Государственная регистрация
от 18.06.2025 № ГР/457/2025

МИНИСТЕРСТВО ЦИФРОВЫХ ТЕХНОЛОГИЙ И СВЯЗИ КАЛИНИНГРАДСКОЙ ОБЛАСТИ

П Р И К А З

18 июня 2025 г. № 136
Калининград

Об утверждении регламента предоставления доступа к информационным ресурсам информационно-телекоммуникационной сети «Интернет» пользователям и подключения объектов единой информационно-телекоммуникационной сети Правительства Калининградской области

В целях обеспечения защиты информации, обрабатываемой в единой информационно-телекоммуникационной сети Правительства Калининградской области, руководствуясь подпунктом 4 статьи 18 Положения о единой информационно-телекоммуникационной сети Правительства Калининградской области, утвержденного постановлением Правительства Калининградской области от 4 июня 2018 года № 301, **п р и к а з ы в а ю**:

1. Утвердить прилагаемый регламент предоставления доступа к информационным ресурсам информационно-телекоммуникационной сети «Интернет» пользователям и подключения объектов единой информационно-телекоммуникационной сети Правительства Калининградской области.
2. Приказ подлежит государственной регистрации.
3. Приказ вступает в силу со дня его официального опубликования.

Исполняющая обязанности
министра А.Н. Голубых

УТВЕРЖДЕНО
приказом Министерства
цифровых технологий и связи
Калининградской области
от 18 июля 2023 № 136

РЕГЛАМЕНТ
предоставления доступа к информационным ресурсам информационно-телекоммуникационной сети «Интернет» пользователям и подключения объектов единой информационно-телекоммуникационной сети Правительства Калининградской области

Глава 1. Общие положения

1. Настоящий регламент предоставления доступа к информационным ресурсам информационно-телекоммуникационной сети «Интернет» пользователям и подключения объектов единой информационно-телекоммуникационной сети Правительства Калининградской области (далее – Регламент) определяет условия и порядок предоставления доступа пользователям и подключения объектов единой информационно-телекоммуникационной сети Правительства Калининградской области к информационным ресурсам информационно-телекоммуникационной сети «Интернет» (далее – сеть Интернет).

2. Нормативно-правовую основу Регламента составляют:

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

2) Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 года № 646;

3) Указ Президента Российской Федерации от 22 мая 2015 года № 260 «О некоторых вопросах информационной безопасности Российской Федерации» (далее – Указ № 260);

4) Указ Президента Российской Федерации от 17 марта 2008 года № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» (далее – Указ № 351);

5) Закон Калининградской области от 24 апреля 2018 года № 165 «О правовом регулировании отдельных вопросов в сфере создания, развития (модернизации) и эксплуатации государственных информационных систем Калининградской области»;

6) положение о единой информационно-телекоммуникационной сети Правительства Калининградской области, утвержденное постановлением Правительства Калининградской области от 04 июня 2018 года № 301 (далее – Постановление № 301);

7) политика информационной безопасности в Правительстве

Калининградской области, утвержденная постановлением Правительства Калининградской области от 01 октября 2024 года № 376-п.

3. В Регламенте применяются понятия, установленные действующим законодательством Российской Федерации в области информации, информационных технологий и защиты информации, а также следующие понятия, определения и сокращения:

1) АРМ – автоматизированное рабочее место, подключенное к ЕИТС самостоятельно или в составе информационного ресурса;

2) администратор защищенной сети ЕИТС – определенная уполномоченным органом организация (учреждение), на которую возложены полномочия администратора защищенной сети ЕИТС;

3) ЕИТС – единая информационно-телекоммуникационная сеть Правительства Калининградской области, функционирующая в соответствии с положением о единой информационно-телекоммуникационной сети Правительства Калининградской области, утвержденным Постановлением № 301;

4) опасный информационный ресурс – информационный ресурс, являющийся источником компьютерной атаки (вторжения) на ЕИТС, содержащий средства реализации компьютерных атак (вторжений) или иные программные средства и информацию, доступ к которым ограничен законодательством Российской Федерации;

5) оператор ЕИТС – определенная уполномоченным органом организация (учреждение), на которую возложены полномочия оператора ЕИТС;

6) объекты ЕИТС – информационные системы, аппаратное и программное обеспечение ЕИТС, использующие для своего функционирования доступ в сеть Интернет;

7) пользователи ЕИТС – участники информационного обмена, осуществляющие информационное взаимодействие посредством ЕИТС;

8) регуляторы – Федеральная служба по техническому и экспортному контролю, Федеральная служба безопасности Российской Федерации, Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций;

9) уполномоченный орган – уполномоченный орган по созданию, использованию и развитию ЕИТС, которым является исполнительный орган Калининградской области, осуществляющий функции в сфере информационных технологий, связи и массовых коммуникаций на территории Калининградской области.

Глава 2. Цели предоставления доступа к сети Интернет пользователям ЕИТС и подключения к сети Интернет объектов ЕИТС

4. Основными целями использования сети Интернет пользователями ЕИТС являются:

1) обеспечение реализации функций и полномочий пользователями ЕИТС, в том числе обеспечение свободного доступа к информации

о деятельности Правительства Калининградской области, исполнительных органов и органов местного самоуправления Калининградской области, подведомственных им организаций (учреждений) с применением информационных технологий;

2) поиск в сети Интернет и получение пользователями ЕИТС информации, информационных услуг и программных средств, необходимых для выполнения должностных обязанностей;

3) осуществление закупок товаров, работ и услуг для обеспечения государственных и муниципальных нужд, нужд пользователей ЕИТС;

4) обеспечение в служебных целях доступа к сторонним информационным системам и их сервисам, реализующим свой функционал посредством сети Интернет;

5) информационный обмен между пользователями ЕИТС посредством сети Интернет в рамках исполнения должностных обязанностей.

5. Основными целями подключения к сети Интернет объектов ЕИТС являются:

1) реализация основного функционала размещаемых в ЕИТС информационных систем и ресурсов посредством сети Интернет;

2) обновление баз данных информационных систем;

3) обновление ключевой информации и баз данных угроз и решающих правил систем защиты информации ЕИТС;

4) обновление микропрограммного обеспечения устройств и программно-аппаратных комплексов ЕИТС;

5) передача данных систем мониторинга и телеметрии внешним центрам обработки и анализа.

Глава 3. Угрозы информационной безопасности при использовании сети Интернет пользователями ЕИТС и подключении к сети Интернет объектов ЕИТС

6. Использование сети Интернет пользователями ЕИТС и подключение объектов ЕИТС к сети Интернет сопряжено со следующими угрозами информационной безопасности:

1) несанкционированный доступ к охраняемым законом сведениям, содержащимся в информационных системах, функционирующих в составе ЕИТС, с целью их добывания, искажения, уничтожения или блокирования к ним доступа;

2) загрузка канала передачи информации в/из сети Интернет на уровне его пропускной способности или выше, а также иные действия, нарушающие доступность данных, обрабатываемых в информационных системах, для авторизованных пользователей;

3) создание условий для внедрения или непосредственное внедрение в информационные системы вредоносного программного обеспечения;

4) утечка служебной и иной конфиденциальной информации за пределы

защищаемой зоны;

5) нарушение доступности информационно-вычислительных ресурсов ЕИТС;

6) нарушение целостности и достоверности открытых и общедоступных ресурсов ЕИТС, размещаемых в сети Интернет во исполнение требований действующего законодательства;

7) нарушение конфиденциальности, целостности и доступности информации ограниченного доступа, передаваемой по сети Интернет в защищенном виде.

Глава 4. Меры обеспечения информационной безопасности при использовании сети Интернет пользователями и подключении к сети Интернет объектов ЕИТС

7. Основными мерами по предотвращению реализации угроз информационной безопасности, указанных в главе 3 Регламента, являются:

1) разработка модели угроз безопасности ЕИТС, проектирование и создание системы защиты информации ЕИТС в соответствии с требованиями законодательства Российской Федерации и Калининградской области, нормативных правовых актов регуляторов;

2) взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

3) взаимодействие в автоматизированном режиме с Центром мониторинга и управления сетью связи общего пользования в рамках противодействия атакам, направленным на отказ в обслуживании;

4) взаимодействие и разграничение зон ответственности с лицами, предоставляющими услуги доступа ЕИТС к сети Интернет;

5) поддержание в актуальном состоянии баз данных угроз и решающих правил средств защиты информации (средств межсетевого экранирования, средств контроля и анализа данных, передаваемых по сети Интернет, средств анализа защищенности, средств защиты от несанкционированного доступа, средств антивирусной защиты, средств криптографической защиты информации, средств детектирования (предотвращения) вторжений (атак) из сети Интернет и вредоносного программного обеспечения и т.п.);

6) преимущественное размещение государственных информационных систем Калининградской области, а также, при необходимости и наличии достаточных оснований, иных информационных систем органов и организаций, независимо от их организационно-правовых форм и форм собственности, на ресурсах георасределенного вычислительного аппаратно-программного комплекса Правительства Калининградской области (метрокластера);

7) выработка и реализация организационных и технических мер по обеспечению информационной безопасности;

8) разработка и утверждение в установленном порядке необходимой организационно-распорядительной документации по обеспечению

информационной безопасности;

9) ограничение доступа пользователей ЕИТС и подключений объектов ЕИТС к опасным информационным ресурсам в сети Интернет;

10) контроль и анализ информации, передаваемой с использованием сети Интернет;

11) учет пользователей ЕИТС и объектов ЕИТС, имеющих доступ (подключение) к сети Интернет;

12) мониторинг и анализ данных о работе с ресурсами сети Интернет;

13) проведение мероприятий по оценке защищенности доступа в сеть Интернет.

Глава 5. Условия и порядок доступа (подключения) к сети Интернет

8. Подключение объектов ЕИТС к сети Интернет осуществляется на основании правового акта уполномоченного органа, в котором указываются цели, обоснование, технические параметры и требования к уровню защищенности канала (каналов) подключения ЕИТС к сети Интернет, и соглашения между оператором ЕИТС и исполнительным органом Калининградской области (органом местного самоуправление Калининградской области, организацией (учреждением).

9. Государственный контракт (далее – договор) с лицом, предоставляющим телекоммуникационный канал и услуги связи ЕИТС с сетью Интернет (далее – провайдер), должен содержать положения по обеспечению провайдером требований информационной безопасности, установленных федеральным законодательством, национальными стандартами и нормативными правовыми актами регуляторов.

10. Соглашение с исполнительным органом Калининградской области (органом местного самоуправления Калининградской области, организацией (учреждением) по подключению обособленных узлов к ЕИТС должно содержать положения о необходимости обеспечения выхода в сеть Интернет через инфраструктуру ЕИТС.

11. Организация пользователями ЕИТС дополнительных каналов выхода в сеть Интернет из АРМ и информационных систем, являющихся узлами ЕИТС, не допускается.

12. Оператор ЕИТС и администратор защищенной сети ЕИТС совместно с уполномоченным органом обеспечивают разработку технического задания, закупку, монтаж, ввод в эксплуатацию, защиту, эксплуатацию и вывод из эксплуатации аппаратно-программного комплекса, осуществляющего связь ЕИТС с сетью Интернет (далее – шлюз сети Интернет).

13. Требования к системе защиты шлюза сети Интернет разрабатываются оператором ЕИТС и утверждаются уполномоченным органом.

14. Оператор ЕИТС осуществляет ввод шлюза сети Интернет в эксплуатацию, обеспечивает наличие и ведение эксплуатационной документации на шлюз сети Интернет.

15. Эксплуатационная документация на шлюз сети Интернет должна,

в том числе содержать следующие сведения и документы:

1) фактический адрес (адреса) размещения оборудования шлюза сети Интернет;

2) данные о провайдере (провайдерах), предоставляющем (предоставляющих) услуги доступа к сети Интернет (наименование, юридический и фактический адрес, ИНН, ОГРН, ЕГРЮЛ/ЕГРИП, реквизиты договора о предоставлении услуг доступа, срок действия договора, контактные данные сотрудников провайдера, ответственных за бесперебойную работу канала связи, и сотрудников провайдера, отвечающих за работу систем защиты канала связи, тип используемого канала связи);

3) реестр объектов ЕИТС, подключенных к сети Интернет;

4) перечень пользователей ЕИТС, которым предоставлен доступ в сеть Интернет;

5) реестр примененных политик и правил ограничения доступа в сеть Интернет для пользователей ЕИТС и объектов ЕИТС;

6) режим подключения ЕИТС к сети Интернет (постоянный, в том числе круглосуточный, временный);

7) организационно-распорядительная документация администраторов шлюза сети Интернет;

8) перечень организационных и технических мер информационной безопасности, которые выполняются перед доступом (подключением) к сети Интернет и в процессе ее использования, в том числе правила контроля использования подключения к сети Интернет, журналирование доступа пользователей ЕИТС и объектов ЕИТС к ресурсам сети Интернет;

9) применяемые в составе шлюза сети Интернет средства защиты информации – наименование (производитель, модель), заводской (серийный) номер или номер лицензии, сведения о сертификате / аттестате соответствия ФСБ России / ФСТЭК России (дата выдачи и номер);

10) схема подключения ЕИТС к сети Интернет посредством шлюза сети Интернет с указанием точек выхода в сеть Интернет, а также используемое для взаимодействия с сетью Интернет оборудование и программное обеспечение;

11) правила разграничения доступа сотрудников уполномоченного органа, оператора ЕИТС и администратора защищенной сети ЕИТС к шлюзу сети Интернет;

12) матрица взаимодействия ответственных за эксплуатацию шлюза сети Интернет сотрудников оператора ЕИТС и провайдера (провайдеров);

13) порядок контроля работы шлюза сети Интернет сотрудниками уполномоченного органа, оператора ЕИТС и администратора защищенной сети ЕИТС;

14) перечень сведений ограниченного доступа и конфиденциального характера, подлежащих передаче и получению с использованием сети Интернет.

16. Ведение перечней и реестров, предусмотренных пунктом 15 настоящего Регламента, допускается в электронном формате, обеспечивающем возможность печати на бумажном носителе всех значимых информационных полей в удобочитаемом виде.

17. Расходы, связанные с функционированием шлюза сети Интернет, осуществляются в пределах лимитов бюджетных обязательств, выделяемых на функционирование ЕИТС.

18. Мероприятия по защите информации, передаваемой по каналам связи между ЕИТС и оконечным оборудованием провайдера услуг по доступу в сеть Интернет, а также по защите оборудования шлюза сети Интернет проводятся оператором ЕИТС по согласованию с уполномоченным органом в соответствии с требованиями федеральных законов и нормативных правовых актов регуляторов.

19. Оператор ЕИТС ведет реестры информационных ресурсов сети Интернет, к которым заблокирован или разрешен доступ пользователям ЕИТС и объектам ЕИТС. Реестры ежеквартально направляются в уполномоченный орган в электронном виде для организации учета и контроля. Регламент ведения реестров ресурсов сети Интернет, к которым заблокирован или разрешен доступ пользователям и объектам ЕИТС, разрабатывается оператором ЕИТС и согласовывается с руководителем уполномоченного органа.

20. При возникновении инцидентов информационной безопасности или получении достоверных данных о наличии предпосылок для реализации угроз информационной безопасности, обусловленных информационным обменом пользователей ЕИТС или объектов ЕИТС с ресурсами сети Интернет, оператор ЕИТС в целях недопущения нанесения ущерба ЕИТС может самостоятельно заблокировать доступ к опасным информационным ресурсам сети Интернет, после чего незамедлительно уведомляет руководство уполномоченного органа по любым доступным каналам связи о выявленной угрозе и принятых мерах с последующим направлением подробного письменного отчета в течение 48 часов.

После ликвидации причин блокирования ресурса сети Интернет оператор ЕИТС в течение 24 часов восстанавливает доступ к данному ресурсу сети Интернет, о чем уведомляет руководство уполномоченного органа.

Глава 6. Полномочия субъектов взаимодействия в рамках предоставления доступа к информационным ресурсам сети Интернет пользователям ЕИТС и подключения объектов ЕИТС

21. Уполномоченный орган:

1) осуществляет контроль за соответствием применяемых решающих правил и настроек шлюза сети Интернет требованиям законодательства Российской Федерации, нормативных правовых документов государственных органов, требованиям и регламентам эксплуатации ЕИТС;

2) утверждает списки администраторов шлюза сети Интернет и иных лиц, имеющих доступ к оборудованию шлюза сети Интернет;

3) разрабатывает и обеспечивает проведение мероприятий по вводу в эксплуатацию, эксплуатации, развитию (модернизации) и выводу из эксплуатации программных и аппаратно-программных средств шлюза сети Интернет.

22. Оператор ЕИТС:

1) обеспечивает функционирование и осуществляет контроль эксплуатации шлюза сети Интернет с привлечением при необходимости специалистов администратора защищенной сети ЕИТС и сторонних подрядных организаций;

2) обеспечивает блокировку доступа к опасным информационным ресурсам в сети Интернет в установленном порядке;

3) обеспечивает в рамках своих полномочий безопасный доступ пользователей ЕИТС и подключение объектов ЕИТС к сети Интернет;

4) в ходе создания (модернизации) и эксплуатации шлюза сети Интернет осуществляет определение актуальных угроз и нарушителей безопасности информации, определение и реализацию на их основе предупреждающих (корректирующих) организационных и технических мер, а также мер, указанных в главе 4 Регламента;

5) обеспечивает мониторинг и обнаружение компьютерных атак (вторжений), регистрацию, реагирование, локализацию и устранение последствий инцидентов информационной безопасности, связанные с совершением компьютерных атак и попытками внедрения в ЕИТС вредоносного программного обеспечения посредством сети Интернет;

6) в целях защиты общедоступной информации, размещаемой пользователями ЕИТС в сети Интернет, использует средства защиты информации, сертифицированные ФСБ России и (или) получившие подтверждение соответствия в ФСТЭК России;

7) вносит руководителю уполномоченного органа предложения по дополнению и изменению правил работы пользователей ЕИТС в сети Интернет в соответствии с действующим законодательством и национальными стандартами Российской Федерации;

8) определяет и представляет на утверждение в уполномоченный орган списки администраторов шлюза сети Интернет и иных лиц, имеющих доступ к оборудованию шлюза сети Интернет.

23. Администратор защищенной сети ЕИТС:

1) разрабатывает и по согласованию с уполномоченным органом утверждает правила доступа пользователей защищенных сегментов ЕИТС к сети Интернет;

2) участвует в настройке правил маршрутизации передаваемых по ЕИТС данных между защищенными сегментами ЕИТС и шлюзом сети Интернет.