



УТВЕРЖДАЮ

Директор ЛОГКУ «Леноблэкомилития»

А.В. Слюньков

«02» декабря 2024 г.

ПОЛОЖЕНИЕ
об информационной
безопасности
и регламенте использования ресурсов сети
«Интернет» сотрудниками ЛОГКУ
«Леноблэкомилития»

1. Общие положения.

1.1. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных (ИСПДн).

1.2. Положение регламентирует единые требования по обеспечению информационной безопасности ЛОГКУ «Леноблэкомилития» при использовании ресурсов и каналов передачи данных сети «Интернет» и определяет полномочия, обязанности и ответственность сотрудников Учреждения.

1.3. Настоящее Положение предназначено для сотрудников ЛОГКУ «Леноблэкомилития», выполнение должностных обязанностей которых связано с использованием персональных компьютеров.

2. Объекты, подлежащие защите

В ЛОГКУ «Леноблэкомилития» обрабатывается информация, содержащая сведения ограниченного распространения (служебная информация, персональные данные), и открытые сведения. Защите подлежат все информационные системы ЛОГКУ «Леноблэкомилития», независимо от их местонахождения.

2.1. Основные объекты, подлежащие защите:

- информационные системы персональных данных (далее ИСПДн), а также открытая (общедоступная) информация, необходимая для работы ЛОГКУ «Леноблэкомилития», независимо от формы и вида ее представления;

- процессы обработки информации в информационных системах ЛОГКУ «Леноблэкомилития», информационные технологии, регламенты и процедуры сбора, обработки,

хранения и передачи информации;

- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации.

2.2. Особенности объектов, подлежащих защите:

- объединение в единую систему большого количества разнообразных технических средств обработки и передачи информации;
- необходимость обеспечения непрерывности функционирования структуры ЛОГКУ «Леноблэкомилция»;
- высокая интенсивность информационных потоков;
- разнообразие категорий пользователей.

3. Цели и задачи обеспечения информационной безопасности

3.1. Субъекты доступа к информации.

Субъектами доступа к информации при обеспечении информационной безопасности ЛОГКУ «Леноблэкомилция» являются:

- структурные подразделения, участвующие в информационном обмене;
- сотрудники ЛОГКУ «Леноблэкомилция», в соответствии с возложенными на них должностными обязанностями;
- физические лица, сведения о которых накапливаются, хранятся и обрабатываются в ИСПДн (в соответствии со ст.14 Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных»);
- сотрудники внешних организаций, занимающихся разработкой, поставкой, ремонтом и обслуживанием оборудования или информационных систем.

Перечисленным субъектам необходимо обеспечить:

- своевременность доступа к необходимой им информации (ее доступность);
- достоверность (полноту, точность, актуальность, целостность) информации;
- конфиденциальность (сохранение в тайне) определенной части информации, защиту от навязывания ложной (недостоверной, искаженной) информации;
- возможность осуществления контроля и управления процессами обработки и передачи информации; -защиту информации от незаконного распространения.

3.2 Цели защиты информации.

Основной целью, на достижение которой направлено настоящее Положение, является защита от возможного нанесения субъектом доступа к информации материального, физического, морального или иного ущерба посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи.

3.3. Основные задачи системы обеспечения информационной безопасности ЛОГКУ «Леноблэкомилция».

Для достижения основной цели защиты и обеспечения указанных свойств информации система обеспечения информационной безопасности ЛОГКУ «Леноблэкомилция» должна обеспечивать решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба субъектам информационных отношений, нарушению нормального функционирования сети ЛОГКУ «Леноблэкомилция»;
- создание механизма оперативного реагирования на угрозы безопасности информации;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;
- защиту от вмешательства в процесс функционирования систем ЛОГКУ «Леноблэкомилция» посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);

- разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам;
- обеспечение доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей;
- обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
- защиту от несанкционированной модификации программных средств, а также защиту систем от внедрения несанкционированных программ, включая компьютерные вирусы;
- защиту информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

3.4. Основные пути решения задач системы обеспечения информационной безопасности ЛОГКУ «Леноблэкомилития» достигаются:

- полнотой, реальной выполнимостью и непротиворечивостью требований правовых актов ЛОГКУ «Леноблэкомилития» по вопросам обеспечения информационной безопасности;
- подготовкой должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению информационной безопасности;
- наделением каждого сотрудника (пользователя) ЛОГКУ «Леноблэкомилития» минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам ЛОГКУ «Леноблэкомилития»;
- четким знанием и строгим соблюдением всеми пользователями информационных систем ЛОГКУ «Леноблэкомилития», требований правовых актов по вопросам обеспечения информационной безопасности;
- персональной ответственностью за свои действия каждого сотрудника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам ЛОГКУ «Леноблэкомилития»;
- непрерывным поддержанием необходимого уровня защищенности элементов информационных систем ЛОГКУ «Леноблэкомилития»;
- применением программно-аппаратных средств защиты информации и непрерывной административной поддержкой их использования;
- эффективным контролем над соблюдением пользователями информационных ресурсов ЛОГКУ «Леноблэкомилития» требований по обеспечению информационной безопасности.

4. Основные требования.

4.1. Доступ в сеть «Интернет» предоставляется сотрудникам ЛОГКУ «Леноблэкомилития» исключительно для выполнения ими своих функциональных обязанностей. При осуществлении доступа в «Интернет», в отношении информации ограниченного использования должен соблюдаться режим конфиденциальности.

4.2. Директор Учреждения отвечает за эффективный и безопасный доступ к сети «Интернет» сотрудниками, назначает лицо, ответственное за информационную безопасность для организации и контроля работы в сети «Интернет».

4.3. Ответственный за информационную безопасность находится в прямом подчинении директора ЛОГКУ «Леноблэкомилития».

4.4. Для работы в сети «Интернет» используются автоматизированные рабочие места, удовлетворяющие техническим требованиям, необходимым для выполнения этих задач. В качестве программного обеспечения для работы в сети «Интернет», рекомендуются к использованию Яндекс Браузер. Возможно использование других браузеров либо лицензионных, либо свободно распространяемых, при согласовании с ответственным за информационную безопасность.

4.5. Используемое в Учреждении программное обеспечение, в том числе для доступа к ресурсам «Интернет», не должно предоставлять возможности создания несанкционированных, неконтролируемых подключений из сети «Интернет» к локальной сети ЛОГКУ «Леноблэкомилития».

4.6. При работе в сети Интернет сотрудникам запрещается:

- загружать, самостоятельно устанавливать прикладное, операционное, сетевое и другие виды программного обеспечения, а также осуществлять обновления, если эта работа не входит в его должностные обязанности;

- подтверждать любые запросы ресурсов в сети «Интернет» на установку любого программного обеспечения, а также переход на другие ресурсы «Интернет», если они не известны сотруднику;

- использование рабочего времени, информационных ресурсов ЛОГКУ «Леноблэкомилития» в личных целях;

- посещение ресурсов, создание, распространение информационных материалов и сообщений, содержащих оскорбительную или провокационную информацию (к примеру, материалы, касающиеся сексуальных домогательств, расовых унижений, дискриминации по половому признаку, затрагивающие в оскорбительной форме вопросы возраста или сексуальной ориентации, религиозные или политические взгляды, национальность или состояние здоровья, нарушающие законодательство РФ);

- несанкционированное распространение информации рекламного характера;

- осуществлять доступ в социальные сети в «Интернет», если это не связано с функциональными обязанностями;

- публиковать релизы, анонсы, объявления и другие материалы ЛОГКУ «Леноблэкомилития» на других ресурсах, не опубликовав на официальном сайте Учреждения в первую очередь, а также копировать информацию на официальный сайт из соцсетей;

- публиковать информацию от имени ЛОГКУ «Леноблэкомилития», либо от лица сотрудника ЛОГКУ «Леноблэкомилития», либо структурных подразделений на сторонних сайтах, чатах, форумах, страницах и группах в соцсетях, неподконтрольных ЛОГКУ «Леноблэкомилития» без согласования с ответственным за информационную безопасность;

- публиковать официальную информацию на ресурсах, тематически не связанных с направлением работы ЛОГКУ «Леноблэкомилития» без согласования с ответственным за информационную безопасность;

- подавать информацию от имени ЛОГКУ «Леноблэкомилития», либо от лица сотрудника ЛОГКУ «Леноблэкомилития», либо структурных подразделений, в СМИ, интернет-издания без согласования с ответственным за информационную безопасность;

- использовать электронную почту ЛОГКУ «Леноблэкомилития» для регистрации в публичных сервисах, если персонализированный доступ к публичному сервису (или получение информации от публичных сервисов) не требуется для выполнения функциональных обязанностей;

- использовать почтовые сервисы для служебной корреспонденции и облачные хранилища для служебных документов, сервера которых расположены за пределами Российской Федерации;

- использовать свою личную почту в деловой переписке без согласования с ответственным за информационную безопасность.

- публиковать рекламную информацию коммерческого и некоммерческого характера без согласования с ответственным за информационную безопасность;

- публиковать символику других организаций, общественных объединений, юридических и частных лиц, не имеющих отношения к деятельности ЛОГКУ «Леноблэкомилития», а также освещать их новости, анонсы и планы без согласования с ответственным за информационную безопасность или директором ЛОГКУ «Леноблэкомилития».

- подключать к автоматизированному рабочему месту любое неавторизованное телекоммуникационное оборудование, осуществлять с помощью него доступ в «Интернет» на территории ЛОГКУ «Леноблэкомилития» без согласования с ответственным за информационную безопасность;

- использовать специальные программные средства обеспечения анонимности доступа в «Интернет».

Сотрудники ЛОГКУ «Леноблэкомилития» обязаны:

- во все рабочие чаты мессенджеров, группы в соцсетях, созданные для выполнения своих служебных обязанностей включать ответственного за информационную безопасность с правами администратора;

- при создании новой группы, чата и любых других каналов коммуникации сотрудники ГАУ ДО РДОЦТ обязаны сообщать ответственному за информационную безопасность о данном факте.

4.7. Сотрудники ЛОГКУ «Леноблэкомилиция» имеют право для выполнения своих служебных обязанностей получить ведомственный почтовый ящик вида «*****@em47.ru». Использование такого почтового сервиса считается приоритетным.

4.8. Сотрудники ЛОГКУ «Леноблэкомилиция» при работе в «Интернет» должны самостоятельно обеспечивать конфиденциальность информации, доступ к которой они получили в рамках функциональной деятельности.

4.9. Сотрудники обязаны незамедлительно сообщать непосредственному руководителю и ответственному за информационную безопасность о подозрении на контакт с представителями экстремистских организаций, а также о таких случаях, ставшими им известными.

4.10. Сотрудники обязаны незамедлительно сообщать непосредственному руководителю и ответственному за информационную безопасность обо всех случаях обнаруженных фактов нарушения данного Положения.

5. Основные правила работы.

5.1. За одним рабочим местом должно находиться не более одного сотрудника. Запрещается работать под чужим регистрационным именем, сообщать кому-либо свой пароль, одновременно входить в систему более чем с одного персонального устройства, допускать к оборудованию посторонних лиц.

5.2. Сотруднику разрешается записывать полученную служебную информацию из сети «Интернет» на личные носители информации, предварительно проверенные на наличие вирусов. Запрещено копировать на личные носители информацию с персональными данными и информацию ограниченного использования.

5.3. Сотруднику запрещено вносить какие-либо изменения в программное обеспечение, установленное на персональном компьютере.

5.4. Разрешается использовать оборудование только для выполнения своих функциональных обязанностей. Любое использование оборудования в коммерческих целях запрещено.

5.5. Сотрудник обязан сохранять оборудование в целости и сохранности.

5.6. Сотрудник обязан помнить свой пароль.

5.7. Не позже, чем за две недели до увольнения сотрудник обязан передать все доступы и пароли (к сайтам, группам и страницам соцсетей, любым другим ресурсам, серверам и оборудованию), полученные либо созданные и используемые им для выполнения своих функциональных обязанностей в ЛОГКУ «Леноблэкомилиция», что должно быть завизировано ответственным за информационную безопасность.

5.8. Правообладателем всех результатов труда сотрудника в период выполнения им своих функциональных обязанностей является ЛОГКУ «Леноблэкомилиция».

5.8. При нанесении любого ущерба (порча имущества, вывод оборудования либо программного обеспечения из рабочего состояния, несанкционированное изменение, удаление информации на Интернет-ресурсах, подконтрольных ЛОГКУ «Леноблэкомилиция», информационных и методических материалов, несанкционированная смена ключей доступа, логинов и паролей, уровней доступа на Интернет-ресурсах, подконтрольных ЛОГКУ «Леноблэкомилиция», сотрудник несет ответственность в соответствии с действующим законодательством РФ.

6. Заключительные положения.

- 6.1. Положение вступает в силу с момента его утверждения.
- 6.2. Положение является локальным актом. Внесение изменений и дополнений в Положение осуществляется в порядке его принятия.
- 6.3. Настоящее Положение может быть изменено (дополнено) локальным актом.