Приложение

УТВЕРЖДЁН
приказом министерства цифрового развития Белгородской области
от 30.06.2022 **№** 98

Регламент
взаимодействия участников защищённой виртуальной сети ViPNet № 3168 региональной системы межведомственного электронного взаимодействия Белгородской области

1. ТЕРМИНЫ И СОКРАЩЕНИЯ

ViPNet Administrator	Программное обеспечение, предназначенное для конфигурирования и управления виртуальной защищённой сетью ViPNet
ViPNet Client	Программное обеспечение, реализующее на рабочем месте пользователя или сервере функцию VPN-клиента, персонального экрана и клиента защищённой почтовой службы
ViPNet Coordinator	Шлюз безопасности, предназначенный для построения виртуальной сети ViPNet и обеспечения безопасной передачи данных между её защищёнными сегментами, а также фильтрации IP-трафика
Virtual Private Network (VPN)	Обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети
Технология ViPNet	Технология, предназначенная для построения виртуальных защищённых сетей путём использования системы персональных и межсетевых экранов на защищаемых компонентах распределённой сети и объединения защищаемых элементов через виртуальные соединения (туннели), обеспечивающие шифрование сетевого трафика между этими элементами на базе средства криптографической защиты информации
АРМ	Автоматизированное рабочее место
Региональная система межведомственного электронного взаимодействия Белгородской области	Информационная система Белгородской области, являющаяся частью системы межведомственного электронного взаимодействия (СМЭВ), которая позволяет федеральным, региональным и местным органам власти, кредитным организациям (банкам), внебюджетным фондам и прочим участникам СМЭВ обмениваться данными, необходимыми для оказания государственных услуг гражданам и организациям в электронном виде
Аттестат	Аттестат соответствия требованиям по безопасности информации

Защищённая сеть	Защищённая виртуальная сеть Белгородской области, построенная по технологии ViPNet № 3168
Оператор	Министерство цифрового развития Белгородской области
Администратор	ОГБУ «Белгородский информационный фонд»
Администратор сети № 3168	Сотрудник Администратора, осуществляющий общую политику администрирования всей Защищённой сети
Заявитель	Организация, имеющая намерения подключиться к Защищённой сети
Участник	Организация, подключённая к Защищённой сети в установленном в настоящем регламенте порядке
Администратор сторонней сети	Назначенный приказом сотрудник Участника, осуществляющий администрирование информационных систем и абонентских пунктов, принадлежащих данному Участнику
Абонент Защищённой сети	Назначенный приказом руководителя сотрудник Участника, использующий для выполнения своих служебных обязанностей сервисы и информационные системы Защищённой сети
Владелец ИС	Организация, владеющая информационной системой
Абонентский пункт (АП)	Персональный компьютер или сервер с установленным программным обеспечением ViPNet Client
ViPNet NCC (Центр управления сетью, ЦУС)	Приложение для конфигурирования и управления виртуальной Защищённой сетью ViPNet, входящее в состав ViPNet Administrator
ViPNet KCA (Удостоверяющий и ключевой центр, УКЦ)	Приложение, которое выполняет функции центра формирования ключей шифрования и персональных ключей пользователей, входящее в состав ViPNet Administrator
Компрометация ключа	Утрата доверия к тому, что используемые ключи обеспечивают безопасность информации
Информационная система (ИС)	Совокупность содержащихся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств
Несанкционированный доступ	Доступ к информации, хранящейся на различных типах носителей, в базах данных, файловых хранилищах, путём изменения (повышения, фальсификации) своих прав доступа
СКЗИ	Средство криптографической защиты информации
ПК, ПАК	Программный комплекс, программно-аппаратный комплекс

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Регламент взаимодействия участников Защищённой сети Региональной системы межведомственного электронного взаимодействия Белгородской области (далее – Регламент) разработан в соответствии со следующими нормативными правовыми актами:

– Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

– Приказ ФАПСИ от 13 июня 2001 года № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

– Федеральный закон от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи»;

– Приказ ФСБ России от 9 февраля 2005 года № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

– Приказ ФСБ России от 27 декабря 2011 года № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи»;

– Приказ ФСБ России от 27 декабря 2011 года № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»;

– Приказ ФСТЭК России от 18 февраля 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 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– Руководящий документ «Решение Коллегии Гостехкомиссии России № 7.2» от 2 марта 2001 года;

– Руководящий документ «Решение председателя Гостехкомиссии России» от 30 марта 1992 года;

2.2. Регламент определяет и устанавливает:

– порядок организации и подключения Участников Защищённой сети (далее – Порядок);

– порядок предоставления доступа к информационным системам, размещённым в Защищённой сети;

– порядок организации защищённого межсетевого взаимодействия;

– порядок действий при компрометации ключей;

– порядок разрешения конфликтных ситуаций.

3. ОБЩИЕ ТРЕБОВАНИЯ К ЗАЩИТЕ ИНФОРМАЦИИ

3.1. Подключаемый к Защищённой сети объект информатизации должен иметь действующий Аттестат, который подтверждает полное соответствие объекта информатизации для подключения к информационным системам по требованиям информационной безопасности и рекомендациям по технической защите конфиденциальной информации.

3.2. СКЗИ на подключаемых к Защищённой сети объектах информатизации с введёнными криптоключами относятся к материальным носителям, содержащим служебную информацию ограниченного распространения, согласно нормативным правовым актам по информационной безопасности.

3.3. При необходимости передачи по техническим средствам связи служебных сообщений, касающихся организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации, соответствующие указания необходимо передавать только применяя СКЗИ. Передача по открытым каналам связи криптоключей не допускается.

3.4. Необходимо соблюдать меры по обеспечению безопасности персональных данных согласно приказу ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при обработке в ИСПДн».

3.5. Для защиты общедоступной информации, содержащейся в государственных информационных системах, необходимо применять требования 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».

4. ПОРЯДОК ОРГАНИЗАЦИИ ПОДКЛЮЧЕНИЯ УЧАСТНИКОВ К ЗАЩИЩЁННОЙ СЕТИ

4.1. Администратор назначает сотрудников, ответственных за администрирование защищенной сети VipNet № 3168.

4.2. Заявитель направляет в адрес Оператора заявку о намерении подключиться к Защищённой сети (приложение № 1), в которой должен быть отражён перечень аппаратных и программных средств защиты для каналов связи, а также список сотрудников, которым планируется предоставить доступ.

4.3. Оператор и Администратор после получения заявки о намерении подключиться к Защищённой сети проводят оценку нормативных оснований

для подключения Заявителя к Защищённой сети, технической возможности подключения, проверку согласования доступа к информационным системам от Владельца ИС.

4.4. Наличие программного обеспечения и оборудования до рассмотрения заявки о намерении подключиться к Защищённой сети не является основанием и гарантией подключения Заявителя к Защищённой сети.

4.5. Оператор имеет право отказать Заявителю в подключении к Защищённой сети в следующих случаях:

– некорректное составление заявления;

– отсутствие согласованной заявки на предоставление доступа к ИС по форме Владельца ИС;

– отсутствие связи с подключаемым рабочим местом (не запущен, не установлен ViPNet Client, Coordinator);

– обнаруженная на подключаемом АРМ (АП) вирусная активность или другие деструктивные воздействия.

4.6. Оператор передаёт заявление на подключение Администратору, который осуществляет подключение АП или ПАК заявителя к Защищённой сети, после этого Заявитель считается Участником.

4.7. Администратор сети № 3168 имеет право отключить АП или ПАК от Защищённой сети при отсутствии активности более трёх месяцев.

4.8. Участник должен оперативно информировать Оператора и Владельца ИС обо всех изменениях АП (уволился или сменился сотрудник, перемещение рабочей станции, переустановка программного обеспечения, приостановка или отзыв аттестата соответствия по требованиям безопасности информации ФСТЭК России).

4.9. В рамках заявки взаимодействие Участника и Администратора осуществляется по электронной почте serviceuc@belregion.ru или по телефону (4722) 42-41-31.

5. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ИНФОРМАЦИОННЫМ СИСТЕМАМ

5.1. Подключение к информационным системам производится согласно заявке по форме Владельца ИС.

5.2. Администратор уведомляет Участника и Владельца ИС об организации защищённого взаимодействия в соответствии с пунктом 4.8 настоящего регламента.

5.3. Участник и Владелец ИС проверяют возможность взаимодействия с информационной системой и направляют Оператору уведомление о запуске в продуктивное использование.

5.4. Если не поступает сообщение о проблеме взаимодействия в течение 5 рабочих дней согласно пункту 5.2 настоящего регламента, то заявка является исполненной.

6. ОРГАНИЗАЦИЯ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ С ДРУГИМИ СЕТЯМИ ViPNet

6.1. Для организации межсетевого взаимодействия между Защищённой сетью и сторонней сетью ViPNet Участник направляет заявку (приложение № 1), в которой уведомляет Оператора о необходимости организации информационного межсетевого взаимодействия с указанием контактов лиц, ответственных за организацию межсетевого взаимодействия (технических специалистов), и цели подключения.

6.2. Заявка на создание подключения межсетевого взаимодействия (приложение № 1) направляется Оператору от органов государственной власти, органов исполнительной власти, федеральных органов исполнительной власти, органов местного самоуправления, муниципальных учреждений, а также их подведомственных организаций, являющихся владельцами защищённых сетей.

6.3. Подать заявку может только бюджетная организация, владелец защищённой сети. Оператор и Администратор проводят оценку нормативных оснований и технической возможности (приложение № 1) для организации межсетевого взаимодействия, согласовывают подключение и инициируют подписание соглашения (приложение № 2).

6.3.1. Оператор имеет право отказать в организации межсетевого взаимодействия в следующих случаях:

– сеть ViPNet организации и АРМ Администратора системы не соответствуют требованиям информационной безопасности;

– отсутствует Аттестат;

– отсутствуют сертифицированные средства криптографической защиты информации соответствующего класса;

– отсутствует сертификат Администратора системы защиты информации ViPNet, подтверждающий компетенции сотрудников Участника;

– не согласовано адресное пространство подключаемой сети.

6.3.2. В случае принятия решения об организации межсетевого взаимодействия Оператор в письменной форме уведомляет о принятии такого решения Заявителя, инициирующего данное взаимодействие, с подписанием соглашения (приложение № 2).

6.4. Организация межсетевого взаимодействия с передачей ключевой информации между Заявителем и Администратором осуществляется в соответствии с нормативными правовыми актами по требованию информационной безопасности.

6.5. После завершения процедуры организации межсетевого взаимодействия между Защищённой сетью и сторонней сетью ViPNet подписывается Протокол установления межсетевого взаимодействия между Оператором и Заявителем, который оформляется в рамках соглашения об установлении межсетевого взаимодействия (приложение № 3).

7. КОМПРОМЕТАЦИЯ КЛЮЧЕЙ

7.1. К событиям компрометации ключей АП относятся следующие случаи:

– компрометация файла ключевого дистрибутива АП;

– компрометация съёмного носителя ключевой информации АП;

– компрометация парольной защиты АП;

– прекращение полномочий пользователя АП или Администратора сторонней сети, согласно соответствующему приказу имевшего доступ к паролям и ключам, в том числе в связи с расторжением трудового договора.

7.2. В случае наступления любого из событий, связанных с компрометацией ключевой информации, Участник немедленно сообщает о факте компрометации Администратору путём взаимодействия согласно пункту 4.8.

7.3. Администратор при получении сообщения о компрометации ключевой информации объявляет ключи АП скомпрометированными и создаёт средствами VipNet Administrator обновление справочников связей защищаемой сети с исключением скомпрометированных узлов.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 43ff563eb3cbfe7b362130ebe2eac12ef222c439
Владелец Мирошников Евгений Владимирович
Действителен с 13.01.2022 по 13.04.2023

Первый заместитель Губернатора Белгородской области – министр цифрового развития Белгородской области **Е.В. Мирошников**