E-mail: rector@sakhgu.ru
ОГРН 1026500534720 ОКПО 48714232
ИНН 6500005706 КПП 650101001
УФК по Сахалинской области (СахГУ л/с 20616U92860)
Банк: отделение Южно-Сахалинск Банк России//УФК
по Сахалинской области г. Южно-Сахалинск
Р/счет 03214643000000016100
К/счет 40102810845370000053
БИК 016401800

Врио ректора

_____/Шмерецкий А.А./

М.П.

ПРОВАЙДЕР
ПАО «МТС»
109147, Москва, Марксистская ул., д. 4
ИНН: 7740000076 КПП 650102001
Р/с: 40822810000000000008
ПАО «МТС-Банк»
г. Москва
БИК: 044525232
К/с: 30101810600000000232

Начальник отдела по работе с корпоративными клиентами

_____/Борисенко О.И. /

М.п.

Приложение № 1
к Договору № 5-2025
от «24» 01 2025 года

Техническое задание на оказание услуг
телематических служб сети «Интернет»

1. Предметом настоящего технического задания является право заключения государственного контракта на оказание услуг телематических служб сети «Интернет» по выделенной линии с 01 января 2025 года по 31 декабря 2025 года для государственных нужд ФГБОУ ВО Сахалинский государственный университет.

В техническом задании определены требования к техническим характеристикам сети, требования к функциональным характеристикам используемого оборудования, требования к безопасности, требования к результатам работ и иные показатели, связанные с определением соответствия создаваемых компьютерных систем, выполняемых работ, оказываемых услуг потребностям заказчика.

2. Стоимость контракта 1980000 (один миллион девятьсот восемьдесят) рублей, с учетом НДС 20%.

3. Цена включает в себя:

- входящий и исходящий трафик;
- поддерживание статических IP-адресов;
- предоставление в пользовании абонентских линий, организуемых оператором для предоставления доступа;
- предоставление в пользование резервных каналов.
- предоставление в пользование оконечного и транзитного оборудования для доступа в сеть Интернет;
- предоставление в пользование оконечного и транзитного оборудования для организации доступа Free Wi-Fi;
- расходы на систему авторизации в зоне доступа Free Wi-Fi
- расходы на первоначальное подключение, включая приёмосдаточные испытания, устранение возникающих проблем;
- налоги, страховку, иные сборы и платежи, связанные с исполнением Контракта, в соответствии с действующим законодательством РФ.

При неработающем канале связи должен производиться перерасчет абонентской платы.

4. **Место, условия и сроки выполнения работ** – г. Южно-Сахалинск, ул. Ленина 290, ФГБОУ ВО «Сахалинский государственный университет».

Услуги оказываются с момента подписания контракта по 31 декабря 2025 г.

В течение 5 календарных дней после подписания Контракта Исполнитель должен организовать каналы связи к оборудованию узлов связи Единой корпоративной сети передачи данных ФГБОУ ВО «Сахалинский государственный университет» с указанными в техническом задании характеристиками:

5. Технические требования на абонентские линии организуемые оператором для предоставления доступа

4.1 Гарантированная симметричная полоса пропускания Интернет-канала Исполнитель - ФГБОУ ВО «Сахалинский государственный университет» (ул. Пограничная, 68 (корпус № 2), точка входа - кабинет № 216 «А» (серверная)) – не менее **512 Мбит/с**; Физическая среда канала – оптоволоконная линия;

4.2 Объём общего входящего и исходящего трафика, включенного в ежемесячную базовую плату неограничен.;

4.3 Исполнитель должен обеспечить использование существующих у Заказчика IP v.4 адресов и прилагает для этого все меры. В исключительном случае, когда Исполнитель не в состоянии сохранить существующие адреса, ему предоставляется возможность выделения Заказчику не менее 14 реальных IP v.4 адресов из адресного пространства Провайдера, смежных, находящихся в одной подсети с префиксом не более 24.

4.4 Исполнитель должен гарантировать, что ни один из выделяемых адресов не содержится в «черных» списках интернет (internet blacklists and spam databases) и выполняет все работы, связанные с проверкой данного факта. Заказчик производит проверку адресов выделяемых подсетей, кроме уже используемых Заказчиком, на их отсутствие в «черных» списках интернет до принятия решения о заключении Договора с Исполнителем.

4.5 Исполнитель должен предоставить Заказчику адреса не менее двух DNS серверов и обеспечить их бесперебойную работу.

4.6 Для обеспечения высокой доступности Услуг, Исполнитель организовывает систему мониторинга трафика и подсистему защиты от DDOS атак, включающую анализ входящего трафика Заказчика на выделенную подсеть IP адресов, соответствующую следующим требованиям:

- Подсистема должна обеспечивать защиту от всего спектра атак вида «отказ в обслуживании», направленных как на исчерпание канальной емкости, так и на исчерпание ресурсов прикладной системы;
- Подсистема должна сохранять функциональность и инфраструктуру телекоммуникационной сети Заказчика, находящейся на момент разработки настоящего ТЗ в эксплуатации. Обеспечение возможности фильтрации вредоносного трафика и защиты не должно зависеть от физического расположения компонентов веб-инфраструктуры заказчика;

- Подсистема должна поддерживать возможность фильтровать зашифрованный трафик (HTTPS) сайта на всех уровнях сети, включая прикладной, без предоставления закрытых ключей шифрования;
- Подсистема должна поддерживать возможность работы с зашифрованным трафиком (HTTPS) сайта, включая:
  - фильтрация HTTPS-трафика на всех уровнях сети, включая прикладной, с использованием предоставляемых клиентом закрытых ключей шифрования;
  - фильтрация HTTPS-трафика на всех уровнях сети, включая прикладной, без предоставления закрытых ключей шифрования, на основе анализа журналов доступа защищаемой системы;
  - анализ и защита сервиса на транспортном и сетевом уровне (протоколы IP, TCP и т. д.);
- Подсистема должна поддерживать возможность импорта информации о подозрительных IP-адресах, подлежащих блокировке, посредством протокола syslog от систем управления событиями информационной безопасности (SIEM), обслуживающих сетевую инфраструктуру Заказчика.
- Подсистема должна поддерживать возможность немедленной блокировки подозрительного IP-адреса по особому HTTP-коду ответа сервера Заказчика как в раскрытом HTTP и HTTPS-трафике, так и зашифрованном HTTPS-трафике на основе анализа журналов доступа.
- Подсистема должна обладать собственным номером автономной системы (AS) и собственными IP-сетями для фильтрации и перенаправления трафика;
- Подсистема должна предоставлять возможность подключения посредством установления BGP-сессий между автономной системой (AS) Заказчика и своей AS в каждой точке присоединения и анонса любого подмножества сетевых префиксов Заказчика размерностью не менее /24.
- Подсистема должна быть в состоянии обрабатывать трафик защищаемого ресурса единовременно на не менее чем двух центрах очистки трафика, расположенных на территории Российской Федерации и использующих для этой цели не менее чем трёх различных поставщиков услуг связи.
- Подсистема должна осуществлять обработку и фильтрацию трафика без непосредственного подключения к точкам обмена трафиком (Internet Exchange);
- Подсистема должна функционировать без вмешательства во взаимодействие пользователя и веб-приложения;
- Подсистема должна поддерживать функциональность мониторинга IP-сетей на предмет утечек BGP-маршрутов и угона IP-префиксов;
- Подсистема должна поддерживать функциональность мониторинга IP-сетей на предмет наличия серверов, уязвимых к атакам типа amplification;
- Подсистема должна иметь возможность предоставить IP-адреса из своего адресного пространства в количестве не менее 128 шт.;
- Подсистема должна поддерживать возможность осуществления HTTP redirect;
- Подсистема должна поддерживать предоставление программного интерфейса (API) для управления доступом к ресурсу на основе «чёрных» и «белых» списков IP-адресов, получения статистики работы защищаемого ресурса;
- Подсистема должна поддерживать возможность использования совместно с системами кеширования статического контента сайта (CDN);
- Подсистема должна предоставлять возможности по защите DNS-серверов от DDoS-атак следующими методами:
  - с размещением доменной зоны Заказчика на собственном распределенном DNS-сервере, функционирующем на всех центрах очистки Подсистемы. Сервер должен уметь принимать файл зоны от DNS-сервера Заказчика.
  - с предоставлением распределенного DNS-сервера, функционирующего на всех центрах очистки Подсистемы, в качестве DNS-рекурсора, кэширующего данные о подключенной доменной зоне Заказчика.
- Подсистема должна поддерживать возможность балансировки нагрузки между серверами защищаемого веб-приложения по алгоритмам primary-backup, round-robin, iphash, а также в определённых пропорциях;
- Подсистема должна поддерживать возможность осуществлять автоматическое перераспределение нагрузки между защищаемыми серверами веб-приложения в случае отказа на стороне заказчика, если доступен хотя бы один из серверов;
- Подсистема должна иметь функционал формирования отчетов о произошедших инцидентах безопасности, включающих в себя данные о количестве и составе заблокированных ip-адресов, тип атаки и ее показатели;
- Подсистема должна иметь функционал формирования ежемесячных отчетов о предоставленном сервисе и уровне его качества;
- Подсистема должна поддерживать возможность установки как выделенного канала (MPLS L2 VPN или физическое сетевое подключение) между центрами очистки трафика и интернет-инфраструктурой заказчика, при этом в случае физического сетевого подключения система должна поддерживать возможность установления подключения по стандарту интерфейса 100 гигабит/с.;
- Подсистема должна поддерживать возможность установки туннельных инкапсулирующих соединений (IP-in-IP, GRE) между центрами очистки трафика и интернет-инфраструктурой заказчика;
- Подсистема должна поддерживать приём и передачу трафика (как входящего, так и исходящего) с использованием вышеуказанных каналов и тоннельных соединений в любом формате подключения;
- Подсистема должна производить постоянный анализ пользовательского трафика как в случае наличия атаки, так и при ее отсутствии;

- В системе должен быть реализован сбор статистики в реальном времени со средним (за неделю) интервалом не более 5 минут и предоставление ее в виде графиков в персональном кабинете пользователя и в виде программного интерфейса (API);
- Подсистема должна поддерживать горизонтальное масштабирование точек фильтрации для увеличения пропускной способности сети;
- Подсистема должна поддерживать возможность защиты не менее 10 ЦОД и не менее 256 сервисов клиента;
- Классификация запросов пользователей к защищаемому сервису в системе должна осуществляться на основе поведенческого анализа, моделирования взаимодействия легитимных пользователей с защищаемым ресурсом и генерации сценариев их поведения;
- Блокирование запросов в системе должно производиться только в случае возникновения проблем у защищаемого ресурса (увеличение времени отклика, рост числа HTTP-ошибок, исчерпание доступной для защищаемого ресурса полосы пропускания);
- Подсистема должна реализовывать следующие методы для обнаружения и фильтрации трафика DDoS-атак в зависимости от их направленности, указанные в таблице 1.

Таблица 1. Методы обнаружения и устранения атак

Класс атак	Примеры	Методы обнаружения	Методы защиты
Атаки на исчерпание канальной емкости	IP flood, IP fragment flood, DNS/NTP/ SNMP/LDAP Amplification	Статистический анализ трафика	Выявление вектора атаки, фильтрация наиболее близко к источнику атаки, распыление трафика атаки по узлам сети фильтрации
Атаки на стек TCP/IP	SYN/ACK Flood, Sockstress, TCP Connection Flood	Статистический анализ трафика, инспекция заголовков TCP, возможность отвечать на каждую попытку соединения без потери производительности	SYN Cookies, SYN Proxy
Атаки прикладного уровня	HTTP/HTTPS Flood, генерация нагрузки HTTPS handshake запросами, медленная отдача заголовков в рамках 1 запроса, эксплойт узких мест веб-приложения таргетированными запросами	Анализ и классификация поведения пользователей, корреляционный анализ, мониторинг доступности защищаемого приложения	Динамическая фильтрация на основе поведения пользователей, объемов rps/pps, управление черными/белыми списками в реальном времени

- Подсистема должна иметь возможность сбора и отображения статистики:
  - общий объем входящего трафика (Мбит/с, пакетов/с),
  - объем легитимного входящего трафика (Мбит/с, пакетов/с),
  - объем исходящего трафика (Мбит/с),
  - количество входящих HTTP-запросов,
  - скорость работы защищаемого HTTP-ресурса,
  - количество HTTP-ошибок,
  - динамику списка заблокированных IP-адресов,
  - географическое распределение списка заблокированных IP-адресов,
  - прочие параметры работы ресурса -- по запросу,
  - ежемесячное формирование отчетов об инцидентах;
- Подсистема должна осуществлять мониторинг и оповещение по SMS и электронной почте о проблемах с защищаемыми ресурсами.

4.7 Исполнитель должен предоставить Заказчику прямые «темные» оптические волокна по следующим маршрутам:

- ул. Пограничная, 68 (**корпус № 2**, точка входа - серверная, каб. № 216«А») – ул. Ленина, 290 (**корпус №1**, точка входа - серверная, каб. № 37);

- ул. Пограничная, 68 (**корпус № 2**, точка входа - серверная, каб. № 216 «А») – ул. Ленина, 296 (**корпус № 6**, точка входа - компьютерный класс № 413);
- ул. Пограничная, 68 (**корпус № 2**, точка входа - серверная, каб. № 216 «А») – ул. Ленина, 284 (**ЮСПК, точка входа – кабинет №113**);_
- ул. Пограничная, 68 (корпус № 2, точка входа - серверная, каб. № 216«А») – ул. Ленина, 288 (корпус № 5, точка входа - каб. № 402);
- ул. Пограничная, 68 (**корпус № 2**, точка входа - серверная, каб. № 216«А») –ул. Пограничная, 2 (**ТНИ, серверная каб №201**);
- ул. Пограничная, 68 (**корпус № 2**, точка входа - серверная, каб. № 216 «А») – ул. Горького, 26 (**корпус ПТК, точка входа – серверная**);
- ул. Пограничная, 68 (**корпус № 2**, точка входа - серверная, каб. № 216 «А») – ул. Пограничная, 70 (**археологический музей**);
- ул. Пограничная, 68 (**корпус № 2**, точка входа - серверная, каб. № 216 «А») – Коммунистический проспект, 33 (**корпус № 4**, точка входа - серверная, каб. № 23);
- ул. Пограничная, 68 (**корпус № 2**, точка входа - серверная, каб. № 216 «А») – ул. Крюкова, 171 «А» (**научная библиотека**);
- ул. Пограничная, 68 (**корпус № 2**, точка входа - серверная, каб. № 216 «А») – ул. Ленина, 282 (**общежитие ЮСПК, точка входа библиотека**);
- ул. Горького, 26 - пр. Победы, 25-А;
- ул. Горького, 26 - ул. Горького, 30;
- ул. Горького, 26 – ул. Горького, 30 «А» (**общежитие ПТК**);
- ул. Пограничная, 68 (корпус № 2, точка входа - серверная, каб. № 217 «А») – ул. Крюкова, 167 (**общежитие № 3**);
- ул. Пограничная, 68 (корпус № 2, точка входа - серверная, каб. № 217 «А») – ул. Пограничная, 70 (общежитие, точка входа – кабинет 101);
- ул. Пограничная, 68 (корпус № 2, точка входа - серверная, каб. № 216 «А») – ул. Пограничная 68/1 (ЮСНИС);
- ул. Пограничная, 68 (корпус № 2, точка входа - серверная, каб. № 216 «А») – ул. Леонова, 38 (первый этаж. Приемная комиссия)
- ул. Пограничная, 68 (корпус № 2, точка входа - серверная, каб. № 216 «А») – ул. М.А. Горького, 25 (3 этаж, лаборатории восточного водородного кластера)

4.8 Оптические волокна, соединяющие все маршруты, должны быть окончены в коммутационных шкафах Заказчика с использованием оптических портов SC/UPC и размещены в 19-дюймовые оптические кроссы.

4.9 По адресам ул. Пограничная 68 и ул. Горького 26 все оконченные оптические порты должны быть расположены в едином оптическом кроссе в коммутационном шкафу Заказчика. В объединенный оптический кросс заводится не более двух кабелей (объединение выполняется на стороне Исполнителя).

4.10 Конструкция оптических кроссов должна предусматривать легкий доступ для ремонтно-восстановительных работ. Каждый оптический порт должен быть разборчиво промаркирован с целью его однозначной идентификации с адресом конечной точки маршрута которую он соединяет.

4.11 Каналы должны быть организованы без использования IP-VPN и маршрутизации L2.

4.12 Используемые для предоставления услуги технические решения должны:

- обеспечить для взаимодействия стандартизованные интерфейсы и поддерживать стандартизованные протоколы для обмена данными;
- обеспечить пользование базовыми сетевыми сервисами – доступ к веб - сервисам (протокол HTTP), электронная почта (протокол SMTP, POP3), обмен файлами (протокол FTP), управление и контроль сетевых устройств;

5. Резервирование

5.1 Гарантированная симметричная полоса пропускания резервного Интернет-канала Исполнитель - ФГБОУ ВО «Сахалинский государственный университет» (ул. Пограничная, 68 (корпус № 2), точка входа - кабинет № 216 «А» (серверная)) – не менее 100.0 Мбит/с. Переход на резервный канал осуществляется с сохранением плана адресации сети университета;

5.2 Гарантированная симметричная полоса пропускания резервного Интернет-канала Исполнитель - ФГБОУ ВО «Сахалинский государственный университет» (Коммунистический проспект, 33 (корпус № 4), точка входа - кабинет № 23 (серверная)) – не менее 100.0 Мбит/с. Переход на резервный канал осуществляется с сохранением плана адресации сети университета;

5.3 Гарантированная симметричная полоса пропускания резервного канала ул. Пограничная, 68 (корпус № 2), точка входа - кабинет № 216 «А» (серверная) - Коммунистический проспект, 33 (корпус № 4, точка входа - серверная, каб. № 23); не менее 50.0 Мбит/с.

5.4 Гарантированная симметричная полоса пропускания резервного канала ул. Пограничная, 68 (корпус № 2), точка входа - кабинет № 216 «А» (серверная) - ул. Горького, 26 (корпус ПТК, точка входа - серверная); не менее 50.0 Мбит/с.

5.5 Для организации резервного канала должны использоваться раздельные линии доступа, проходящие по независимым физическим маршрутам, то есть не имеющие общих точек отказа.

5.6 Резервные каналы должны быть организованы без использования IP-VPN и маршрутизации L2.

6. Технические требования оказания услуг по организации зон доступа Free Wi-Fi

6.1 Wi-Fi сеть должна представлять из себя законченное техническое решение с централизованным управлением и мониторингом. Система мониторинга и управления Wi-Fi сети должна обеспечивать централизованное управление и мониторинг беспроводной сети, а также поддерживать возможность настройки беспроводных точек доступа.

6.2 Гарантированная симметричная полоса пропускания Wi Fi канала – не менее 100 Мбит/с;

6.3 Сеть абонентского радиодоступа Исполнителя должна быть построена на радиооборудовании стандарта IEEE 802.11.

6.4 Для обеспечения электропитания точки доступа должен использоваться технология, позволяющая передавать удалённому устройству электрическую энергию вместе с данными через стандартную витую пару в сети Ethernet (POE).

6.5 Исполнитель обязан обеспечить требование системы технических средств для обеспечения функций оперативно - розыскных мероприятий

6.6 Предоставление пользователям доступа к сети Интернет по адресам:

- общежитие № 3 ФГБОУ ВО СахГУ - г. Южно-Сахалинск, ул. Крюкова, д. 167 (в настоящее время общежитие закрыто на капитальный ремонт, доступ потребуется организовать в течении 21 дня после получения письма уведомления от ФГБОУ ВО СахГУ»;
- общежитие № 4 ФГБОУ ВО СахГУ - г. Южно-Сахалинск, ул. Пограничная, д. 70;
- учебный корпус №4 ФГБОУ ВО СахГУ: коридор 2 и 3 этаж, холл 1 этаж, малый актовый зал, большой актовый зал - Южно-Сахалинск, Коммунистический проспект 33;
- учебный корпус №2 ФГБОУ ВО СахГУ: кабинеты № 214 - № 218, читальный зал (2 этаж), холл 1 этаж - г. Южно-Сахалинск, ул. Пограничная, д. 68;
- учебный корпус №1 ФГБОУ ВО СахГУ: 1 этаж холл - ул. Ленина 290;
- учебный корпус №6 ФГБОУ ВО СахГУ, читальный зал - ул. Ленина 296;
- учебный корпус №9 ФГБОУ ВО СахГУ, читальный зал библиотека - ул. Пограничная 2;
- учебный корпус ПТК ФГБОУ ВО СахГУ, холл (полное покрытие), читальный зал библиотека – ул. Горького 26;
- учебный корпус ЮСПК ФГБОУ ВО СахГУ, холл 1 этаж - ул. Ленина 284;
- Приемная комиссия СахГУ, ул. Леонова, 38 первый этаж;
- Лаборатории СахГУ, ул. Леонова 38, третий, четвертый этаж;
- Лаборатории ВВК, ул. Горького, 25 3 этаж(галерея).

6.7 Исполнитель должен выполнить установку оборудования Wi-Fi (точек доступа), включая монтаж и прокладку коммуникаций. Расходы на необходимое оборудование, прокладку коммуникаций до места монтажа точек доступа Wi-Fi, монтаж и настройку точек доступа Wi-Fi, а также все иные расходы, связанные с организацией доступа к сети Интернет по технологии Wi-Fi, с его обслуживанием и ремонтом на объектах заказчика, входят в стоимость государственного контракта на оказание услуг телематических служб сети «Интернет» и не подлежат дополнительной оплате со стороны Заказчика.

6.8 Исполнитель должен обеспечить наличие резервного оборудования на случай его замены при выходе из строя в количестве не менее 5 % каждой используемой номенклатуры.

6.9 Исполнитель должен обеспечить предоставление услуги доступа к сети Интернет по технологии Wi-Fi и техническую поддержку данной услуги. Служба технической поддержки должна регистрировать все происходящие события и обращения, относящиеся к работе беспроводной сети передачи данных.

6.10 При развертывании Wi-Fi сети Исполнитель должен обеспечить однородное покрытие в диапазонах 2.4 ГГц и 5 ГГц с уровнем сигнала достаточным для выполнения требований по пропускной способности. Уровень сигнала в зонах необходимого покрытия по адресам приведённых в приложении № 1 к данному техническому заданию должен составлять не менее - 80 dBm.

6.11 Исполнитель организует и регистрирует SSID с названием, предоставленным Заказчиком.

7. Требования к системе авторизации при оказании услуг по организации зон доступа Free Wi-Fi

7.1 Авторизация пользователей в беспроводной сети должна выполняться в соответствии с правилами авторизации доступа пользователей публичной зоны Wi-Fi предусмотренными действующим законодательством Российской Федерации (Федеральный закон от 07.07.2003 N 126-ФЗ, Постановление Правительства РФ № 758 от 31 июля 2014 г., Постановление Правительства РФ № 801 от 12 августа 2014 г.)

7.2 Исполнитель обеспечивает возможность web-авторизация по логину и паролю.

7.3 Исполнитель размещает брендированную web-страницу, согласованную с Заказчиком, и использует ее как стартовую для доступа к сети.

7.4 Исполнитель организует SMS-регистрацию пользователей в собственной сертифицированной билинговой системе с последующей передачей индивидуального логина и пароля для доступа к сети Интернет.

7.5 Исполнитель обеспечивает отправку пользователям SMS-сообщений с авторотационными данными в период не превышающий 5 минут с момента отправки пользователем SMS-запроса.

7.6 Пользовательская часть сервиса авторизации должна состоять из следующих веб-страниц:

а) Страница для аутентификации пользователей, которая содержит:

• текст с предложением пройти аутентификацию для получения доступа,

• поле для ввода номера телефона (в данное поле можно вводить только цифры, другие символы игнорируются при вводе, пользователю при этом показывается уведомление о вводе недопустимых символов до момента ввода допустимых. Поле не может быть пустым, до его заполнения минимально необходимым количеством цифр (цифр) кнопка «Получить пароль по СМС» неактивна.

• Кнопку «Получить пароль по СМС», которая становится активной после ввода номера телефона. При нажатии на данную кнопку пользователю высылается СМС с паролем для подтверждения идентификации. Для формирования пароля нужно формировать только цифры. После подтверждения от сервера подтверждения отправки СМС осуществляется переход на страницу авторизации. Если сервер вместо подтверждения отправки СМС вернул ошибку, то ее текст выводится на данном экране между полем для ввода телефона и кнопкой «Получить пароль по СМС»

• Текст «Нажав кнопку «Получить пароль по СМС» Вы соглашаетесь с условиями использования» (является ссылкой на экран условий использования). В ходе реализации к данному тексту может быть добавлен элемент управления «флажок», до переключения которого из неактивного в активное состояние кнопка «Получить пароль по СМС» так же должна быть неактивна. О принятии такого решения будет сообщено дополнительно.

• Текст с предложением ввести полученный проверочный код, содержащийся в присланном СМС

• Поле для ввода пароля из СМС. Поле обязательно для заполнения, до его заполнения кнопка «Войти в Интернет» неактивна.

• После нажатия на кнопку «Войти в Интернет». в случае успешной аутентификации пользователь автоматически авторизуется, получает доступ в Интернет. В случае возникновения ошибки на этом шаге, пользователю выводится соответствующее сообщение. Данная форма должна иметь защиту от подбора пароля и после 9 попыток неправильно введенных паролей с одного устройства на время блокировать для него возможность подключения, выводя соответствующее уведомление.

• Кнопку «Выслать повторно», после нажатия на которую, сервер повторяет отправку СМС с паролем.

• Ссылку «Вернуться к вводу телефона» для возвращения на страницу идентификации с возможностью изменить номер телефона.

Если аутентификация прошла успешно пользователь получает доступ в Интернет

б) **Страница с условиями использования** содержит текст условий использования от поставщика Wi-Fi-решения в соответствии с российским законодательством, предусматривающим обязательную идентификацию пользователей публичных Wi-Fi-сетей, и кнопку «Вернуться назад», ведущую на предыдущую страницу. При возврате данные, введенные пользователем на предыдущей странице, должны быть сохранены.

7.7 Пользовательский интерфейс сервиса авторизации должен быть выполнен в едином дизайне для университета или оператора. Дизайн предоставляется исполнителем или заказчиком. Интерфейс должен быть реализован на русском языке.

7.8 Поставщик Wi-Fi решения должен самостоятельно подготовить текст страницы с условиями использования, а также тексты всех сообщений об ошибках и системных уведомлений.

7.9 Все системные уведомления и все сообщения об ошибках должны быть приведены к виду удобному для понимания конечными пользователями и содержать точные инструкции по решению проблемы.

7.10 Все информационное наполнение, все системные уведомления и сообщения об ошибках должны выводиться на русском языке.

8. Требования к наличию защиты доступа к ресурсам сети Интернет при организации зон доступа Free Wi-Fi

8.1 Исполнитель самостоятельно обеспечивает техническую возможность на аппаратно-программном уровне исключения доступа к ресурсам, несовместимым с задачами образования обучающихся и обеспечивает возможность доступа к сетевым фильтрам сервера (серверов) контентной фильтрации в соответствии с Федеральным законом от 29 декабря 2010 г. N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию".

8.2 Исполнитель обеспечивает фильтрацию трафика от веб-узлов, расположенных в сети Интернет (далее - контентная фильтрация), в учреждении в соответствии со следующими требованиями:

• выполнение требований ФЗ № 436 «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.10 с учетом ФЗ № 139 «О внесении изменений в федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 28.07.12 г. в части фильтрации Интернет-трафика;

• блокировка Интернет-ресурсов из Единого реестра доменных имён, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию,

распространение которой в Российской Федерации запрещено, формируемого Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций;

- блокировка Интернет-ресурсов из Федерального списка экстремистских материалов, формируемого Министерством юстиции Российской Федерации на основании статьи 13 Федерального закона от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности», пунктом 7 Положения о Министерстве юстиции Российской Федерации, утвержденного Указом Президента Российской Федерации от 13.10.2004 № 1313;
- Правила подключения общеобразовательных учреждений к единой системе контент- фильтрации доступа к сети Интернет, реализованной Министерством образования и науки Российской Федерации от 11.05.2011 г. № АФ-12/07вн

.

9. Общие требования к исполнителю

9.1 Исполнитель должен иметь следующие действующие лицензии (в том числе на все время предоставления Услуг) на осуществление деятельности в области оказания услуг связи с местом действия на территории Российской Федерации, на которой располагаются объекты заказчика (в соответствии с п. 36 ч. 1 ст. 12 Федерального закона от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности»), со следующими внесенными наименованиями услуг связи, утвержденными постановлением Правительства РФ от 18.02.2005 № 87 «Об утверждении перечня наименований услуг связи, вносимых в лицензии и перечней лицензионных условий»:

- Услуги связи по предоставлению каналов связи;
- Услуги связи по передаче данных, за исключением услуг связи по передаче данных для целей передачи голосовой информации;
- телематические услуги связи и на услуги связи по передаче данных.
- Наличие разрешений на использование радиочастот и радиочастотных каналов в сети беспроводного доступа в радиусе действия перечня объектов (приложение №1) в диапазоне частот 2.4 ГГц и 5 ГГц.

10. Перечень дополнительных условий:

10.1 Услуги связи должны соответствовать по качеству действующим стандартам, техническим нормам и правилам, 24 часа в сутки, 7 дней в неделю, без перерывов, за исключением времени, необходимого для проведения профилактических и/или регламентных работ.

10.2 При проведении профилактических и/или регламентных работ уведомить не менее чем за 24 часа до начала их проведения. О чем предупреждать по электронной почте на адрес chernolivskiy_av@sakhgu.ru . И планировать их на время, когда это может нанести наименьший ущерб Заказчику;

10.3 Исполнитель должен обеспечить предоставление технических консультаций Заказчику в рабочие дни с 9 до 22 часов по круглосуточному выделенному телефону.

10.4 Исполнитель должен иметь ремонтно-восстановительной службу;

10.5 Исполнитель должен выделить Заказчику персонального менеджера на время оказания услуг.

10.6 Исполнитель должен соблюдать тайну связи в соответствии с законодательством РФ.

10.7 Исполнитель должен подтвердить наличие минимум 2-х независимых каналов к провайдерам верхнего уровня, не учитывая каналов местного уровня;

10.8 Исполнитель должен предоставить круглосуточный доступ к статистике потребления услуг, включающий в себя доступ к информации об использовании основного и резервного Интернет-канала в виде графиков загрузки канала и статистики по ежедневно потребляемому трафику;

10.9 Исполнитель должен предоставить круглосуточный доступ к сервису сбора и анализа статистики с правами, позволяющими просматривать всю статистическую и аналитическую информацию по использования free Wi-Fi. Система сбора статистики должна предоставлять возможность отслеживать в режиме реального времени и выводить показатели в виде графиков. График должен отображать следующие показатели:

- Количество устройств, подключенных в настоящий момент к интернету через Wi-Fi.
- Потребление интернет-трафика на текущий момент (с разделением на входящий и исходящий трафик)
- суммарное количество уникальных устройств, подключившихся к сети Wi-Fi за произвольный период
- суммарный объем потребленного интернет-трафика за произвольный период (с разделением на входящий и исходящий трафик)

10.10 Все статистические данные должны храниться и быть в доступе для использования в течение 3 календарных месяцев.

10.11 Все отчеты должны быть доступны для экспорта в формате MS Excel и PDF.

10.12 Статистические отчеты по умолчанию должны формироваться за полные сутки дня (далее - Отчетный период). Также должна быть возможность задать период отчетности вручную.

10.13 Исполнитель должен предоставить схему расположения вышеперечисленных маршрутов каналов связи между корпусами университета. При приемосдаточных работах необходимо провести измерения всех смонтированных волокон в двух направлениях методом вносимых потерь на длинах двух длинах волн 1310 и 1550 нм. Протоколы измерений должны быть предоставлены Заказчику в виде таблиц и графиков с указанием конечных адресов маршрутов и их характеристик (расстояние, вносимые потери, затухание, суммарные потери).

10.14 В случае использования беспроводное подключение по технологии WiMAX должно регламентироваться Правилами применения оборудования радиодоступа для беспроводной передачи данных часть 1, Приказ № 19 от 13.02.2007 г. Министерства информационных технологий и связи Российской Федерации.

11. Требования к действиям в аварийных ситуациях

11.1 Исполнитель должен приступать к устранению любых недостатков Услуг в течение 3 (трех) часов в период с 09 ч. 00 мин. до 18 ч. 00 мин. и в течение 4 (четырех) часов в период с 18 ч. 00 мин. до 09 ч. 00 мин. в рабочие дни, а также в выходные и праздничные дни с момента получения заявки от Заказчика.

11.2 Заявка Заказчика может быть передана Исполнителю в устной форме, в письменной форме электронной почтой. Заявка Заказчика должна быть зарегистрирована, а Исполнитель должен сообщить Заказчику регистрационный номер заявки.

12. Порядок проведения подготовительных работ

12.1 Допуск сотрудников Исполнителя для выполнения работ в рамках данного технического задания на объекты Заказчика будет возможен только после заключения Договора.

12.2 Место проведения работ должно быть защищено Исполнителем с целью исключения на него доступа посторонних лиц.

12.3 Работы возможно производить в рабочие дни, с 9-00 до 20-00. Исполнитель должен не менее, чем за три дня до начала работ согласовать проведение работ с Заказчиком с предоставление списка сотрудников исполнителя по форме, предоставляемой Заказчиком.

12.4 При проведении работ в серверных помещениях и местах установки коммутационных шкафов не допускать образования пыли, работы проводить с использованием пылесоса. Незамедлительно принимать меры по удалению образовавшейся пыли и мусора. Ежедневно по окончанию работ производить уборку.

12.5 Работы должны быть выполнены с сохранением в первоначальном виде всех неремонтируемых конструктивных частей зданий, домовладений, полов, отделки, имеющихся коммуникационных сетей. В случае невыполнения Исполнителем указанных в настоящем пункте условий, Исполнитель обязан в кратчайшие сроки, согласованные с Заказчиком, восстановить за свой счет поврежденные (разрушенные, испорченные) конструктивные части здания, полы, отделку, дверные полотна (включая окраску их поверхности), остекление оконных рам, имеющиеся коммуникационные сети, асфальтобетонное покрытие, нарушенное при производстве работ по прокладке кабелей.

12.6 Учитывая режимный характер объекта, Исполнитель должен не позднее 3 рабочих дней до начала выполнения работ представить Заказчику для оформления пропусков список персонала, который будет задействован на объекте (включая персонал субподрядчиков), с указанием фамилии, имени, отчества и паспортных данных каждого работника, данных по регистрации в Сахалинской области.

12.7 Все материалы, используемые для проведения работ, должны быть разрешены для применения. На скрытые работы должны быть оформлены соответствующие акты.

12.8 Отключения инженерных систем, сетей или отдельных их участков могут производиться только по предварительному согласованию с Заказчиком.

12.9 При необходимости прокладки дополнительных кабелей по зданию и сооружениям Заказчика, Исполнитель производит согласование со специалистами Заказчика, после чего возможно приступить к работам.

12.10 Исполнитель обязан выполнить работы по радиочастотному планированию с выездом на место и предоставить результаты Заказчику не позднее чем через 5 рабочих дней с момент заключения договора.

12.11 Необходимо провести приемосдаточные испытания не позднее чем на следующий день после строительной готовности объекта. Представители управления информатизации СахГУ должны быть приглашены на приемосдаточные испытания.

Подписи сторон:

АБОНЕНТ
ФГБОУ ВО «СахГУ»
Врио ректора

_____ /Шмерецкий А.А./

М.п.

ПРОВАЙДЕР
ПАО «МТС»
Начальник отдела по работе с корпоративными клиентами

_____ / Борисенко О.И. /