УТВЕРЖДЕНА
приказом государственного автономного
учреждения Республики Коми
«Центр информационных технологий»
от 19.08.2020 № 94
(приложение № 7)

ПОЛИТИКА
информационной безопасности
«Удаленный доступ в ГИТС»

1. Общие положения

1.1. Настоящая политика информационной безопасности «Удаленный доступ в ГИТС» (далее – Политика) определяет обязательные требования к организации удаленного доступа:

– из Интернета к ресурсам ЦТУ;

– из ГИТС к защищенному сегменту ЦТУ;

– из ГИТС к АРМ, находящимся на обслуживании ГАУ РК «ЦИТ», в случае, когда отсутствует прямая маршрутизация до этих АРМ;

– из Интернета к АРМ, находящимся на обслуживании ГАУ РК «ЦИТ».

1.2. Для отдельных случаев может устанавливаться определенный порядок организации удаленного доступа, согласованный с управлением по безопасности ГАУ РК «ЦИТ».

2. Термины и обозначения

АРМ – автоматизированное рабочее место - компьютер, включенный в ЛВС и предоставляющий пользователю доступ к ее ресурсам.

ГАУ РК «ЦИТ» - государственное автономное учреждение Республики Коми «Центр информационных технологий». На основании постановления Правительства Республики Коми от 21 марта 2011 г. № 60 ГАУ РК «ЦИТ» является оператором ГИТС, осуществляющим техническое, организационное управление и эксплуатацию ГИТС.

ГИТС - государственная информационно-телекоммуникационная сеть Республики Коми. Компоненты ГИТС: ЦТУ, базовая ЛВС - ЛВС в зданиях, находящихся по адресам: г. Сыктывкар, ул. Коммунистическая, д. 9 и ул. Коммунистическая, д. 8, выделенные каналы передачи данных, объединяющие ЛВС в других зданиях, в которых расположены пользователи ГИТС.

DMZ ГИТС - демилитаризованная зона ГИТС – сегмент сети, содержащий сетевые узлы с внешними IP ГАУ РК «ЦИТ» (91.227.92.0/22, 46.61.145.0/25).

ИС - информационная система.

Ресурсы ГИТС - вычислительная мощность оборудования и иных средств, составляющих ГИТС (серверов, их дискового пространства, сетевого

периферийного оборудования, сетевых сервисов, массивов информации, программных средств, предоставленных пользователям ГИТС).

СВТ - средство вычислительной техники.

СЗИ от НСД - средство защиты информации от несанкционированного доступа.

СКЗИ – средство криптографической защиты информации.

ЦТУ - центральный телекоммуникационный узел - основное звено ГИТС, интегрирующее ресурсы ГИТС, располагается в помещениях центра обработки данных ГАУ РК «ЦИТ».

Экстренный случай — зарегистрированный в Службе технической поддержки ГАУ РК «ЦИТ» случай выхода находящейся в защищенном сегменте ЦТУ ИС из строя, при котором ее работоспособность невозможно восстановить имеющимися силами ГАУ РК «ЦИТ» и требуется привлечение третьих лиц, и сроки организации защищенного сертифицированными СКЗИ канала к ИС превышают утвержденные ГАУ РК «ЦИТ» сроки допустимого простоя этой ИС.

3. Требования по удаленному доступу

3.1. Удаленный доступ, за исключением доступа из сети Интернет к ресурсам ЦТУ, находящимся в DMZ ГИТС, должен осуществляться только посредством разрешенных систем удаленного доступа в ГИТС. Использование иных систем удаленного доступа запрещено (в частности, VPN-систем, VNC-систем и т.п.).

3.2. Использование систем удаленного доступа с нарушением порядка и условий, закрепленных в Перечне разрешенных систем удаленного доступа в ГИТС (приложение 1), за исключением случая, указанного в пункте 3.4. настоящей Политики, запрещено.

3.3. Доступ из сети Интернет к критичным службам хостов с внешними IP ГАУ РК «ЦИТ» (приложение 2) должен осуществляться только посредством разрешенных систем удаленного доступа в ГИТС. При необходимости осуществления прямого доступа из сети Интернет к таким службам на отдельных хостах допускается исключение из этого правила при условии обязательного предварительного согласования с управлением по безопасности ГАУ РК «ЦИТ» через Службу технической поддержки ГАУ РК «ЦИТ» или в официальном порядке.

3.4. В экстренном случае удаленный доступ к ИС, находящейся в защищенном сегменте ЦТУ, может быть осуществлен без организации канала доступа посредством сертифицированных СКЗИ при соблюдении всех перечисленных ниже условий:

– доступ должен быть согласован с управлением по безопасности ГАУ РК «ЦИТ» и, при необходимости, проводиться при непосредственном участии сотрудника подразделения;

– удаленный доступ к ИС должен осуществляться через АРМ сотрудника ГАУ РК «ЦИТ»[1] (далее — промежуточный АРМ) посредством

[1] Предпочтительно — АРМ администратора ИС.

системы удаленного доступа, указанной в Перечне разрешенных систем удаленного доступа в ГИТС как используемой в экстренном случае;

– канал доступа от промежуточного АРМ до серверов ИС должен быть организован с использованием сертифицированных СКЗИ;

– на промежуточном АРМ должна вестись запись действий, происходящих на экране за все время предоставления доступа, а также сниматься копии всех файлов, загруженных на сервер в ходе работ, указанная запись и файлы передаются в управление по безопасности ГАУ РК «ЦИТ» для анализа;

– привлеченные сотрудники управления по безопасности ГАУ РК «ЦИТ» обязаны осуществлять визуальный контроль проводимых действий с ИС, в частности, пересекать передачу по незащищенному сертифицированными СКЗИ каналу защищаемой в соответствии с законодательством информации (персональных данных и др.).

3.5. При необходимости организации дистанционного режима работы с предоставлением удаленного доступа к ресурсам ЦТУ рекомендуется принятие следующих мер защиты информации:

– для удаленного доступа запрещается использование личных СВТ, в том числе портативных мобильных СВТ;

– организация удаленного доступа с удаленного СВТ к защищенному сегменту ЦТУ должна осуществляться с применением сертифицированных СКЗИ и СЗИ от НСД;

– на удаленные СВТ должны быть установлены сертифицированные средства антивирусной защиты информации;

– на удаленном СВТ должна быть исключена возможность установки работником программного обеспечения, за исключением программного обеспечения, установка и эксплуатация которого определена служебной необходимостью, реализуемое штатными средствами операционной системы удаленного СВТ или сертифицированными СЗИ от НСД;

– должно быть организовано обеспечение мониторинга действий работников удаленных СВТ и ведения журналов регистрации их действий;

– должна быть обеспечена возможность оперативного реагирования и принятия мер защиты информации при возникновении компьютерных инцидентов.

3.6. Дистанционный режим работы с предоставлением удаленного доступа к ресурсам ЦТУ должен быть согласован с управлением по безопасности ГАУ РК «ЦИТ».

3.7. Перечень мер защиты информации, указанный в пункте 3.5. настоящей Политики, может изменяться в зависимости от условий организации дистанционного режима работы по согласованию с управлением по безопасности ГАУ РК «ЦИТ» и с учетом требований и рекомендаций регуляторов в области защиты информации.

Приложение 1
к Политике информационной безопасности
Удаленный доступ в ГИТС

ПЕРЕЧЕНЬ
разрешенных систем удаленного доступа в ГИТС

№ п/п	Наименование	Дополнительная информация, условия	Порядок предоставления
1.	ViPNet Custom	Доступ к любому сегменту ГИТС	Письменный запрос в ГАУ РК «ЦИТ»
2.	Ideco	Шлюз: vpn2.rkomi.ru Доступ к ресурсам ГИТС, не входящим в защищенный сегмент	Письменный запрос в ГАУ РК «ЦИТ»
3.	RMS для доступа к защищенным ресурсам	Шлюз: будет определен после ввода в эксплуатацию Доступ к любому сегменту ГИТС	
4.	RMS для доступа к открытым ресурсам	Шлюз: 91.227.93.63 Доступ к ресурсам ГИТС, не входящим в защищенный сегмент Может использоваться в экстренном случае.[2]	
5.	Резервные VPN-серверы Оператора связи электронного правительства Республики Коми	Шлюз 1 (l2tp): 91.227.92.88, 46.61.145.120 Шлюз 2 (OpenVPN): 91.227.93.39 Доступ к ресурсам ГИТС, не входящим в защищенный сегмент	

[2] Согласно Политике информационной безопасности «Удаленный доступ в ГИТС»

№ п/п	Наименование	Дополнительная информация, условия	Порядок предоставления
6.	VPN-сервер Отдела администрирования инфраструктуры электронного правительства Республики Коми	m.rkomi.ru Доступ к ресурсам ГИТС, не входящим в защищенный сегмент	Доступ только специалистов отдела администрирования электронного правительства Республики Коми

Приложение 2
к Политике информационной безопасности
Удаленный доступ в ГИТС

ПЕРЕЧЕНЬ
критичных служб хостов с внешними IP ГАУ РК «ЦИТ»

Наименование	Дополнительная информация
SSH-сервер.	Служба удаленного администрирования ОС Linux/Unix/BSD. В основном размещается на TCP 22.
RDP-сервер.	Служба удаленного администрирования ОС Windows. В основном размещается на TCP 3389.
Веб-службы администрирования оборудования.	Веб-приложения для администрирования коммутационного оборудования (маршрутизаторы и т.п.).