ГУБЕРНАТОР
КУРСКОЙ ОБЛАСТИ
П О С Т А Н О В Л Е Н И Е

от 17.08.2018 Курск № 336-пг

О внесении изменений в постановление Губернатора Курской области от 09.10.2009 № 335 «Об утверждении Регламента использования Единой информационной коммуникационной среды Курской области»

Во изменение постановления Губернатора Курской области от 09.10.2009 №335 «Об утверждении Регламента использования Единой информационной коммуникационной среды Курской области» ПОСТАНОВЛЯЮ:

1. Внести в Регламент использования Единой информационной коммуникационной среды Курской области, утвержденный постановлением Губернатора Курской области от 09.10.2009 №335 «Об утверждении Регламента использования Единой информационной коммуникационной среды Курской области» (в редакции постановления Губернатора Курской области от 27.05.2014 №242-пг), изменения, изложив его в новой редакции (прилагается).

2. Признать утратившим силу пункт 3 изменений, которые вносятся в постановления Губернатора Курской области, утвержденных постановлением Губернатора Курской области от 27.05.2014 № 242-пг «О внесении изменений в постановления Губернатора Курской области».

Губернатор Курской области А.Н.Михайлов

Управление Администрации Курской области
Отдел делопроизводства

305220 649108

УТВЕРЖДЕН
постановлением Губернатора
Курской области
от 09.10.2009 № 335
(в редакции постановления Губернатора
Курской области
от 17.08.2018 № 336-пг)

РЕГЛАМЕНТ
использования Единой информационной коммуникационной среды Курской области

1. Принятые сокращения и термины

АС - автоматизированная система.

ЕИКС Курской области - единая информационная коммуникационная среда Курской области.

ЛВС - локальная вычислительная сеть.

МЭ - межсетевой экран.

НСД - несанкционированный доступ.

ОС - операционная система.

ИС – информационная система.

ПО - программное обеспечение.

РД - руководящий документ.

СВТ - средства вычислительной техники.

СЗИ НСД - средства защиты информации от несанкционированного доступа.

СУБД - система управления базами данных.

ФСТЭК - Федеральная служба по техническому и экспортному контролю.

ЭП - электронная подпись.

ЦУС - Центр управления сетью.

УКЦ - Удостоверяющий Ключевой центр.

ИСММК - Индивидуальный Симметричный Межсетевой Мастер-ключ.

ПАК - программно-аппаратный комплекс.

СЦ ГКО - Ситуационный центр Губернатора Курской области.

Дистрибутив ключей - файл с расширением .dst, создаваемый в программе ViPNet Удостоверяющий и ключевой центр или ViPNet Manager для каждого пользователя сетевого узла ViPNet. В этом файле помещены адресные справочники, ключевая информация и файл лицензии, необходимые для обеспечения первичного запуска и последующей работы

программы ViPNet на сетевом узле. Для обеспечения работы программы ViPNet дистрибутив ключей необходимо установить на сетевой узел.

Администрация ЕИКС Курской области - орган исполнительной власти Курской области, уполномоченный в сфере развития и использования информационных технологий на территории Курской области (региональной информатизации) и обеспечения защиты информации.

Ядро ЕИКС Курской области – оборудование и коммутационные сети, принадлежащее или арендуемые Администрацией ЕИКС Курской области.

Администратор ЕИКС Курской области – сотрудник(-и) Администрации ЕИКС Курской области, который отвечает за администрирование и защиту ядра ЕИКС Курской области.

Претендент - органы исполнительной власти Курской области, органы местного самоуправления Курской области, подведомственные учреждения и организации Курской области и сторонние организации, желающие подключиться к ЕИКС Курской области, в том числе к защищенному сегменту сети ViPNet ЕИКС.

Участник информационного взаимодействия (Участник ЕИКС Курской области) – органы исполнительной власти Курской области, органы местного самоуправления Курской области, подведомственные учреждения и организации Курской области и сторонние организации, имеющие подключение к ЕИКС Курской области.

Участок ЕИКС Курской области – оборудование и коммутационные сети, принадлежащее или арендуемые Участником ЕИКС Курской области.

Локальный администратор – сотрудник(-и) Участника ЕИКС Курской области, который отвечает за администрирование и защиту Участка ЕИКС Курской области, находящегося в ответственности Участника ЕИКС Курской области.

Абонент ЕИКС Курской области – сотрудник(-и) Участника ЕИКС Курской области, имеющий доступ к информационным ресурсам ЕИКС Курской области (в том числе Локальный администратор Участника ЕИКС Курской области).

Оператор информационной системы - орган государственной власти Курской области, орган местного самоуправления, территориальный орган федерального органа исполнительной власти или организация, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Защищенный сегмент сети ViPNet ЕИКС – сегмент сети ЕИКС, к которому подключение осуществляется посредством программных и программно-аппаратных средств ViPNet.

Владелец сети ViPNet – орган государственной власти Курской области, орган местного самоуправления, территориальный орган федерального органа исполнительной власти или организация, которой принадлежит право использования и администрирования сети ViPNet.

Администратор сети ViPNet - лицо, отвечающее за конфигурирование сети ViPNet, создание и обновление справочно-ключевой информации для сетевых узлов ViPNet, настройку межсетевого взаимодействия с доверенными сетями и обладающее правом доступа к программе ViPNet Manager или ViPNet ЦУС и (или) ViPNet УКЦ.

Сеть ViPNet 1366 – сеть, владельцем которой является Администрация ЕИКС Курской области.

Абонентский пункт - сетевой узел ViPNet, который является начальной или конечной точкой передачи данных.

Пользователь Абонентского пункта - обладатель неисключительных прав на ПО ViPNet из ViPNet-сети, а также владелец ключевой информации для доступа в сеть.

2. Общие положения. Основные задачи, организация, контроль, руководство

Регламент использования ЕИКС Курской области (далее - Регламент) определяет содержание и порядок совместного использования ЕИКС Курской области и обеспечения безопасности информационных ресурсов ЕИКС Курской области.

Настоящий Регламент предназначен для практического использования участниками информационного взаимодействия при организации и проведении мероприятий по использованию ЕИКС Курской области.

Требования и рекомендации Регламента обязательны для выполнения всеми должностными лицами участников информационного взаимодействия при организации и проведении мероприятий по использованию ЕИКС Курской области.

Регламент разработан в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации», Федеральным законом «О персональных данных», Федеральным законом «О коммерческой тайне», Федеральным законом «Об электронной подписи», Указом Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», Указом Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера», руководящими документами ФСТЭК России и Законом Курской области «Об информационных системах Курской области».

Регламент определяет комплекс организационных и технических мероприятий по обеспечению эффективного и бесперебойного функционирования ЕИКС Курской области.

Регламент проходит согласование у руководителей участников информационного взаимодействия и утверждается Губернатором Курской области.

Доступ к ресурсам ЕИКС Курской области предоставляется Абонентам ЕИКС Курской области для выполнения ими должностных обязанностей.

ЕИКС Курской области предназначена для:

осуществления информационного взаимодействия, в том числе юридически значимого, между Абонентами ЕИКС Курской области;

формирования и использования общих информационных ресурсов;

предоставления собственных информационных ресурсов в совместное пользование определенным участникам информационного взаимодействия для более эффективного выполнения служебных задач;

проведения единой политики в сфере информационных технологий и безопасности информации всеми участниками информационного взаимодействия.

Основными задачами Регламента являются:

определение порядка создания и формирования информационных ресурсов ЕИКС Курской области;

организация иерархической системы администрирования ЕИКС Курской области;

определение порядка использования информационных ресурсов ЕИКС Курской области;

организация электронного документооборота, в том числе юридически значимого, между пользователями ЕИКС Курской области;

определение порядка использования ЭП в процессе информационного взаимодействия между Участниками ЕИКС Курской области;

определение требований при подключении к сторонним информационным сетям и предоставлении доступа к информационным ресурсам ЕИКС Курской области сторонним организациям, учреждениям и предприятиям;

определение методов защиты информационных ресурсов ЕИКС Курской области и организация мероприятий по обеспечению их безопасности;

организация контроля защищенности информационных ресурсов ЕИКС Курской области.

В состав информационных ресурсов ЕИКС Курской области входят:

общие информационные ресурсы ЕИКС Курской области;

информационные ресурсы участников информационного взаимодействия, предоставленные для совместного использования в рамках ЕИКС Курской области;

информационные ресурсы участников информационного взаимодействия, входящие в состав ЕИКС Курской области, но не предназначенные для совместного использования;

устройства и средства информационного взаимодействия и защиты информации.

Информационные ресурсы, созданные или приобретенные участником информационного взаимодействия, являются его собственностью. Участник информационного взаимодействия в рамках использования информационных ресурсов ЕИКС Курской области обязан обеспечить проведение всех необходимых мероприятий по защите указанных информационных ресурсов на уровне не ниже установленного для информационных ресурсов ЕИКС Курской области соответствующего класса.

Общими информационными ресурсами ЕИКС Курской области являются ресурсы, созданные участниками информационного взаимодействия количеством более одного и расположенные на серверах ЕИКС Курской области. Ограничения по доступу к указанным ресурсам определяются Администрацией ЕИКС Курской области. Собственником данных ресурсов является Администрация Курской области в лице уполномоченного органа, определяемого актом Губернатора Курской области.

Ответственность за обеспечение проведения мероприятий по защите и формированию информационных ресурсов участников информационного взаимодействия возлагается на руководителя участника информационного взаимодействия.

Ответственность за обеспечение проведения мероприятий по защите и формированию общих информационных ресурсов ЕИКС Курской области возлагается на Администрацию ЕИКС Курской области.

Общее руководство в сфере развития и формирования ЕИКС Курской области и информационных ресурсов осуществляет Администрация ЕИКС Курской области, для исполнения чего Администрация ЕИКС Курской области наделяется следующими правами и обязанностями:

разрабатывать, согласовывать и вносить предложения об изменении и дополнении настоящего Регламента;

самостоятельно проводить мероприятия по контролю защищенности общих информационных ресурсов ЕИКС Курской области - информационных ресурсов Участников ЕИКС Курской области по согласованию с руководством и с привлечением Локальных администраторов;

координировать работу по администрированию ЕИКС Курской области;

формировать реестр участников информационного взаимодействия;

подготавливать и вносить предложения по реформированию и развитию ЕИКС Курской области;

делегировать полномочия по подключению/отключению участников ЕИКС и обслуживанию ЕИКС своим подведомственным учреждениям.

3. Подключение к ЕИКС Курской области

Настоящий Регламент определяет следующий порядок по присоединению к ЕИКС Курской области Претендентов.

Претендент совместно с Администрацией ЕИКС Курской области должен определить возможный способ подключения к ЕИКС:

прямое подключение к ЕИКС (к ближайшему узлу ЕИКС);

подключения к защищенному сегменту сети ViPNet ЕИКС (с использованием сторонних провайдеров).

Для этого в адрес Администрации ЕИСК Курской области от Претендента направляется заявка о присоединении к ЕИКС Курской области, содержащая данные о полном наименовании, месте нахождении, основных направлениях деятельности, форме собственности, учредителях юридического лица и экземпляр соглашения об обеспечении доступа к ЕИКС Курской области, подписанный со стороны Претендента. Форма соглашения об обеспечении доступа к ЕИКС Курской области представлена в приложении №1 к настоящему Регламенту. Поступившие заявки подлежат обязательной регистрации в течение 2 рабочих дней со дня их поступления.

В случае необходимости уточнения сведений о подавшем заявку Претенденте, а также структуре и порядке эксплуатации их ИС Администрация ЕИКС Курской области запрашивает у Претендента необходимую информацию.

Администрация ЕИКС Курской области в течение 30 календарных дней со дня регистрации заявки принимает решение о возможности подключения Претендента к ЕИКС Курской области и определяет способ подключения к ЕИКС.

В случае принятия положительного решения Администрация ЕИКС Курской области в течение 5 рабочих дней со дня принятия решения заключает с Претендентом соглашение об обеспечении доступа к ЕИКС Курской области и предоставляет Претенденту сведения о технологической возможности для присоединения к ЕИКС Курской области, в том числе способ подключения к сети ЕИКС.

В случае отсутствия юридической или технической возможности подключения Претендента к ЕИКС Курской области Администрация ЕИКС Курской области принимает отрицательное решение, о котором информирует Претендента в течение 5 рабочих дней со дня принятия решения.

Подключение к защищенному сегменту сети ViPNet ЕИКС включает в себя следующие стадии:

закупка ПО и/или ПАК;

подача заявки;

рассмотрение заявки;

получение регистрационных файлов;

формирование и передача ключевой информации.

После заключения соглашения об обеспечении доступа к ЕИКС

Курской области Претендент самостоятельно приобретает ПО ViPNet [Клиент] и/или ViPNet [Координатор] и/или ПАК.

При оформлении договорных отношений по приобретению ПО ViPNet [Клиент] и/или ViPNet [Координатор] и/или ПАК Претендент указывает номер Защищённой сети для подключения - 1366.

После приобретения вышеуказанного ПО или ПАК Претендент направляет в Администрацию ЕИКС Курской области заявку о подключении к защищенному сегменту сети ViPNet ЕИКС (приложение №2 к настоящему Регламенту).

В заявке должна содержаться следующая информация:

точное количество подключаемых Абонентских пунктов;

подробная схема сети Претендента с указанием всех IP-адресов, в том числе запланированных для подключения;

общий перечень Участников ЕИКС Курской области, с которыми необходима организация защищённого обмена;

полный перечень ИС, к которым необходимо организовать доступ;

тип подключения к сети «Интернет» или иной сети передачи данных с указанием сведений о провайдере и используемом оборудовании;

заверенная Претендентом копия документа, подтверждающего законное приобретение ПО ViPNet (Договор/Контракт);

ФИО, контактный телефон и адрес электронной почты лица, ответственного за подключение Претендента.

Также в адрес Администрации ЕИКС Курской области необходимо предоставить:

копии приказов о назначении Локального администратора (приложение №3 к настоящему Регламенту) и Абонентов (приложение №4 к настоящему Регламенту);

копии соглашений с Локальным администратором и Абонентами ЕИКС Курской области о неразглашении информации, к которой будет получен доступ в связи с выполнением своих функций (приложение №5 к настоящему Регламенту);

доверенность на получение дистрибутива ключей (приложение №6 к настоящему Регламенту). Предоставление доверенности возможно в момент получения дистрибутива ключей.

Администрация ЕИКС Курской области регистрирует заявку Претендента о подключении к защищенному сегменту сети ViPNet ЕИКС в течение 2 рабочих дней со дня поступления и в течение 20 рабочих дней со дня регистрации заявки проводит оценку правильности заполнения всех документов, оснований для подключения Претендента и технической возможности организации направлений связи, доступа к ИС.

Решение Администрации ЕИКС Курской области о возможности предоставления доступа к информационным ресурсам направляется посредством электронной почты на электронный адрес, указанный в заявлении (адрес лица, ответственного за подключение), в течение 3

рабочих дней со дня принятия указанного решения.

Администрация ЕИКС Курской области отказывает Претенденту в подключении к защищенному сегменту сети ViPNet ЕИКС в случае предоставления Претендентом недостоверной и(или) неполной информации. Решение об отказе в подключении Претендента к защищенному сегменту сети ViPNet ЕИКС направляется в письменной форме в адрес Претендента в течение 3 рабочих дней со дня принятия указанного решения.

Подключение Претендента осуществляется Администрацией ЕИКС Курской области только после получения регистрационных файлов от производителя ПО или представителя производителя ПО.

В течение 3 рабочих дней со дня принятия положительного решения и получения регистрационных файлов Администрация ЕИКС Курской области:

производит регистрацию Абонентских пунктов в ЦУС;

организовывает направления связи между Абонентскими пунктами, в соответствии с заявкой на подключение;

формирует дистрибутивы ключей для Абонентских пунктов вместе с паролем доступа к нему;

уведомляет о готовности дистрибутива ключей Претендента посредством электронной почты на электронный адрес, указанный в заявлении (адрес лица, ответственного за подключение).

В случае заявки на изготовление более 5 Абонентских пунктов срок выполнения увеличивается пропорционально количеству Абонентских пунктов из расчета каждые 5 Абонентских пунктов на 1 день.

Претендент в день получения дистрибутива ключей и пароля доступа к нему должен иметь:

доверенность на получение дистрибутива ключей (приложение №6 к настоящему Регламенту);

журнал учета машинных носителей и средств криптографической защиты информации;

учтенный служебный носитель информации;

документ, удостоверяющий личность.

Факт выдачи и получения дистрибутива ключей заносится в Журнал учёта выдачи ключевых документов.

В случае обнаружения вредоносного ПО на носителе информации, предоставленном для записи дистрибутива ключей, а также если данный носитель информации не учтен в соответствии с Инструкцией 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, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152, запись на

такой носитель не осуществляется.

Администрация ЕИКС Курской области не несет ответственности за неисполнение требований договорных соглашений и/или сроков исполнения договорных соглашений Претендента в случае соблюдения Администрацией ЕИКС Курской области сроков и процедур, установленных данным Регламентом.

В случае если требуется повторное получение дистрибутивов ключей для Абонентских пунктов и паролей доступа к ним Участник ЕИКС Курской области направляет заявку (приложение №10 к настоящему Регламенту) в адрес Администрации ЕИКС Курской области. Поступившие заявки подлежат обязательной регистрации в течение 2 рабочих дней со дня их поступления.

Администрация ЕИКС Курской области в течение 5 рабочих дней со дня регистрации заявки принимает решение о возможности повторного получения дистрибутивов ключей для Абонентских пунктов и паролей доступа к ним.

В случае необходимости уточнения сведений для повторного предоставления дистрибутивов ключей для Абонентских пунктов и паролей доступа к ним Администрацией ЕИКС Курской области запрашивается необходимая информация от подавшего заявку Участника ЕИКС Курской области.

В случае принятия положительного решения Администрация ЕИКС Курской области в течение 3 рабочих дней со дня принятия решения проводит процедуру формирования новых дистрибутивов ключей для Абонентских пунктов.

В течение 2 рабочих дней со дня формирования новых дистрибутивов Администрация Курской области направляет на адрес электронной почты Участника ЕИКС Курской области, указанный в заявке, уведомление о готовности дистрибутивов ключей для Абонентских пунктов. В случае отсутствия в заявке адреса электронной почты Участника ЕИКС Курской области уведомление не направляется.

Администрация ЕИКС Курской области отказывает Участнику ЕИКС Курской области в повторном предоставлении дистрибутива ключей для Абонентских пунктов и пароля доступа к нему в следующих случаях: пароль для административного доступа к Абонентскому пункту действителен; предоставлена недостоверная и(или) неполная информация; дистрибутив ключей или пароль доступа утерян и не предоставлены результаты проведения служебной проверки. Данное решение направляется Администрацией ЕИКС Курской области в письменной форме в адрес Участника ЕИКС Курской области в течение 3 рабочих дней со дня принятия указанного решения.

Порядок получения дистрибутива ключей не меняется.

4. Организация межсетевого взаимодействия сети ViPNet 1366 с другими сетями ViPNet

4.1. Обеспечение защиты информации при передаче сведений.

Обеспечение защиты информации при передаче сведений осуществляется с использованием сертифицированных криптографических средств защиты информации, с использованием программно-аппаратных средств защиты информации «ViPNet» в рамках заключенного соглашения об обеспечении доступа к ЕИКС Курской области.

4.2. Передача служебных сведений.

Передача служебных сведений обеспечивается средствами ПО ViPNet MFTP, а при невозможности использования вышеуказанных средств - вручную, с использованием учтенных носителей информации, непосредственно между Владельцами сетей ViPNet. В случае передачи служебных сведений Владелец сети ViPNet, инициализирующий передачу, обязан не позднее, чем за 3 дня до факта передачи уведомить другого Владельца сети ViPNet официальным письмом.

4.3. Подтверждение достоверности и подлинности передаваемых сообщений.

Подтверждение достоверности, подлинности и авторства передаваемых сведений обеспечивается средствами ЭП с использованием ПО ViPNet Деловая почта, входящего в состав ПАК защиты информации «ViPNet».

5. Порядок организации межсетевого защищенного информационного взаимодействия

5.1. Определение условий межсетевого взаимодействия сетей ViPNet.

Передача данных между узлами сетей ViPNet может осуществляться либо напрямую, либо через узлы одной и/или другой сети ViPNet.

Межсетевое защищенное информационное взаимодействие сетей ViPNet организуется по технологии межсетевого взаимодействия сетей ViPNet.

Межсетевое защищенное информационное взаимодействие организуется с помощью ИСММК.

ИСММК формирует Администраторы сети ViPNet для каждой из сетей, с которой должно осуществляться взаимодействие.

Администраторы сетей ViPNet выделяют узлы своих сетей, которые будут участвовать в межсетевом взаимодействии. Выделенные узлы сетей будут связаны в ЦУСах взаимодействующих сетей, а также будут иметь ключи для шифрования и подтверждения достоверности и подлинности передаваемых данных.

Администраторы сетей ViPNet выбирают устройства (Координаторы), которые будут выполнять функции серверов-шлюзов при межсетевом взаимодействии сетей.

5.2. Порядок организации межсетевого защищенного информационного взаимодействия между сетями ViPNet.

Порядок организации межсетевого защищенного информационного взаимодействия между сетями ViPNet предполагает выполнение следующих технологических и организационных мероприятий.

Для организации межсетевого защищенного информационного взаимодействия между сетями ViPNet инициатор межсетевого взаимодействия готовит официальное информационное письмо, в котором информирует Владельца другой сети ViPNet о необходимости организации межсетевого защищенного информационного взаимодействия между заданными сетями ViPNet с обязательным указанием целей, причин и предполагаемых результатов подключения, а также узлов своей сети, шлюза и предполагаемых клиентов противоположной сети. В течение 30 календарных дней со дня получения официального информационного письма Владелец сети ViPNet, не являющийся инициатором организации межсетевого защищенного информационного взаимодействия, обязан дать официальный ответ с подтверждением или отказом от межсетевого защищенного информационного взаимодействия с указанием причин.

После получения официального подтверждения в течение 14 рабочих дней в ЦУС и УКЦ Владельца сети ViPNet, инициализирующего межсетевое защищенное информационное взаимодействие, Администратор сети ViPNet производит формирование необходимой адресной и ключевой информации - формирование начального экспорта (индивидуальные симметричные межсетевые мастер-ключи связи и шифрования, справочная информация), включая свои корневые сертификаты для каждой из сетей, с которой должно осуществляться взаимодействие.

Указанные данные (начальный экспорт) доверенным способом передаются в ЦУС другой сети ViPNet.

В течение 5 рабочих дней со дня получения начального экспорта в ЦУС и УКЦ Владельца сети ViPNet, получившей начальный экспорт, Администратор сети ViPNet производит ввод и обработку (импорт) полученных из ЦУСа другой сети ViPNet (начального экспорта), установление связей своих узлов с узлами ЦУСа, предоставившим информацию. Далее Администратор сети ViPNet, получивший начальный экспорт, создает ответную информацию (ответный экспорт) для ЦУСа, приславшего первичную информацию, включая свои корневые сертификаты.

В течение 5 рабочих дней ответная информация (ответный экспорт) доверенным способом передается в ЦУС Владельца сети ViPNet, создавшего начальный экспорт, где она обрабатывается и вводится в

действие Администратором сети ViPNet. На этом этапе завершается процесс создания межсетевого защищенного взаимодействия между ЦУСами, и дальнейший обмен данными между ними производится в автоматическом режиме, а в случае невозможности – иным доверенным способом.

После рассылки каждым ЦУСом сформированных обновлений ключевой и справочной информации на свои узлы, участвующие в межсетевом взаимодействии, между данными узлами различных сетей можно осуществлять защищенный обмен информацией.

После завершения процедуры организации межсетевого защищенного информационного взаимодействия между Владельцами сетей ViPNet подписывается Протокол установления межсетевого взаимодействия (приложение № 9 к настоящему Регламенту).

В случае возникновения проблем, препятствующих осуществлению межсетевого защищенного информационного взаимодействия, Владелец сети ViPNet, обнаруживший проблему, обязан в течение 3 рабочих дней с момента обнаружения неисправности проинформировать (письмом или по каналам электронной почты) Владельца другой сети ViPNet о выявленной проблеме, после чего Администраторами сетей ViPNet в течение 3 рабочих дней со дня получения официального сообщения решается вопрос о принадлежности выявленной неисправности к сферам ответственности Администраторов сетей ViPNet. После этого один из Администраторов сетей ViPNet (в случае нахождения проблемы в его сфере ответственности) или оба Администратора сетей ViPNet (в случае нахождения проблемы в их сфере ответственности) принимают меры по устранению выявленной неисправности, после реализации которых в течение 5 рабочих дней информируют Владельца другой сети ViPNet официальным информационным сообщением.

5.3. Порядок модификации межсетевого защищенного информационного взаимодействия между сетями ViPNet при изменении состава узлов.

Порядок модификации межсетевого защищенного информационного взаимодействия между сетями ViPNet предполагает выполнение следующих технологических и организационных мероприятий.

В процессе функционирования межсетевого защищенного информационного взаимодействия сетей ViPNet в одной или нескольких сетях может потребоваться изменение состава узлов, участвующих в межсетевом защищенном взаимодействии, - добавление или удаление сетевого узла, а также установление или удаление связей между существующими узлами.

При модификации межсетевого защищенного информационного взаимодействия в какой-либо сети ViPNet Владелец данной сети ViPNet не позднее, чем за 5 рабочих дней направляет официальное информационное

сообщение Владельцу другой сети ViPNet с указанием предполагаемых изменений.

После получения от Владельца другой сети ViPNet официального ответа (в течение 3 рабочих дней с момента получения официального информационного сообщения), разрешающего внесение изменений в структуру сети ViPNet, Администратор сети ViPNet в своем ЦУСе производит соответствующие изменения в структуре связей своей сети ViPNet, формирует экспортные данные и передает их в соответствующий ЦУС в автоматическом режиме, а в случае невозможности - иным доверенным способом в течение 3 рабочих дней с момента получения официального разрешения.

В ЦУСе сети ViPNet, которой касается данная модификация, в течение 5 рабочих дней с момента получения экспортных данных производится обработка (импорт) полученных данных. Далее в ЦУСе создается ответная информация (ответный экспорт) для ЦУСа, приславшего первичную информацию.

Ответная информация передается в ЦУС сети ViPNet, от которой поступила первичная информация, в автоматическом режиме по защищенному каналу связи либо иным доверенным способом, где она обрабатывается и вводится в действие в течение 3 дней с момента получения. На этом завершается процесс модификации межсетевого защищенного взаимодействия между ЦУСами сетей ViPNet.

5.3.6. После рассылки каждым ЦУСом сформированных обновлений ключевой и справочной информации на свои узлы, которых касается модификация, данные узлы продолжают или прекращают производить защищенный электронный документооборот при межсетевом взаимодействии.

6. Порядок организации межсетевого защищенного информационного взаимодействия между сетями ViPNet в случае плановой смены межсетевого мастер-ключа

Порядок модификации межсетевого защищенного информационного взаимодействия между сетями ViPNet в случае плановой смены межсетевого мастер-ключа предполагает выполнение следующих технологических и организационных мероприятий.

6.1. Предварительные организационные мероприятия.

Перед тем как осуществлять плановую смену межсетевого мастер-ключа, Администраторы сетей ViPNet, для связи которых будет использоваться новый межсетевой мастер-ключ, должны согласовать следующие вопросы:

выбрать тип межсетевого мастер-ключа, который будет использоваться для связи между сетями;

если предполагается использовать симметричный мастер-ключ, необходимо определить, какая из сторон межсетевого взаимодействия будет создавать новый межсетевой мастер-ключ;

выбрать и согласовать время проведения смены межсетевого мастер-ключа и последующего обновления ключей шифрования для узлов своих сетей.

6.2. Формирование нового межсетевого мастер-ключа.

После проведения предварительных организационных мероприятий необходимо сформировать новый межсетевой мастер-ключ и произвести его смену.

6.3. Процедура создания экспорта и приема импорта.

После смены межсетевого мастер-ключа производится процедура создания экспортных данных (не позднее 5 рабочих дней с момента формирования нового межсетевого мастер-ключа) и приема импортных данных (не позднее 5 рабочих дней с момента получения экспортных данных).

6.4. Межсетевое взаимодействие после смены межсетевого мастер-ключа.

Связь между сетевыми узлами взаимодействующих сетей ViPNet после смены межсетевого мастер-ключа возможна только после прохождения обновлений ключевой информации на всех соответствующих сетевых узлах данных сетей.

7. Порядок организации межсетевого защищенного информационного взаимодействия между сетями ViPNet в случае компрометации ключей

7.1. Компрометация ключей пользователей.

Под компрометацией ключей подразумевается утрата доверия к используемым ключам, обеспечивающим безопасность информации (целостность, конфиденциальность, подтверждение авторства, невозможность отказа от авторства).

При наступлении любого из перечисленных событий Пользователь Абонентского пункта должен немедленно прекратить работу на Абонентском пункте и сообщить о факте компрометации (или предполагаемом факте компрометации) Администратора своей сети ViPNet.

По факту компрометации ключей должно быть проведено служебное расследование.

Администратор сети ViPNet в случае компрометации ключей Пользователя Абонентского пункта своей сети в ЦУСе и УКЦ своей сети проводит процедуру внеплановой компрометации ключей данного пользователя, которая предполагает выполнение следующих технологических и организационных мероприятий в течение 3 рабочих дней с момента получения данных о компрометации ключа.

Администратор сети ViPNet оповещает о факте компрометации ключей всех Пользователей Абонентских пунктов, связанных со скомпрометированным Пользователем Абонентского пункта. После получения данного сообщения Пользователи Абонентских пунктов не должны использовать скомпрометированные ключи.

Администратор сети ViPNet объявляет ключи данного Пользователя Абонентского пункта скомпрометированными, создает и отправляет экспорт адресно-ключевой информации в другие сети ViPNet, с которыми был связан скомпрометированный Пользователь Абонентского пункта.

Администратор сети ViPNet создает и отправляет (либо передает доверенным способом) новую ключевую информацию как для скомпрометированного Пользователя Абонентского пункта, так и для всех Пользователей Абонентских пунктов своей сети, с которыми он был связан.

В течение 4 рабочих дней после приема и обработки импорта переданных данных Администратор сети ViPNet, Пользователи Абонентских пунктов которой взаимодействовали с Пользователем Абонентского пункта, ключи которого скомпрометированы, создаёт новую ключевую информацию своим Пользователям Абонентских пунктов.

После прохождения обновления новой ключевой информации на всех взаимодействующих узлах сетей ViPNet Сторон Пользователи Абонентских пунктов могут продолжать производить защищенный электронный документооборот.

7.2. Внеплановая смена межсетевого мастер-ключа.

Внеплановая смена ключей выполняется в случае компрометации или угрозы компрометации межсетевого мастер-ключа, на котором происходит организация межсетевого защищенного информационного взаимодействия между сетями ViPNet.

В случае компрометации симметричного межсетевого мастер-ключа считается скомпрометированной вся ключевая информация, которая используется при межсетевом взаимодействии сетей ViPNet, о чем в течение 1 рабочего дня направляется официальное информационное сообщение другому Владельцу сети ViPNet.

Должно быть немедленно остановлено межсетевое защищенное информационное взаимодействие между сетями ViPNet.

Для восстановления работы межсетевого защищенного информационного взаимодействия между сетями ViPNet необходимо провести все необходимые технологические и организационные мероприятия.

8. Компрометация ключей

8.1. К событиям компрометации, когда ключи Абонента считаются скомпрометированными, относятся следующие случаи:

потеря ключевых носителей;

потеря ключевых носителей с их последующим обнаружением;

увольнение сотрудников, имевших доступ к ключевой информации;

нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа;

случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в т.ч. случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленников);

на Абонентском пункте отсутствовал (был отключен) модуль ViPNet Client Monitor или он устанавливался в 4-й или 5-й режим, и в локальной сети считается возможным присутствие посторонних лиц.

8.2. При возникновении сомнений в неизвестности посторонним лицам пароля доступа Пользователя Абонентского пункта при старте модуля ViPNet Client Monitor, при условии, что доступ к Абонентскому пункту посторонних лиц был возможен, ключи считаются скомпрометированными.

8.3. К событиям, требующим проведения расследования и принятия решения на предмет компрометации ключевой информации, относится возникновение подозрений в утечке информации при её передаче посредством защищённой сети.

8.4. В случае наступления любого из событий, связанных с компрометацией ключевой информации, Пользователь Абонентского пункта немедленно прекращает связь с другими Абонентскими пунктами и сообщает о факте компрометации своему Администратору сети ViPNet.

8.5. Администратор сети ViPNet при получении сообщения о компрометации ключевой информации в течение 1 рабочего дня должен:

объявить ключи Абонентского пункта скомпрометированными и создать средствами ПО ViPNet справочники связей при компрометации с необходимой информацией;

оповестить о факте компрометации ключей всех Абонентов, связанных с Абонентом, ключевая информация которого была скомпрометирована;

сформировать средствами ПО ViPNet новую ключевую информацию. Все файлы с новой ключевой информацией зашифрованы на нескомпрометированных ключах из резервного набора персональных ключей, поэтому могут передаваться на скомпрометированный Абонентский пункт по любым каналам связи;

произвести рассылку или передать иным доверенным способом сформированных обновлений ключей на Абонентские пункты сети ViPNet.

9. Назначение Локального администратора

9.1. Локальный администратор назначается и отстраняется от исполнения возложенных функций приказом руководителя Участника ЕИКС Курской области.

9.2. Необходимым условием назначения Локального администратора является подписание с ним соглашения о неразглашении информации, полученной вследствие выполнения своих обязанностей.

9.3. В случае смены сотрудника, на которого возложены функции Локального администратора, Участник ЕИКС Курской области обязан в течение 2 рабочих дней известить об этом Администрацию ЕИКС Курской области.

9.4. При заполнении заявки необходимо указывать всех назначенных на данный момент Локальных администраторов и Абонентов ЕИКС Курской области.

9.5. Копия приказа о возложении функций Локального администратора, а также копия подписанного с этим сотрудником соглашения о конфиденциальности информации ограниченного доступа, полученной вследствие выполнения своих обязанностей, передаются Участником ЕИКС Курской области Администрации ЕИКС Курской области в течение 15 календарных дней со дня возложения вышеуказанных функций.

10. Ответственность администраторов

10.1. Ответственность за исправное функционирование ПО ViPNet у Участника ЕИКС Курской области возлагается на Локального администратора.

10.3. Ответственность за последствия, вызванные перебоями в функционировании и/или неправильным функционированием ПО ViPNet Участника ЕИКС Курской области, возлагается на Локального администратора.

10.4. Администрация ЕИКС Курской области осуществляет методическую помощь Участникам ЕИКС путем изготовления инструкций и методических рекомендаций, размещаемых на информационных ресурсах Администрации Курской области.

10.5. Администрация ЕИКС Курской области не осуществляет настройку и не несет ответственности за оборудование и ПО, принадлежащие Участнику ЕИКС Курской области.

10.6. Ответственность за защиту Ядра ЕИКС Курской области от несанкционированного доступа к информации возлагается на Администратора ЕИКС Курской области.

10.7. Ответственность за защиту Участков ЕИКС Курской области, входящих в сферу ответственности Участников ЕИКС Курской области, от

несанкционированного доступа к информации возлагается на Локального администратора.

10.8. Администратор ЕИКС Курской области и Локальный администратор несут персональную ответственность за качество проводимых ими работ по контролю действий пользователей при работе ЕИКС Курской области, состояние и поддержание установленного уровня защиты.

11. Права и обязанности администраторов

11.1. Администратор ЕИКС Курской области обязан:

следить за работоспособностью Ядра ЕИКС Курской области;

оперативно решать все проблемы, возникающие в Ядре ЕИКС Курской области;

изготавливать ключевые файлы и передавать их согласно настоящему Регламенту;

оказывать Участникам ЕИКС Курской области методическую помощь в настройках криптосредств путем изготовления инструкций и пособий, размещаемых на информационных ресурсах Администрации Курской области;

оказывать методическую помощь Участникам ЕИКС Курской области в организационных вопросах, связанных с эксплуатацией средств криптографической защиты.

11.2. Локальный администратор обязан:

знать структуру и состав своего Участка ЕИКС Курской области;

следить за работоспособностью Участка ЕИКС Курской области, находящегося в ответственности Участника ЕИКС Курской области;

оперативно решать все проблемы, возникающие на Участке ЕИКС Курской области, находящемся в ответственности Участника ЕИКС Курской области;

выполнять требования действующего законодательства Российской Федерации и настоящего Регламента.

11.3. Администратор ЕИКС Курской области отказывает в помощи в настройке средств криптографической защиты Участника ЕИКС Курской области в случае возникновения неисправностей на Участке ЕИКС Курской области, находящемся в ответственности Участника ЕИКС Курской области.

11.4. Администрация ЕИКС Курской области или Участник ЕИКС Курской области в случае недостаточной квалификации Администраторов ЕИКС Курской области или Локальных администраторов для выполнения части их функций привлекает на договорной основе сторонние организации. Если функции связаны с обслуживанием средств криптографической защиты информации, привлекаемые организации должны иметь соответствующие лицензии на работу и обслуживание средств криптографической защиты информации.

12. Порядок разрешения конфликтных ситуаций

12.1. Возникновение конфликтных ситуаций может быть связано с формированием, доставкой, получением, подтверждением получения Участниками ЕИКС Курской области электронных документов и/или получение доступа к ИС других Участников ЕИКС Курской области.

12.2. Разрешение конфликтных ситуаций осуществляется путём взаимодействия Локальных администраторов, у которых возникли претензии.

12.3. В случае необходимости для разрешения конфликтных ситуаций может быть привлечена Администрация ЕИКС Курской области.

13. Порядок формирования, использования, разграничения доступа единых, совместных и распределенных информационных систем

13.1. Формирование информационных ресурсов ЕИКС Курской области осуществляется при соблюдении следующих требований:

эффективное использование информационных ресурсов в общественном производстве и для управления территорией;

обеспечение необходимого уровня информационной безопасности субъектов информационных отношений;

обеспечение структурной и функциональной устойчивости системы информационных ресурсов органов государственной власти и органов местного самоуправления;

обеспечение экономической эффективности пользования информационными ресурсами;

вхождение информационных ресурсов федеральных, муниципальных и иных информационных систем, расположенных на территории Курской области, в ЕИКС Курской области.

13.2. Формирование информационных ресурсов ЕИКС Курской области производится на основе:

единой системы правового регулирования информационных отношений на территории Курской области;

унификации системы документов и правил документирования на всей территории Курской области, ведения и применения регистров, кадастров, классификаторов, иных стандартов и нормативов в управлении информационными ресурсами;

единого порядка учета, регистрации, сертификации и лицензирования в системе формирования информационных ресурсов;

обеспечения потребителей достоверной, полной информацией;

обеспечения совместимости информационных ресурсов в информационных системах органов государственной власти Курской области и органов местного самоуправления, организаций и общественных объединений.

13.3. Информационные ресурсы ЕИКС Курской области формируются на основе информации, создаваемой, обрабатываемой и накапливаемой в процессе:

деятельности органов государственной власти Курской области, органов местного самоуправления, государственных (муниципальных) учреждений, иных организаций;

информационного взаимодействия органов государственной власти Курской области с федеральными органами государственной власти, с органами государственной власти других субъектов Российской Федерации, организациями и гражданами.

13.4. В случае принятия решения о прекращении деятельности Оператора информационной системы, данный Оператор информационной системы самостоятельно определяет порядок передачи информации, содержащейся в базах данных информационной системы, иному Оператору информационной системы и (или) порядок дальнейшего использования такой информации.

13.5. Лица, уполномоченные создавать и формировать информационные ресурсы, предназначенные для использования в ЕИКС Курской области, несут дисциплинарную, гражданско-правовую, административную и уголовную ответственность за предоставление несоответствующей информации и несоблюдение требований по информационной безопасности в соответствии с действующим законодательством Российской Федерации.

13.6. Порядок получения Абонентами ЕИКС Курской области информации (указание места, времени, ответственных должностных лиц, необходимых процедур) определяет Оператор информационной системы с соблюдением требований, установленных настоящим Регламентом.

13.7. Использование сведений информационных систем должно соответствовать правовому режиму, установленному федеральным законодательством и законодательством Курской области.

Объектами правового режима являются:

информация, составляющая информационные ресурсы;

программные и иные средства организации (представления) информации в информационных системах;

материальные (бумажные, магнитные, оптические и иные) носители информации, составляющей информационные ресурсы, а также иные технические средства обеспечения информационных систем.

Использование указанных объектов в нарушение установленного правового режима не допускается.

13.8. Участник ЕИКС Курской области обеспечивает неразглашение Абонентами ЕИКС Курской области информации, к которой будет получен доступ в связи с выполнением своих обязанностей.

13.9. Использование государственных информационных ресурсов в интересах органов государственной власти Курской области,

информационное взаимодействие между органами государственной власти Курской области, органами местного самоуправления, территориальными органами федеральных органов исполнительной власти, государственными (муниципальными) учреждениями по вопросам их компетенции и деятельности производятся на безвозмездной основе. Финансирование мероприятий по созданию и эксплуатации государственных информационных ресурсов производится за счет средств, направляемых на финансирование деятельности указанных органов (организаций) или соответствующих программ.

13.10. Порядок накопления, обработки, использования информации и порядок доступа к ней определяются Оператором информационной системы в пределах своей компетенции в соответствии с законодательством Российской Федерации.

14. Ситуационный центр Губернатора Курской области (межведомственная информационная служба) и его взаимодействие с информационными службами органов, учреждений и организаций

СЦ ГКО предназначен для обеспечения информационно-аналитической поддержки принятия управленческих решений на основе интеграции, регулярного, бесперебойного представления и анализа достоверной и актуальной информации о социально-экономической и общественно-политической ситуации в Курской области.

СЦ ГКО должен соответствовать требованиям Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», распорядительных и методических документов федеральных органов исполнительной власти, уполномоченных в области информационной безопасности.

Обеспечение информационной безопасности оборудования ИС СЦ ГКО должно осуществляться по требованиям нормативных и методических документов ФСБ России и ФСТЭК России.

СЦ ГКО должен проектироваться в качестве элемента Системы распределенных ситуационных центров (далее - СР СЦ), предназначенного для обеспечения деятельности Губернатора Курской области и Администрации Курской области.

Проектирование взаимодействия СЦ ГКО в рамках СР СЦ выполняется по следующим направлениям:

с ситуационными центрами Президента Российской Федерации, Полномочного представителя Президента Российской Федерации в Центральном федеральном округе, Правительства Российской Федерации, Администрации Президента Российской Федерации и других федеральных органов исполнительной власти;

с органами исполнительной государственной власти Курской области;

с муниципальными образованиями Курской области;

с территориальными органами федеральных органов исполнительной власти Курской области;

с предприятиями и организациями.

В состав СЦ ГКО входят следующие подсистемы:

комплекс средств представления информации (КСПИ);

подсистема видеосвязи (включает в себя подсистему защищенной видеосвязи органов государственной власти Российской Федерации закрытого контура и подсистему видеоконференцсвязи Администрации Курской области (далее - ВКС АКО));

средства вычислительной техники;

кабельная подсистема передачи аудио -, видеосигналов;

транспортно - коммуникационные системы ЛВС;

ПО;

комплекс модулей информационно-аналитической подсистемы поддержки управления Курской областью, включая следующие:

а) подсистема сбора, хранения и управления информацией;

б) подсистема централизованного управления нормативно-справочной информацией;

в) подсистема поддержки управления Курской областью;

г) подсистема инструментальных средств анализа, прогнозирования и моделирования;

д) подсистема геоинформационных инструментальных программных средств;

е) подсистема представления информации;

ж) система обеспечения информационной безопасности.

Перечень объектов, с которыми взаимодействует СЦ ГКО в рамках СР СЦ:

Государственная информационная система Курской области, созданная на базе Типового регионального решения, государственная автоматизированная информационная система «Управление»;

Единая межведомственная информационно-статистическая система (ЕМИСС);

Электронный бюджет;

Автоматизированная информационная система «Госпрограммы»;

Федеральная государственная информационная система территориального планирования;

ИС в сфере управления государственными финансами Курской области (в том числе в сфере представления оперативных данных об исполнении бюджета региона, финансировании мероприятий государственных, целевых и адресных инвестиционных программ Курской области);

ИС органа исполнительной государственной власти Курской области по строительству и жилищно-коммунальному хозяйству;

ИС органа исполнительной государственной власти Курской области по имущественным и земельным отношениям субъекта Российской Федерации;

органы ЗАГС Курской области.

ПО автоматизированной ИС СЦ ГКО должно обладать компонентной (модульной) архитектурой, обеспечивающей возможность эволюционного развития, в частности, с учетом включения в состав средств информатизации новых объектов автоматизированной ИС СЦ ГКО.

Функционирование СЦ ГКО будет осуществляться на основании регламента СЦ ГКО, разработанного Администрацией ЕИКС Курской области при создании автоматизированной ИС СЦ ГКО.

15. Требования к классу защищенности информационных систем с ограниченным доступом. Требования к программно-аппаратным средствам защиты информации

Обеспечение защиты информации в информационных системах осуществляется в соответствии с приказами ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (далее - Приказ ФСТЭК России №17), 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» в зависимости от вида ИС.

Классификация ИС осуществляется на основании требований Приказа ФСТЭК России №17 и проводится в зависимости от значимости обрабатываемой в ней информации и масштаба ИС (федеральный, региональный, объектовый).

Устанавливаются три класса защищенности ИС, определяющие уровни защищенности содержащейся в ней информации. Самый низкий класс - третий, самый высокий - первый.

Требования к системе защиты информации ИС определяются в зависимости от класса защищенности ИС и угроз безопасности информации, включенных в модель угроз безопасности информации.

Класс защищенности определяется для ИС в целом и, при необходимости, для ее отдельных сегментов (составных частей). Требование к классу защищенности включается в техническое задание на создание ИС и (или) техническое задание (частное техническое задание) на создание системы защиты информации ИС, разрабатываемые с учетом ГОСТ 34.602 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы» (далее - ГОСТ 34.602), ГОСТ Р 51583 и ГОСТ Р 51624.

Класс защищенности ИС подлежит пересмотру при изменении масштаба ИС или значимости обрабатываемой в ней информации.

В случае обработки в ИС информации, содержащей персональные данные, необходимо определить уровень защищённости персональных данных в соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и соотнести его с ранее определенным классом защищенности в соответствии с Приказом ФСТЭК России №17 следующим образом:

для ИС 1 класса защищенности обеспечивают 1, 2, 3 и 4 уровни защищенности персональных данных;

для ИС 2 класса защищенности обеспечивают 2, 3 и 4 уровни защищенности персональных данных;

для ИС 3 класса защищенности обеспечивают 3 и 4 уровни защищенности персональных данных.

Если определенный в установленном порядке уровень защищенности персональных данных выше, чем установленный класс защищенности ИС, осуществляется повышение класса защищенности до значения, обеспечивающего выполнение определенного уровня защищенности персональных данных.

Для обработки конфиденциальной информации необходимо использовать технические и программные средства, удовлетворяющие установленным в соответствии с действующим законодательством требованиям, обеспечивающим защиту информации. Требования к программно-аппаратным средствам защиты информации государственных ИС устанавливаются в Приказе ФСТЭК России №17 в соответствии с определенным классом защищённости для ИС.

Для передачи информации по каналам связи, выходящим за пределы контролируемой зоны, необходимо использовать защищенные каналы связи, в том числе защищенные волоконно-оптические линии связи или предназначенные для этого криптографические средства защиты информации. Применяемые при этом средства защиты информации должны быть сертифицированы.

Подключение ИС операторов к ЕИКС Курской области должно осуществляться в соответствии с требованиями действующего законодательства в сфере защиты информации.

Средства защиты информации от несанкционированного доступа (СЗИ НСД), устанавливаемые на рабочие станции и серверы при обработке на них информации с ограниченным доступом, должны осуществлять:

идентификацию и аутентификацию пользователей при доступе к рабочим станциям и серверам внутренней ЛВС по идентификатору и паролю;

контроль доступа к ресурсам рабочих станций и серверов внутренней ЛВС на основе дискреционного принципа;

управление доступом к машинным носителям информации;

регистрацию доступа к ресурсам рабочих станций и серверов внутренней ЛВС, включая попытки НСД;

регистрацию фактов отправки и получения абонентом сообщений (файлов, писем, документов).

При этом СЗИ НСД должна запрещать запуск абонентом произвольных программ, не включенных в состав ПО рабочей станции или сервера.

16. Абоненты ЕИКС Курской области. Доступ к информационным ресурсам ЕИКС Курской области

Состав Абонентов ЕИКС Курской области и их допуск к информационным ресурсам ЕИКС Курской области устанавливаются по письменному разрешению Администрации ЕИКС Курской области, которое дается по рассмотрению заявки Участника ЕИКС Курской области (приложение №7 или №8 к настоящему Регламенту) и строго контролируется. Поступившие заявки подлежат обязательной регистрации в течение 2 рабочих дней со дня их поступления.

В случае необходимости Администрация ЕИКС Курской области вправе запрашивать дополнительную информацию у Участника ЕИКС Курской области, подавшего заявку на предоставление или прекращение доступа к информационным ресурсам ЕИКС Курской области.

Администрация ЕИКС Курской области в течение 14 рабочих дней со дня регистрации заявки принимает решение о возможности предоставления или прекращения доступа к информационным ресурсам ЕИКС Курской области, указанных в заявке.

В случае принятия положительного решения Администрация ЕИКС Курской области в течение 5 рабочих дней со дня принятия решения предоставляет или прекращает доступ к соответствующим информационным ресурсам ЕИКС Курской области и в течение 3 рабочих дней с момента предоставления или прекращения доступа направляет на адрес электронной почты Участника ЕИКС Курской области, указанный в заявке, уведомление о предоставлении или прекращении доступа. В случае отсутствия в заявке адреса электронной почты Участника ЕИКС Курской области уведомление не направляется.

В случае отсутствия юридической или технической возможности предоставления Участнику ЕИКС Курской области доступа к информационной системе Администрация ЕИКС Курской области принимает отрицательное решение, о котором информирует Участника ЕИКС Курской области в течение 5 рабочих дней со дня принятия решения.

Участник ЕИКС Курской области имеет доступ только к тем информационным ресурсам ЕИКС Курской области, которые разрешены для него.

Каждый Абонент ЕИКС Курской области должен иметь уникальные идентификаторы и пароли для доступа к информационным ресурсам ЕИКС Курской области, при этом Абоненты ЕИКС Курской области должны нести ответственность за сохранность своих идентификаторов и паролей.

Администратор ЕИКС Курской области, Локальные администраторы Участника ЕИКС Курской области, Абоненты ЕИКС Курской области несут персональную ответственность за нарушения порядка автоматизированной обработки информации, правил хранения, использования и передачи находящихся в их распоряжении защищаемых ресурсов системы.

17. Единый электронный документооборот. Почтовые системы. Использование юридически значимого документооборота в ЕИКС Курской области

Настоящий раздел регламентирует общие правила использования почтовых систем и ЭП для обеспечения единого электронного документооборота между участниками информационного взаимодействия.

Виды ЭП, используемых органами исполнительной власти Курской области, порядок их использования, а также требования об обеспечении совместимости средств ЭП при организации электронного взаимодействия указанных органов между собой устанавливает Правительство Российской Федерации.

Участники информационного взаимодействия в рамках действующего законодательства признают юридическую значимость документов, подписанных ЭП, наряду с бумажными документами, при наличии всех обязательных реквизитов.

Правила выдачи, приостановления действия и аннулирования сертификата ключа подписи устанавливаются действующим законодательством Российской Федерации. ЭП используется Участниками ЕИКС Курской области, которым выданы сертификаты ключа подписи удостоверяющим центром органов государственной власти Курской области (далее - УЦ ОГВ). Наряду с подписями УЦ ОГВ могут использоваться ЭП, выданные другими удостоверяющими центрами, созданными в рамках действующего законодательства и имеющими кросс-сертификацию с УЦ ОГВ.

Участники информационного взаимодействия для приема и отправки корреспонденции в электронной форме используют общепринятые почтовые системы, позволяющие применять технологии ЭП, используемые в удостоверяющем центре.

Для обеспечения поэтапного перехода на электронный документооборот Участникам ЕИКС Курской области рекомендуется придерживаться следующих правил преобразования электронной и бумажной формы документов:

1) при поступлении документа в электронной форме лицу, ответственному за получение и отправку электронной почты, необходимо выполнить следующие действия:

а) произвести проверку юридической значимости принимаемого документа, т.е. наличие сертификата ключа подписи:

проверить срок действия сертификата ключа подписи;

в случае если сообщение зашифровано, произвести расшифровку документа;

б) сохранить электронное сообщение с ЭП в соответствующем электронном хранилище;

в) отослать отправителю сообщения информацию о получении документа;

г) распечатать основной документ;

д) проставить на бумажной форме документа штамп и внести данные о дате и времени отправки сообщения, дате и времени получения документа в электронной форме и подтвердить данную информацию своей подписью;

е) передать документ в подразделение, ответственное за прием и регистрацию документов, в бумажной форме для дальнейшей работы;

2) при отправке юридически значимого документа в электронной форме лицу, ответственному за получение и отправку электронной почты, отправителем должны быть предоставлены электронная и бумажная форма данного документа. При отправке электронной корреспонденции оператор должен выполнить следующие действия:

а) создать сообщение с указанием получателя, вложив файл в электронной форме и определив тему пересылаемого сообщения;

б) при необходимости зашифровать документ в электронной форме;

в) подписать ЭП;

г) проставить на бумажной форме документа штамп и внести данные о дате и времени отправки сообщения, электронном адресе респондента, а также времени приема подтверждения от него получения сообщения. Подтвердить данную информацию своей подписью;

д) передать документ в подразделение, ответственное за отправку и регистрацию документов, в бумажной форме для дальнейшей работы.

Каждый участник ЕИКС Курской области может дополнить правила, указанные в настоящем разделе, в соответствии с инструкцией по делопроизводству, применяемой в каждом конкретном Участке ЕИКС Курской области.

18. Требования по подключению ЕИКС Курской области к информационным средам, не входящим в состав ЕИКС Курской области, в том числе к сетям общего доступа

Подключение ЕИКС Курской области или Участков ЕИКС Курской области к информационным средам, не входящим в состав ЕИКС Курской области, в том числе к сетям общего доступа (далее - внешние сети) осуществляется по решению Администрации ЕИКС Курской области на основании заявки, которая содержит следующие обоснования необходимости подключения ЕИКС Курской области к внешним сетям:

наименование внешней сети, к которой осуществляется подключение, и реквизиты организации-владельца сети и провайдера сети;

состав технических средств Участка ЕИКС Курской области;

предполагаемые виды работ и используемые прикладные сервисы сети (E-Mail, FTP, Telnet, HTTP и т.п.) ЕИКС (или ее Участка ЕИКС Курской области) в целом и для каждого абонента в частности;

состав общего и телекоммуникационного ПО Участка ЕИКС Курской области (ОС, клиентские прикладные программы для сети и т.п.);

IP-адрес абонентского пункта в случае его расположения за районным координатором;

число и перечень предполагаемых абонентов (диапазон используемых IP-адресов);

меры и средства защиты информации от НСД, которые будут применяться на Участке ЕИКС Курской области, организация-изготовитель, сведения о сертификации, установщик, конфигурация, правила работы с ними;

тематика (перечень) сведений, обрабатываемых (хранимых) на рабочих станциях и серверах Участка ЕИКС Курской области, подлежащих передаче и получаемых из внешней сети, с указанием уровня конфиденциальности (служебная, коммерческая тайна и т.п.).

Заявка о подключении Участка ЕИКС Курской области к внешней сети направляется в Администрацию ЕИКС Курской области.

Подключение Участка ЕИКС Курской области к внешней сети должно осуществляться через средства разграничения доступа в виде межсетевых экранов. Не допускается подключение к внешней сети в обход межсетевого экрана. Межсетевые экраны должны быть сертифицированы по требованиям безопасности информации.

Доступ к межсетевому экрану, к средствам его конфигурирования должен осуществляться только выделенным администратором с консоли. Средства удаленного управления должны быть исключены из конфигурации.

Межсетевой экран должен обеспечивать создание сеансов связи абонентов с внешними серверами сети и получать с этих серверов только ответы на запросы пользователей ЕИКС Курской области. Настройка

межсетевого экрана должна обеспечивать отказ в обслуживании любых внешних запросов, которые могут направляться к пользователям ЕИКС Курской области.

При использовании почтового сервера и Web-сервера Участка ЕИКС Курской области последние не должны входить в состав локальной вычислительной сети организации и должны подключаться к внешней сети по отдельному сетевому фрагменту (через маршрутизатор).

На технических средствах Участка ЕИКС Курской области должно находиться ПО только в той конфигурации, которая необходима для выполнения работ, заявленных в обосновании необходимости подключения Участка ЕИКС Курской области к внешней сети (обоснование может корректироваться в установленном порядке).

В ПО должны быть физически удалены не нужные для работы и не включенные в обоснование прикладные сервисы (протоколы) и не требующиеся привязки протоколов к портам.

Установку ПО, обеспечивающего функционирование Участка ЕИКС Курской области, должны выполнять Локальные администраторы. Абоненты ЕИКС Курской области не имеют права производить самостоятельную установку указанного ПО, однако могут обращаться к Локальному администратору для проведения его экспертизы на предмет улучшения характеристик, наличия вирусов, замаскированных возможностей выполнения непредусмотренных действий. Ответственность за использование не прошедшего экспертизу и не рекомендованного к использованию ПО возлагается на Абонента ЕИКС Курской области. При обнаружении фактов такого рода Локальный администратор обязан логически (а при необходимости - физически вместе с включающей подсетью) отключить рабочее место Абонента ЕИКС Курской области от внешней сети и локальной вычислительной сети и поставить об этом в известность руководителя Участника ЕИКС Курской области.

В случае несанкционированного изменения настроек ПО Участник ЕИКС отключается от ЕИКС Курской области.

Устанавливаемые межсетевые экраны должны соответствовать классу защищенности ГИС и должны быть сертифицированы в соответствии с приказом ФСТЭК России от 9 февраля 2016 г. № 9 «Об утверждении требований к межсетевым экранам».

В информационных (автоматизированных) системах, созданных до вступления в силу Приказа ФСТЭК России № 17, допускается применение межсетевых экранов, сертифицированных на соответствие РД МЭ (при условии наличия действующих сертификатов соответствия требованиям по безопасности информации). При проведении повторной аттестации (после окончания срока действия аттестата соответствия) ИС допускается применение эксплуатируемых межсетевых экранов, сертифицированных на соответствие требованиям РД МЭ (при условии наличия на них действующих сертификатов соответствия).

СЗИ НСД, устанавливаемые на рабочие станции и серверы внутренней локальной вычислительной сети при обработке на них информации с ограниченным доступом, должны осуществлять:

идентификацию и аутентификацию пользователей при доступе к рабочим станциям и серверам внутренней локальной вычислительной сети (ЛВС) по идентификатору и паролю;

контроль доступа к ресурсам рабочих станций и серверов внутренней ЛВС на основе дискреционного принципа;

управление доступом к машинным носителям информации;

регистрацию доступа к ресурсам рабочих станций и серверов внутренней ЛВС, включая попытки НСД;

регистрацию фактов отправки и получения абонентом сообщений (файлов, писем, документов) и другие функции в соответствии с выбранным классом защиты.

Модификация конфигурации ПО Участка ЕИКС Курской области должна быть доступна только со стороны администратора Участка ЕИКС Курской области, ответственного за эксплуатацию Участка ЕИКС Курской области.

Средства регистрации и регистрируемые данные должны быть недоступны для пользователя.

СЗИ НСД должны быть целостны, т.е. защищены от несанкционированной модификации, и не содержать путей обхода механизмов контроля.

Технические средства Участка ЕИКС Курской области должны быть размещены в рабочих помещениях пользователей с принятием организационных и технических мер, исключающих несанкционированную работу во внешней сети.

При подключении Участка ЕИКС Курской области у внешней сети рекомендуется:

размещать межсетевые экраны для связи с внешней сетью, Web-серверы, почтовые серверы в отдельном контролируемом помещении, доступ в которое имел бы ограниченный круг лиц (ответственные специалисты, администраторы);

периодически проверять работоспособность межсетевого экрана с помощью сканеров, имитирующих внешние атаки на внутреннюю ЛВС. Не рекомендуется устанавливать на межсетевой экран какие-либо другие прикладные сервисы (СУБД, E-mail, прикладные серверы и т.п.);

при предоставлении пользователям прикладных сервисов исходить из принципа минимальной достаточности;

при подключении Участка ЕИКС Курской области к внешним сетям следует использовать операционные системы со встроенными функциями защиты информации от НСД или использовать сертифицированные СЗИ НСД;

эффективно использовать имеющиеся в маршрутизаторах средства разграничения доступа (фильтрацию), включающие контроль по списку доступа, аутентификацию пользователей, взаимную аутентификацию маршрутизаторов;

в целях контроля за правомерностью использования подключения к внешней сети и выявления нарушений требований по защите информации осуществлять систематический анализ принимаемой из внешней сети и передаваемой во внешнюю сеть информации, в том числе на наличие вирусов;

проводить постоянный контроль информации, помещаемой на Web-серверы. Для этого следует назначить ответственного (ответственных) за ведение информации на Web-сервере. Предусмотреть порядок размещения на Web-сервере информации, разрешенной к открытому опубликованию.

Администрацией ЕИКС Курской области назначаются лица, допущенные к работам во внешней сети с соответствующими полномочиями, лица, ответственные за эксплуатацию указанного Участка ЕИКС Курской области и контроль над выполнением мероприятий по обеспечению безопасности информации при работе пользователей во внешней сети.

Вопросы обеспечения безопасности информации на Участке ЕИКС Курской области должны быть отражены в инструкции, определяющей:

порядок подключения и регистрации абонентов во внешней сети;

порядок установки и конфигурирования на Участке ЕИКС Курской области общесистемного (ОС), прикладного, коммуникационного ПО (серверов, маршрутизаторов, шлюзов, мостов, межсетевых экранов, браузеров), их новых версий;

порядок применения средств защиты информации от НСД на Участке ЕИКС Курской области при взаимодействии абонентов с внешней сетью;

порядок работы абонентов во внешней сети, в том числе с электронной почтой (E-mail), порядок выбора и доступа к внутренним и внешним серверам сети (Web-серверам);

обязанности и ответственность абонентов и администратора внутренней ЛВС по обеспечению безопасности информации при взаимодействии с внешней сетью;

порядок контроля за выполнением мероприятий по обеспечению безопасности информации и работой абонентов во внешней сети.

Органы исполнительной власти Курской области в соответствии с постановлением Губернатора Курской области от 10.12.2004 № 566 «Об утверждении Инструкции по защите конфиденциальной информации на объектах информатизации органов исполнительной власти Курской области» обязаны организовывать подключение к сети «Интернет» только через централизованный и защищенный канал уполномоченного органа исполнительной власти Курской области в сфере развития и использования

информационных технологий на территории Курской области (региональной информатизации) и обеспечения защиты информации. Работа в сети «Интернет» осуществляется в соответствии с требованиями инструкции по работе в сети «Интернет». Текст Типовой инструкции по работе в сети «Интернет» представлен в приложении № 11 к настоящему Регламенту.

При работе во внешней сети категорически запрещается:

подключать технические средства (серверы, рабочие станции), имеющие выход во внешнюю сеть, к другим техническим средствам (сетям), не определенным в обосновании подключения к внешней сети;

изменять состав и конфигурацию программных и технических средств Участка ЕИКС Курской области без санкции Локального администратора.

Контроль за выполнением мероприятий по обеспечению безопасности информации на Участке ЕИКС Курской области возлагается на Локальных администраторов, руководителей соответствующих подразделений, определенных приказом Участника ЕИКС Курской области.

19. Требования при предоставлении доступа к сегментам ЕИКС Курской области сторонним организациям

К сегментам Курской области могут подключаться органы исполнительной власти, органы местного самоуправления и подведомственные учреждения. Сторонним организациям доступ к сегментам ЕИКС Курской области может быть предоставлен по решению Управляющего делами Администрации Курской области.

20. Контроль за обеспечением безопасности информационных ресурсов ЕИКС Курской области

Контроль за обеспечением безопасности информационных ресурсов ЕИКС Курской области осуществляется с целью своевременного выявления и предотвращения утечки информации по техническим каналам, несанкционированного доступа к ней, преднамеренных программно-технических воздействий на информацию и оценки эффективности ее защиты.

Контроль заключается в проверке выполнения участниками ЕИКС Курской области законодательства Российской Федерации по вопросам защиты информации, решений ФСТЭК России, а также в оценке обоснованности и эффективности принятых мер защиты информации.

При этом оценка эффективности мер защиты информации проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям по защите информации.

Контроль за обеспечением информационной безопасности ЕИКС Курской области осуществляют:

подразделение, ответственное за обеспечение информационной безопасности ЕИКС Курской области;

подразделения участников ЕИКС Курской области, ответственные за обеспечение информационной безопасности соответствующих Участков ЕИКС Курской области;

ФСТЭК России в пределах своей компетенции.

Контроль за обеспечением информационной безопасности в ЕИКС Курской области проводится подразделением в пределах своих полномочий не реже одного раза в год. Участники ЕИКС Курской области осуществляют контроль обеспечения информационной безопасности соответствующих Участков ЕИКС Курской области не реже одного раза в полгода.

Обеспечение информационной безопасности в ЕИКС Курской области считается эффективным, если принимаемые меры соответствуют установленным требованиям или нормам по защите информации. Несоответствие мер установленным требованиям или нормам по защите информации является нарушением.

Нарушения по степени важности делятся на три категории:

первая - невыполнение требований или норм по защите информации, в результате чего имелась или имеется реальная возможность ее утечки;

вторая - невыполнение требований по защите информации, в результате чего создаются предпосылки к ее утечке;

третья - невыполнение иных требований по защите информации.

21. Проведение работ по контролю защищенности ЕИКС Курской области. Установка и обслуживание средств технического контроля защищенности ЕИКС Курской области

Администрация ЕИКС Курской области имеет право:

1) отключать от ЕИКС Курской области Участников ЕИКС Курской области:

а) осуществивших попытку несанкционированного доступа к защищаемым ресурсам ЕИКС Курской области;

б) осуществивших попытку несанкционированного изменения настроек ПО и/или технических средств;

в) нарушивших установленные требования по информационной безопасности;

г) в случае заражения технических средств вредоносным ПО;

2) участвовать в проверках выполнения требований по информационной безопасности Участников ЕИКС Курской области;

3) запрещать устанавливать на серверах и рабочих станциях Участника ЕИКС Курской области нештатное программное и аппаратное обеспечение;

4) осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования средств защиты Участков ЕИКС Курской области;

5) запрашивать в установленном порядке обязанности Локального администратора по поддержанию уровня защиты Участка ЕИКС Курской области.

Администратор ЕИКС Курской области обязан:

участвовать в контрольных и тестовых испытаниях и проверках Участков ЕИКС Курской области;

вести контроль за процессом функционирования Ядра ЕИКС Курской области;

вносить предложения по совершенствованию уровня защиты ЕИКС Курской области;

оценивать возможность и последствия внесения изменений в состав ЕИКС Курской области с учетом требований нормативных документов по защите информации, подготавливать свои предложения;

запрещать и немедленно блокировать попытки изменения Участником ЕИКС Курской области программно-аппаратной среды Участка ЕИКС Курской области, если изменения произведены Участником ЕИКС Курской области без предварительного согласования с Администрацией ЕИКС Курской области;

запрещать и немедленно блокировать применение Абонентами ЕИКС Курской области ПО, с помощью которого возможны факты несанкционированного доступа к ресурсам ЕИКС Курской области;

анализировать состояние защиты Ядра ЕИКС Курской области;

контролировать состояние средств и систем защиты ядра ЕИКС Курской области;

оказывать консультационную помощь Абонентам ЕИКС Курской области в части применения средств защиты от НСД и других средств защиты;

своевременно анализировать журнал учета событий, регистрируемых средствами защиты Ядра ЕИКС Курской области, с целью выявления возможных нарушений.

22. Порядок согласования и внесения изменений в Регламент

Дополнения и изменения в настоящий Регламент (далее - изменения) разрабатываются Администрацией ЕИКС Курской области и (или) участниками информационного взаимодействия и утверждаются Губернатором Курской области.

При подготовке изменений участником информационного взаимодействия соответствующее предложение направляется в адрес Администрации ЕИКС Курской области для рассмотрения.

Администрация ЕИКС Курской области направляет сопроводительным письмом участникам информационного взаимодействия информацию о предлагаемом изменении. Участник информационного взаимодействия в сроки, указанные в сопроводительном письме, представляет заключение о предлагаемом изменении в Администрацию ЕИКС Курской области. В случае предоставления отрицательного заключения участником информационного обмена данное заключение должно содержать четкое и мотивированное обоснование отказа.

Администрация ЕИКС Курской области проводит анализ поступивших заключений участников информационного взаимодействия. На основании результатов проведенного анализа дается заключение о принятии предложения о внесении изменений в настоящий Регламент. Предложение о внесении изменений считается принятым при наличии более 50% положительных заключений из числа поступивших.

В случае положительного заключения по предложению о внесении изменений Администрацией ЕИКС Курской области подготавливается проект правового акта, который представляется Губернатору Курской области.

В случае отрицательного заключения по предложению о внесении изменений Администрация ЕИКС Курской области в двухнедельный срок информирует об этом участника информационного взаимодействия, представившего изменения.

Сроки предоставления в Администрацию ЕИКС Курской области заключений на предложения о внесении изменений:

без ограничительной пометки - в течение 30 календарных дней со дня получения предложения об изменении;

срочно - в течение двух недель со дня получения предложения об изменении;

весьма срочно - в течение одной недели со дня получения предложения об изменении.

Приложение № 1
к Регламенту использования
Единой информационной
коммуникационной среды Курской области

СОГЛАШЕНИЕ
ОБ ОБЕСПЕЧЕНИИ ДОСТУПА К ЕИКС КУРСКОЙ ОБЛАСТИ

г.Курск «__»_____20__г.

Администрация Курской области в лице _____
_____,
именуемая в дальнейшем «Администрация ЕИКС Курской области», с одной стороны, и _____ в лице _____ именуемое в дальнейшем «Участник ЕИКС Курской области», с другой стороны, вместе именуемые «Стороны», заключили настоящее Соглашение о нижеследующем:

1. Предмет Соглашения

1.1. В силу настоящего Соглашения Администрация ЕИКС Курской области обеспечивает доступ Участника ЕИКС Курской области к информационным ресурсам ЕИКС Курской области и оказывает Участнику ЕИКС Курской области определенные в пункте 1.2 настоящего соглашения услуги, а Участник ЕИКС Курской области принимает на себя обязательства по соблюдению положений и требований Регламента использования Единой информационной коммуникационной среды Курской области (далее – Регламент).

1.2. Перечень предоставляемых Администрацией ЕИКС Курской области услуг:

№ п/п	Наименование услуг
1.	
2.	
3.	

1.3. Отмеченные Участником ЕИКС Курской области услуги оказываются Администрацией ЕИКС Курской области в соответствии с условиями, определенными в соответствующих статьях настоящего Соглашения.

1.4. Проведение работ, перечисленных в пункте 1.2 настоящего Соглашения, производится при наличии технической возможности проведения данных работ и в соответствии с требованиями Регламента.

1.5. Перечень информационных ресурсов, к которым предоставляется доступ Участнику ЕИКС Курской области, определяется в соответствии с заявкой, одобренной Администрацией ЕИКС Курской области.

1.6. Доступ Участника ЕИКС Курской области к ЕИКС Курской области осуществляется Администрацией ЕИКС Курской области в соответствии с Регламентом ЕИКС Курской области.

2. Права и обязанности Сторон

2.1. Администрация ЕИКС Курской области вправе:

2.1.1. Проводить регламентные работы с приостановкой доступа Участника ЕИКС Курской области к ресурсам ЕИКС Курской области на период проведения работ. При этом Администрация ЕИКС Курской области должна известить Участника ЕИКС Курской области о проведении данных работ не менее чем за 24 часа до начала проведения регламентных работ.

2.1.2. Приостановить доступ Участника ЕИКС Курской области к ресурсам ЕИКС Курской области в случае нарушения им утвержденных документов, регламентирующих работу ЕИКС Курской области, а также нарушения положений действующего законодательства на территории Российской Федерации.

2.1.3. В случае необходимости изменять условия подключения к ресурсам ЕИКС Курской области, предварительно уведомив об этом Участников ЕИКС Курской области.

2.2. Администрация ЕИКС Курской области обязана:

2.2.1. Обеспечить подключение Участника ЕИКС Курской области к ЕИКС Курской области и доступ к информационным ресурсам ЕИКС Курской области в соответствии с одобренной заявкой Участника ЕИКС Курской области.

2.2.2. Предоставлять Участникам ЕИКС Курской области необходимые идентификационные данные.

2.2.3. В соответствии со своими полномочиями принимать меры по защите информации при работе в ЕИКС Курской области и доступе к информационным ресурсам ЕИКС Курской области.

2.2.4. Незамедлительно информировать Участников ЕИКС Курской области и требовать принятия ими мер в случае обнаружения угроз информационной безопасности при работе в ЕИКС Курской области.

2.2.5. Своевременно информировать Участников ЕИКС Курской области обо всех изменениях, вносимых в структуру ЕИКС Курской области, а также документов, регламентирующих работу ЕИКС Курской области.

2.3. Участник ЕИКС Курской области вправе:

2.3.1. Получать доступ к информационным ресурсам ЕИКС Курской области в соответствии с документами, регламентирующими работу ЕИКС

Курской области, и в объеме, указанном в заявке Администрации ЕИКС Курской области.

2.3.2. В одностороннем порядке отказаться от доступа к информационным ресурсам ЕИКС Курской области после соответствующего письменного уведомления Администрации ЕИКС Курской области.

2.4. Участник ЕИКС Курской области обязан:

2.4.1. Строго соблюдать положения документов, регламентирующих работу ЕИКС Курской области.

2.4.2. Обеспечить сохранность и невозможность передачи третьим лицам идентификационных параметров, используемых в процессе работы в ЕИКС Курской области, или доступа к информационным ресурсам ЕИКС Курской области.

2.4.3. Принимать необходимые меры по защите информации при работе в ЕИКС Курской области или доступе к информационным ресурсам ЕИКС Курской области в соответствии со своими полномочиями.

2.4.4. Довести до всех Абонентов ЕИКС Курской области и обеспечить выполнение ими всех инструкций и правил работы в ЕИКС Курской области.

2.4.5. Незамедлительно устранять причины (как выявленные самим Участником ЕИКС Курской области, так и указанные Администрацией ЕИКС Курской области) нарушений информационной безопасности при работе в ЕИКС Курской области либо неправомерного использования информационных ресурсов ЕИКС Курской области третьими лицами.

3. Ответственность Сторон

Стороны несут ответственность за неисполнение обязанностей по настоящему Соглашению в соответствии с законодательством Российской Федерации.

4. Разрешение споров

Стороны принимают необходимые меры к тому, чтобы любые спорные вопросы и разногласия, которые могут возникнуть из настоящего Соглашения или в связи с ним, были урегулированы путем переговоров.

5. Обстоятельства и действия непреодолимой силы

5.1. Стороны освобождаются от ответственности за частичное или полное неисполнение обязательств, если такое неисполнение является следствием непреодолимой силы и их последствий: землетрясение, ураган, смерч, другие признанные официально стихийные бедствия, а также

военные действия, массовые заболевания, забастовки, ограничения перевозок, изменение существующего законодательства.

5.2. В случае действия обстоятельств непреодолимой силы срок выполнения настоящего Соглашения сторонами отодвигается соразмерно времени, в течение которого действуют обстоятельства непреодолимой силы и их последствия.

6. Срок действия Соглашения, условия его расторжения

6.1. Соглашение вступает в силу с момента его подписания и действует в течение 1 календарного года.

6.2 Действие настоящего Соглашения автоматически продлевается на следующий календарный год, если ни одна из сторон в течение 30 (тридцати) дней до истечения его срока в письменном виде не известит другую сторону о расторжении Соглашения.

6.3. Настоящее Соглашение может быть расторгнуто по соглашению Сторон.

7. Дополнительные условия

7.1. Все изменения и дополнения оформляются в письменном виде и подписываются уполномоченными представителями Сторон.

7.2. По всем вопросам, не урегулированным настоящим Соглашением, Стороны руководствуются действующим законодательством.

7.3. Настоящее Соглашение составлено в двух экземплярах, имеющих одинаковую юридическую силу, по одному для каждой из Сторон.

8. Адреса и подписи Сторон

«Администрация ЕИКС Курской области»	«Участник ЕИКС Курской области»
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

Приложение № 2
к Регламенту использования
Единой информационной
коммуникационной среды Курской области

Официальный бланк Претендента
Реквизиты письма

Председателю комитета
информатизации, государственных и
муниципальных услуг Курской
области

_____ *(ФИО)*

Уважаемый _____!

Прошу подключить _____ (наименование Претендента) к защищённой сети ViPNet ЕИКС Курской области для _____ (указать цель подключения к ЕИКС).

Число подключаемых абонентских пунктов – _____.

Перечень информационных систем, к которым необходим доступ: _____.

Лицо, ответственное за подключение, и контактный телефон: ФИО, номер телефона, адрес электронной почты

Подробная схема сети _____ (наименование Претендента) и копия договора от ____ 20 года № с _____ (наименование организации, с которой заключен договор на поставку программного обеспечения ViPNet Client) прилагается.

Должность руководителя _____ (ФИО)

М.П. (при наличии)

Приложение № 3
к Регламенту использования
Единой информационной
коммуникационной среды Курской области

_____
(наименование Участника ЕИКС Курской области/Претендента)

П Р И К А З

«___»_____20__г. №____

О назначении Локального администратора сети _____
_____ (наименование Участника ЕИКС Курской области/Претендента).

Для осуществления мер по пресечению несанкционированного доступа, администрирования и обеспечения бесперебойной работы информационных систем и Абонентских пунктов, принадлежащих _____ (наименование Участника ЕИКС Курской области/Претендента) и относящихся к защищённой сети ViPNet ЕИКС Курской области.

ПРИКАЗЫВАЮ:

1. Назначить Локальным администратором _____ (наименование Участника ЕИКС Курской области/Претендента):
_____ (ФИО) - _____ (должность).
2. В своей работе по выполнению функций Локального администратора _____ (наименование Участника ЕИКС Курской области/Претендента) руководствоваться:
- действующим законодательством Российской Федерации;
- регламентом использования ЕИКС Курской области
3. Контроль за исполнением приказа _____.

Должность руководителя _____ (ФИО)
М.П. (при наличии)

Приложение № 4
к Регламенту использования
Единой информационной
коммуникационной среды Курской области

_____

(наименование Участника ЕИКС Курской области/Претендента)

П Р И К А З

«___»_____20__г. №____

О назначении Абонентов Защищённой сети ViPNet ЕИКС Курской области

Для выполнения служебных обязанностей с использованием сервисов и информационных систем Защищённой сети ViPNet ЕИКС Курской области:

ПРИКАЗЫВАЮ:

1. Назначить Абонентами Защищённой сети ViPNet ЕИКС Курской области:

_____ (ФИО) - _____ (должность),
_____ (ФИО) - _____ (должность),
_____ (ФИО) - _____ (должность).

2. В своей работе Абонентам Защищённой сети ViPNet Курской области руководствоваться:

- действующим законодательством Российской Федерации;
- регламентом использования ЕИКС Курской области

3. Контроль за исполнением приказа _____.

Должность руководителя _____ (ФИО)

М.П. (при наличии)

Приложение № 5
к Регламенту использования
Единой информационной
коммуникационной среды Курской области

Соглашение
о конфиденциальности персональных данных

Я, _____ (фамилия, имя, отчество), понимаю, что получаю возможность доступа к персональным данным третьих лиц.

Я также понимаю, что во время исполнения своих обязанностей я буду заниматься обработкой персональных данных.

Я подтверждаю, что не имею права нарушать конфиденциальность информации о:

- анкетных и биографических данных;
- образовании;
- трудовом и общем стаже;
- составе семьи;
- паспортных данных;
- воинском учете;
- заработной плате;
- социальных льготах;
- специальности;
- занимаемой должности;
- наличии судимостей;
- адресе места жительства, домашнем телефоне;
- месте работы или учебы членов семьи и родственников;
- содержании трудового договора;
- составе декларируемых сведений о наличии материальных ценностей;
- содержании декларации, подаваемой в налоговую инспекцию;
- подлинниках и копиях приказов по личному составу;
- личных делах и трудовых книжках;
- делах, содержащих материалы по повышению квалификации и переподготовке, их аттестации, служебным расследованиям;
- копиях отчетов, направляемых в органы статистики.

Я понимаю, что нарушение конфиденциальности информации такого рода может нанести ущерб субъекту персональных данных, как прямой, так и косвенный.

Я предупрежден(а) о том, что в случае нарушения положений законодательства Российской Федерации в области персональных данных я несу ответственность в соответствии со ст. 90 ТК РФ.

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

«___»_____20__г.

Приложение № 6
к Регламенту использования
Единой информационной
коммуникационной среды Курской области

Доверенность
на получение дистрибутива ключей

(наименование населенного пункта) «_____»_____20__ г.

_____ (наименование Участника ЕИКС Курской области/Претендента) в лице _____ (должность, ФИО) уполномочивает: _____ (ФИО), паспорт _____ (серия, номер, кем и когда выдан) получить в комитете информатизации, государственных и муниципальных услуг Курской области дистрибутив ключей для первичного запуска прикладной программы сети ViPNet №1366.

Настоящая доверенность действительна по «___» _____ 20___г.

Подпись лица, получившего доверенность _____

Должность руководителя _____ (ФИО)

М.П. (при наличии)

Приложение № 7
к Регламенту использования
Единой информационной
коммуникационной среды Курской области

Официальный бланк Участника ЕИКС Курской области
Реквизиты письма

Председателю комитета
информатизации, государственных и
муниципальных услуг Курской
области

_____ (ФИО)

Уважаемый _____!

Прошу предоставить/прекратить доступ_____
_____(наименование Участника ЕИКС Курской области) для абонентских пунктов _____ (наименование абонентских пунктов при необходимости) к информационным ресурсам: _____ (название информационной системы (IP-адрес) или абонентских пунктов с указанием принадлежности к сети ViPNet №____).

Локальный администратор: ФИО, номер телефона, адрес электронной почты.

Должность руководителя _____ (ФИО)
М.П. (при наличии)

Приложение № 8
к Регламенту использования
Единой информационной
коммуникационной среды Курской области

Официальный бланк Участника ЕИКС Курской области
Реквизиты письма

Председателю комитета
информатизации, государственных и
муниципальных услуг Курской
области

_____ (ФИО)

Уважаемый _____!

Прошу предоставить/прекратить доступ _____ (наименование Участника ЕИКС Курской области) к информационным ресурсам: _____(название информационной системы, ip-адрес).

Перечень IP-адресов для который необходимо предоставить или прекратить доступ: _____ (по необходимости).

Локальный администратор: ФИО, номер телефона, адрес электронной почты.

Должность руководителя _____ (ФИО)

М.П. (при наличии)

Приложение № 9
к Регламенту использования
Единой информационной
коммуникационной среды Курской области

ПРОТОКОЛ
установления межсетевого взаимодействия
«____» _____ 20__г.

1. Межсетевое взаимодействие устанавливается между сетями:

Номер сети	Наименование организации
№_____	Полное наименование организации
№_____	Полное наименование организации

2. Целью установления межсетевого взаимодействия является межведомственное защищенное информационное взаимодействие ViPNet сетей указанных организаций.

3. Процедуру установления межсетевого взаимодействия осуществляли:

Номер сети	Должность	ФИО
№_____		
№_____		

4. Передача начального и ответного экспорта между сетями №___ и №___ осуществлялась через специалиста, уполномоченного на данные действия.

5. Для установления межсетевого взаимодействия использовался индивидуальный симметричный межсетевой мастер-ключ, созданный в сети №___.

6. Для установления межсетевого взаимодействия были назначены серверы-маршрутизаторы для организации шлюза:

в сети №___ - «_____»

в сети №___ - «_____»

7. При установлении межсетевого взаимодействия в части ЭЦП были произведены импорты справочников ЭЦП главных абонентов сети №___ и №___.

8. Смена межсетевых ключей, изменение состава АП, участвующих в межсетевом взаимодействии, производится после предварительного согласования средствами взаимного экспорта/импорта, о чём администраторы защищённых сетей уведомляют друг друга с помощью ПО ViPNet [Клиент] [Делова почта] с указанием производимых изменений.

9. Стороны обязуются без предварительного согласия не производить изменений в настройках и структуре защищённых сетей, могущих привести к нарушению межсетевого взаимодействия.

Администратор сети ViPNet №_____	Администратор сети ViPNet №_____
_____ (ФИО)	_____ (ФИО)
_____ (подпись)	_____ (подпись)
«_____»_____20___г.	«_____»_____20___г.
М.П. (при наличии)	М.П. (при наличии)

Приложение № 10
к Регламенту использования
Единой информационной
коммуникационной среды Курской области

Официальный бланк Участника ЕИКС Курской области
Реквизиты письма

Председателю комитета
информатизации,
государственных и
муниципальных услуг
Курской области
_____ (ФИО)

Уважаемый _____!

Прошу перевыпустить dst-файл для узла _____ (наименование узла) по причине _____ (указать причину, по которой требуется перевыпустить дистрибутив).

Должность руководителя _____ (ФИО)
М.П. (при наличии)

Приложение № 11
к Регламенту использования
Единой информационной
коммуникационной среды Курской области

ТИПОВАЯ ИНСТРУКЦИЯ ПО РАБОТЕ В СЕТИ «ИНТЕРНЕТ»

1. Общие положения

1.1. Настоящая Инструкция устанавливает порядок использования средств вычислительной техники и связи для выхода в сеть «Интернет». Инструкция разработана с учетом требований Федерального закона «Об информации, информационных технологиях и о защите информации», а также действующих руководящих документов по организации работ в области защиты информации, обрабатываемой на объектах вычислительной техники и средств связи, в органах исполнительной власти Курской области.

1.2. Инструкция обязательна для выполнения в органах исполнительной власти Курской области.

2. Общие требования к порядку использования средств вычислительной техники и связи при работе в сети «Интернет»

2.1. Для работы на конкретном объекте средств вычислительной техники и связи при работе в сети «Интернет» допускаются лица, внесенные в список пользователей, допущенных к работе на объектах вычислительной техники и средств связи, который утверждается руководителем уполномоченного органа исполнительной власти Курской области в сфере развития и использования информационных технологий на территории Курской области (региональной информатизации и обеспечения защиты информации) (далее - уполномоченный орган).

В списке указываются фамилия, имя, отчество пользователей и их должности.

2.2. Технические средства должны эксплуатироваться с соблюдением требований, указанных в руководстве пользователя производителя технического средства.

2.3. Исходящая корреспонденция, отправляемая открытыми каналами электронной почты (e-mail сети «Интернет»), подлежит строгому учету.

2.4. Подключение информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи сведений, составляющих служебную тайну, к информационно - телекоммуникационным сетям международного информационного обмена производится только с использованием специально предназначенных для этого средств защиты

информации, в том числе шифровальных (криптографических) средств, прошедших в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю. Выполнение данного требования является обязательным для операторов ЕИКС.

2.5. В целях защиты общедоступной информации, размещаемой в информационно-телекоммуникационных сетях международного информационного обмена, используют только средства защиты информации, прошедшие в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получившие подтверждение соответствия в Федеральной службе по техническому и экспортному контролю.

2.6. Запрещается работа со служебной информацией на рабочем месте без проведения работ по защите информации. Для недопущения несанкционированного доступа к сети «Интернет» лиц, не включенных в список, должен быть установлен пароль на загрузку операционной системы. Указанный пароль, а также пароли, используемые для доступа к информационным и вычислительным сетям, должны держаться в тайне. Ответственность за работу с внешними носителями информации возлагается на оператора АРМ.

3. Работа в вычислительных сетях

3.1. Установка протоколов, имена компьютеров определяются системным администратором. Самостоятельная смена настроек и протоколов запрещена.

3.2. Компьютеры, которые обрабатывают информацию конфиденциального характера, не могут быть подсоединены к вычислительным и информационным сетям общего пользования без предварительного проведения работ по защите информации от несанкционированного доступа в соответствии с действующим законодательством по вопросам защиты информации.

4. Доступ к ресурсам сети «Интернет»

4.1. Для выполнения задач, связанных с исполнением служебных обязанностей, пользователю предоставляется доступ к ресурсам сети «Интернет». Доступ к ресурсам сети «Интернет» в других целях запрещен.

4.2. Доступ предоставляется пользователю на основании заявки от руководителя подразделения в адрес уполномоченного органа.

4.3. Доступ к ресурсам сети «Интернет» блокируется системным администратором уполномоченного органа без предварительного уведомления.

4.4. При возникновении нештатных ситуаций уполномоченный орган оставляет за собой право ограничивать доступ к ресурсам сети «Интернет», содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены международным и российским законодательством.

5. Правила работы с ресурсами сети «Интернет»

5.1. При работе с ресурсами сети «Интернет» недопустимы:

разглашение сведений конфиденциального характера, ставших известными пользователю по служебной необходимости либо иным путем;

распространение защищенных авторскими правами материалов, затрагивающих патент, торговую марку, коммерческую тайну, копирайт или иные права собственности и/или авторские и смежные права третьей стороны;

публикация, загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам сети «Интернет», а также размещения ссылок на вышеуказанную информацию.

5.2. При работе с ресурсами сети «Интернет» запрещено:

загружать и запускать файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом;

использовать анонимные прокси-серверы;

использовать программные и аппаратные средства, позволяющие получить доступ к ресурсам сети «Интернет», запрещенным к использованию комитетом информатизации, государственных и муниципальных услуг Курской области;

сохранять пароль на компьютере (процедура используется для доступа к защищенному паролем ресурсу сети «Интернет», интрасети и т.д.), если компьютер используется несколькими пользователями.

6. Доступ к электронной почте

6.1. Для выполнения задач, связанных с исполнением служебных обязанностей, пользователю предоставляется доступ к электронной почте. Использование электронной почты в других целях запрещено.

6.2. Доступ к электронной почте предоставляется пользователю на основании заявки от руководителя структурного подразделения Администрации Курской области в адрес уполномоченного органа.

6.3. Содержимое электронного почтового ящика пользователя может быть проверено без предварительного уведомления по требованию непосредственного либо вышестоящего руководителя.

6.4. При возникновении нештатных ситуаций доступ к серверу электронной почты блокируется системным администратором уполномоченного органа без предварительного уведомления.

7. Правила работы с электронной почтой Администрации Курской области

7.1. При работе с электронной почтой Администрации Курской области запрещено:

использовать адрес почты Администрации Курской области для оформления подписок без предварительного согласования с системным администратором уполномоченного органа;

открывать и сохранять исполняемые вложенные файлы (файлы, имеющие расширения exe, bat и т.п.), полученные от неизвестных отправителей, а также вложенные файлы с незнакомыми расширениями;

публиковать свой адрес либо адреса других пользователей на общедоступных интернет - ресурсах (форумы, конференции и т.п.);

отправлять сообщения с вложенными файлами, общий объем которых превышает 5 Мб, без предварительного согласования с системным администратором уполномоченного органа;

открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами;

осуществлять массовую рассылку почтовых сообщений (более 10) внешним адресатам без согласования с ними;

осуществлять рассылку почтовых сообщений рекламного характера без предварительного согласования с системным администратором уполномоченного органа;

осуществлять рассылку через электронную почту материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам сети «Интернет», а также ссылки на вышеуказанную информацию;

- распространять защищенные авторскими правами материалы, затрагивающие патент, торговую марку, коммерческую тайну, копирайт и иные права собственности и/или авторские и смежные права третьей стороны;

- распространять информацию, содержание и направленность которой запрещены международным и российским законодательством;
- распространять информацию ограниченного доступа;
- предоставлять пароль доступа к своему почтовому ящику.

8. Порядок установки и смены паролей

На компьютерах, используемых для обработки информации, устанавливаются пароли. Пароли устанавливаются самим пользователем или системным администратором уполномоченного органа. Идентификаторы (имена) и пароли для доступа к ресурсам локальных и глобальных вычислительных сетей определяются пользователем, ответственным за эксплуатацию вычислительной техники.