Акционерное общество
«Ленэнергоспецремонт» (АО «ЛЭСР»)

ПРИКАЗ

15.08.2025 г. Санкт-Петербург № 1002

Об утверждении Правил информационной безопасности АО «ЛЭСР»

В соответствии с требованиями пункта 5 приказа ПАО «Россети» от 31.01.2025 № 52 «Об утверждении Правил информационной безопасности ПАО «Россети»

ПРИКАЗЫВАЮ:

1. Утвердить Правила информационной безопасности АО «ЛЭСР» (далее – Правила) согласно приложению 1 к настоящему приказу.
2. Первому заместителю генерального директора, заместителям генерального директора, руководителям прямого подчинения, начальникам структурных подразделений АО «ЛЭСР»:
2.1. Организовать ознакомление подчиненных им работников с Правилами.
Срок: в течение 3 (трех) недель с даты выхода настоящего приказа.
2.2. Обеспечить включение условий согласно приложению 1 к настоящему Приказу в гражданско-правовые договоры, заключаемые АО «ЛЭСР» с физическими и юридическими лицами.
Срок: постоянно.
3. Начальнику отдела управления персоналом Румянцевой Е.Р включить Правила в перечень документов, обязательных для ознакомления при приеме на работу в АО «ЛЭСР».
4. Исполняющему обязанности начальника информационно-программного обеспечения Мурадяну А.Г. организовать размещение Правил на официальном сайте АО «ЛЭСР» в разделе «Устав и внутренние документы»
Срок: Начиная с даты выхода настоящего Приказа.
5. Признать утратившим силу приказ АО «ЛЭСР» от 14.03.2023 № 268 «Об утверждении Правил информационной безопасности АО «ЛЭСР».
6. Контроль за исполнением настоящего Приказа возложить на заместителя генерального директора по безопасности Емешева А.С.

Первый заместитель
генерального директора В.В. Перевалов

Рассылка: заместители генерального директора, руководители прямого подчинения генеральному директору, руководители структурных подразделений
Мурадян А.Г. 460-68

Приложение 1
к приказу АО «ЛЭСР»
от 15.08.2025 № 1002

АКЦИОНЕРНОЕ ОБЩЕСТВО «ЛЕНЭНЕРГОСПЕЦРЕМОНТ»

ПРАВИЛА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АКЦИОНЕРНОГО ОБЩЕСТВА «ЛЕНЭНЕРГОСПЕЦРЕМОНТ»

АО «ЛЭСР»

Редакция 2

Санкт-Петербург
2025

Содержание

Термины и определения

Термин	Определение
Автоматизированная система	Система, состоящая из комплекса средств автоматизации, реализующего информационную технологию выполнения установленных функций, и персонала, обеспечивающего его функционирование «ГОСТ Р 59853-2021. Национальный стандарт Российской Федерации. Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения».
Автоматизированная система управления	Комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами (в соответствии с Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»).
Информационные технологии	Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).
Корпоративный центр кибербезопасности	Специализированное подразделение, созданное для мониторинга и управления информационной безопасностью корпоративной информационной системы и технологических информационных систем, а также обеспечения защиты информационных ресурсов ПАО «Россети» от киберугроз, включая несанкционированный доступ, вредоносное ПО, утечки данных и другие виды атак.
Корпоративный сегмент	Сегмент сети связи электросетевого комплекса, предназначенный для обеспечения телекоммуникационными услугами систем

	административно-хозяйственной деятельности АО «ЛЭСР».
Критическая информационная инфраструктура (КИИ)	Совокупность имеющихся сервисов и систем, сетей, технических и программных средств, данных, автоматизированных процессов, обеспечивающих информационное обеспечение деятельности АО «ЛЭСР».
Информационные ресурсы	Отдельные документы или отдельные массивы документов, документы или массивы документов в информационных системах.
Информационная система	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств (в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).
Многофункциональное устройство (МФУ)	Устройство, сочетающее в себе функции принтера, сканера, факсимильного устройства, копировального модуля.
Общество	АО «ЛЭСР».
Работник	Лицо, с которым у АО «ЛЭСР» заключен трудовой договор.
Пользователь	Лицо, участвующее в функционировании информационной системы или использующее результаты ее функционирования.
Средства вычислительной техники	Совокупность программных технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.
Технологический сегмент	Сегмент сети связи электросетевого комплекса, предназначенный для обеспечения телекоммуникационными услугами с заданными показателями качества обслуживания, включая уровень надежности, необходимый и достаточный для нормального функционирования систем управления технологическими процессами электросетевого комплекса.
BIOS, UEFI	Набор микропрограмм, реализующих интерфейс для работы с аппаратурой компьютера и подключенными к нему устройствами.

Сетевая папка	каталог, размещённый на сервере Общества, с централизованным управлением доступом, логированием и регулярным резервным копированием. Используется как основное и единственно допустимое место для хранения рабочих файлов.
Локальный диск (ПК)	внутренний жёсткий диск или твердотельный накопитель рабочего компьютера. Не предназначен для хранения рабочих документов. Используется исключительно для временных файлов или кэшированных данных.
Резервное копирование	процесс создания копий данных для их восстановления в случае утери, повреждения или несанкционированного доступа. Выполняется централизованно в соответствии с регламентами отдела ИПО.
Инцидент	любое событие, повлёкшее нарушение целостности, конфиденциальности или доступности данных. К инцидентам относятся утеря файлов, их случайное удаление, заражение вирусами, сбой оборудования и др.
ОИПО (Отдел информационно-программного обеспечения)	подразделение, обеспечивающее техническую поддержку пользователей, управление ИТ-инфраструктурой, безопасность информационных систем и контроль соблюдения цифровых регламентов.
Service Desk	Служба технической поддержки пользователей
Недоверенные устройства	Устройства, которые не прошли установленные в Обществе процедуры регистрации, проверки и/или сертификации, не имеют актуальных средств защиты, не управляются централизованными средствами администрирования организации или не соответствуют установленным требованиям безопасности, вследствие чего их использование для обработки, хранения или передачи информации считается небезопасным

Обозначения и сокращения

Сокращение	Полная форма
АВПО	Антивирусное программное обеспечение
АРМ	Автоматизированное рабочее место
АСУ	Автоматизированная система управления
ГИС	Государственная информационная система
ИБ	Информационная безопасность
ИС	Информационная система
ИТ	Информационные технологии
ИТС	Информационно-телекоммуникационная сеть
ЛВС	Локальная вычислительная сеть
ОРД	Организационно-распорядительный документ
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
ДБО	Дистанционное банковское обслуживание
VPN	Виртуальная частная сеть (Virtual Private Network)
СВТ	Средство вычислительной техники

1. Общие сведения

1.1. Цель разработки документа

Настоящие Правила определяют порядок работы с информацией конфиденциального характера, правила безопасной работы на объектах КИИ, действия при возникновении компьютерных инцидентов и иных нештатных ситуаций Работников Общества, а также третьих лиц, получивших доступ к информации конфиденциального характера, объектам КИИ Общества на основании заключенных соглашений и договоров.

1.2. Корпоративный центр кибербезопасности

В ГК Россети действует Корпоративный центр кибербезопасности при организации процессов обнаружения, предотвращения, а также реагирования на компьютерные атаки в отношении объектов критической информационной инфраструктуры.

2. Общие положения

2.1. Субъектами, на которых распространяется действие настоящих Правил, являются (далее – Пользователи):

- работники Общества;
- работники юридических лиц, выполняющих работы на объектах информационной инфраструктуры или в отношении объектов информационной инфраструктуры Общества в соответствии с условиями заключенных договоров, иных законных основаниях;

– физические лица (в том числе осуществляющие предпринимательскую деятельность в порядке индивидуального предпринимателя или самозанятого), с которыми заключены договоры гражданско-правового характера;

– иные физические лица, выполняющие действия в отношении информационной инфраструктуры, зданий и (или) сооружений Общества с размещенными объектами информационной инфраструктуры, включая проведение аудита, стажировок, уборки помещений.

2.2. Объектами защиты в контексте обеспечения безопасности информационной инфраструктуры Общества и информации конфиденциального характера являются:

– корпоративные ИС (в том числе машинные носители информации, АРМ, серверы, средства обработки буквенно-цифровой, графической, видео- и речевой информации, микропрограммное, общесистемное, прикладное программное обеспечение), обеспечивающие устойчивость финансово-хозяйственной деятельности;

– АСУ (в том числе АРМ, промышленные серверы, программируемые логические контроллеры, производственное, технологическое оборудование (исполнительные устройства), имеющее функции как локального, так и дистанционного управления, либо имеющее функционирующие интерфейсы сетевого взаимодействия, микропрограммное, общесистемное, прикладное ПО), обеспечивающие надежное снабжение потребителей электроэнергией;

– корпоративные и технологические ИТС (в том числе телекоммуникационное оборудование, ПО, система управления, линии связи), формирующие единое информационное пространство и цифровую среду взаимодействия;

– цифровые устройства и периферийное оборудование (в том числе принтеры, сканеры, ip-телефоны, цифровые камеры, смартфоны);

– сети электросвязи, используемые для организации взаимодействия объектов и передачи информации, места выхода в сеть Интернет;

– архитектура и конфигурация ИС, ИТС, АСУ, информация (данные) о параметрах (состоянии) управляемого (контролируемого) объекта или процесса (в том числе входная (выходная) информация), управляющая (командная) информация, контрольно-измерительная информация, персональные данные, иная информация конфиденциального характера, в том числе представляющая коммерческую ценность в силу неизвестности третьим лицам.

2.3. Пользователи обязаны неукоснительно соблюдать настоящие Правила при работе с ИС, АСУ, ИТС, включая их элементы (АРМ, серверы, коммутационное, сетевое и иное оборудование), а также при работе с информацией конфиденциального характера.

2.4. Общество предпринимает разумно достаточные средства и методы технической защиты объектов КИИ и обрабатываемой информации конфиденциального характера, а также другие, не противоречащие законодательству Российской Федерации меры.

2.5. С целью повышения уровня внимания Пользователей к вопросам обеспечения безопасности информации, в местах для информирования (информационных стендах, досках) на территории Общества (включая электросетевые объекты) должна быть размещена памятка Работнику субъекта КИИ (приложение 1 к настоящим Правилам).

2.6. В случае организации посещения электросетевых объектов, административных и иных объектов Общества физическими лицами в ходе экскурсий, проверок, иных случаях, не предусматривающих заключение договоров или соглашений, должностные лица Общества, ответственные за организацию (сопровождение) такого рода посещений, должны информировать посетителей о действии Правил на территории Общества.

3. Правила работы с информацией конфиденциального характера

3.1. Информация, обрабатываемая в Обществе, делится на:

– конфиденциальную информацию;

– информацию, содержащую сведения, составляющие государственную тайну;

– иную (в том числе общедоступную) информацию.

3.2. Перечень информации конфиденциального характера определяется в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера» и утверждается соответствующими ОРД Общества или определяется руководством Общества.

3.3. Информация, обрабатываемая на объектах КИИ Общества, относится к охраняемой компьютерной информации конфиденциального характера.

3.4. Информация в Обществе обрабатывается в электронном виде и на бумажных носителях.

3.5. Порядок обработки информации конфиденциального характера определяется локальными нормативными актами и ОРД.

4. Правила безопасной работы на объектах КИИ

4.1. Пользователям запрещено:

1) Разглашать конфиденциальную информацию, включая обрабатываемую на объектах КИИ, в том числе:

– осуществлять фото- и видеосъемку экранов АРМ, офисных помещений, мест расположения средств вычислительной техники в случае, если данные действия не являются необходимыми для выполнения трудовых функций, закрепленных в должностной инструкции Работника, или не предусмотрены договором между Обществом и Пользователем, ОРД Общества;

– осуществлять скрытую аудио- и видеозапись совещаний и переговоров;

– выполнять печать и сканирование документов с конфиденциальной информацией на общедоступных МФУ (расположенных в коридорах, залах, рекреациях, иных местах и помещениях, в которые возможен неконтролируемый доступ посторонних лиц);

– обсуждать сведения, относящиеся к конфиденциальной информации, в присутствии третьих лиц или в местах, где такая информация может быть услышана третьими лицами;

– оставлять бумажные или электронные носители с конфиденциальной информацией в переговорных комнатах и других общедоступных местах, включая общедоступные МФУ;

2) использовать недоверенные устройства и ПО на АРМ, в том числе:

– осуществлять попытки самостоятельного внесения изменений в настройки операционных систем и параметров безопасности средств защиты информации, установленных на АРМ;

– использовать незарегистрированные (в том числе личные) USB накопители на значимых объектах КИИ;

– устанавливать непредусмотренное для выполнения рабочих обязанностей ПО (игры, медиаплееры и т.п.);

– использовать сторонние Wi-Fi сети для подключения корпоративных устройств (в том числе создавать собственные Wi-Fi и иные беспроводные сети);

– использовать некорпоративные почтовые сервисы;

– использовать личную периферийную технику (клавиатуры, мыши, принтеры, сканеры, МФУ);

3) получать несанкционированный доступ к ИС и ресурсам Общества, в том числе:

– использовать чужие данные для доступа к ИС Общества;

– использовать уязвимости и незадокументированные возможности ПО;

– отправлять электронные письма в личных (не связанных с производственной деятельностью) целях.

4.2.Работник обязан незамедлительно сообщать в ОИПО по электронной почте lesrdesk@lenenergo.ru или телефону +7(812)4939545 вн.460-68 информацию о следующих фактах:

– выявлении подозрительной активности на АРМ;

– выявлении вирусной активности;

– утрате носителей служебной информации и мобильных АРМ (ноутбук, планшет, смартфон);

– раскрытии парольной информации;

– утрате или компрометации носителей сертификатов ключа проверки электронной подписи (ключевых носителей);

– обнаружении неопознанных ключевых носителей, носителей информации;

– обнаружении неопределенных технических средств (устройств) несанкционированное подключенных к АРМ, ЛВС;

– обнаружении уязвимостей в любых элементах АРМ, серверов, ЛВС, ИС и АСУ;

– обнаружении ошибок в настройке и работе ИС и АСУ, сетей связи, приводящих к доступу в области, не предусмотренной изначальной заявкой на доступ;

– обнаружении в открытом доступе в любом виде учетных данных (паролей и имен пользователей);

– обнаружении несанкционированного доступа других лиц к информации или СВТ;

– попытках получения парольной информации третьими лицами;

– прекращении работоспособности средств защиты информации.

4.3. Все оборудование, имеющее интерфейсы сетевого взаимодействия, должно быть закреплено за Работниками Общества.

5. Правила работы с учетными записями

5.1. В Обществе используются 3 типа учетных записей:

– пользователь «Непривилегированные учетные записи»;

– администратор «Привилегированные учетные записи»;

– сервисная «Привилегированные учетные записи».

5.2. По умолчанию всем Пользователям предоставляется корпоративная учетная запись типа «Пользователь», позволяющая получить доступ только к АРМ.

5.3. Доступ к ИС, включая системы электронного документооборота, системы планирования и ведения финансово-хозяйственной деятельности, иным ресурсам, необходимым для выполнения производственных задач, предоставляется в соответствии с ОРД Общества по заявке руководителя

структурного подразделения в Service Desk посредством создания отдельной учетной записи (логина) и одноразового пароля.

5.4. Доступ к АСУ, иным технологическим системам осуществляется в соответствии с порядком, предусмотренным эксплуатационной, проектной документацией на данные системы.

5.5. Доступ к информационным ресурсам Общества для лиц, не являющихся Работниками Общества, предоставляется в соответствии с ОРД Общества по заявке руководителя структурного подразделения Общества (куратора соглашения, договора) в ServiceDesk с заполненным обязательством (приложение 2 к настоящим Правилам) на каждого Пользователя после согласования заявки с ОИПО.

5.6. Создание учетной записи типа «Администратор» и «Сервисная», повышение уровня доступа существующей учетной записи осуществляется по согласованию с ОИПО.

5.7. Все учетные записи должны быть персонифицированы, за исключением случаев, когда необходимость работы под обезличенной учетной записью обусловлена техническими требованиями ИС, АСУ или оборудования ИТС.

5.8. В случае необходимости использования одного общего ресурса (почта, лок.УЗ, сетевой каталог, КИДО) одной учетной записи несколькими Пользователями, подразделением – владельцем ИС должен быть разработан и утвержден ОРД с перечнем лиц, допущенных к работе в ИС (АСУ, оборудования ИТС) под указанной учетной записью, и назначен ответственный за периодическую смену пароля. В случае заведения неперсонифицированной учетной записи ответственным назначается владелец той информационной системы, в которой учетная запись заводится.

5.9. Учетные записи, не использовавшиеся более 45 дней, должны быть автоматически заблокированы.

5.10. В случае прекращения трудовых отношений с Работником, прекращения действия договора между Обществом и Пользователем, прекращения договора гражданско-правового характера, окончания практики, ухода Работника в декретный отпуск учетные записи, принадлежащие Пользователю, должны быть заблокированы.

5.11. Сброс пароля и разблокирование учетных записей производятся на основании письменного запроса в ОИПО. Запрещен сброс пароля по обращениям, поданным в устной форме или по телефону.

5.12. В письменном запросе на сброс пароля указывается:

– мобильный телефон для учетной записи работника Общества;

– мобильный телефон или электронная почта для учетной записи специалиста или эксперта организации, с которой непосредственно заключен действующий контракт или договор.

5.13. Сброс пароля по запросу от руководителя Подразделения, обслуживающего корпоративные и технологические системы или владельца

учетной записи осуществляется без согласования с ОИПО. В остальных случаях согласование с ОИПО обязательно.

5.14. Сброс пароля учетной записи работника подразделения, работающего посменно, при формировании запроса иным работником этого подразделения возможен без согласования с ОИПО при наличии служебной записки, направленной в адрес заместителя генерального директора по цифровой трансформации и дополнительным услугам, содержащей перечень лиц с полномочиями по сбросу паролей работников подразделения.

5.15. Запрещен сброс пароля персональной учетной записи в целях использования данной учетной записи другим работником.

5.16. Разблокирование учетной записи осуществляется по согласованию с ОИПО.

5.17. Установленный после сброса новый временный пароль передается владельцу учетной записи по реквизитам в запросе, указанном в соответствии с пунктом 5.12 настоящих Правил.

5.18. В случае применения механизмов двухфакторной аутентификации с использованием связанного с учетной записью телефонного номера номер, используемый для получения второго фактора, должен принадлежать Пользователю или быть закрепленным за ним (в случае использования корпоративных телефонных номеров Общества).

5.19. Требования к имени учетной записи:

– имя учетной записи должно быть уникальным в пределах используемой ИС или ПАК;

– следует избегать применения специальных символов и цифр в учетной записи, за исключением «.»;

– все учетные записи типа «администратор» должны содержать приставку «LRD.» и иметь формат «LRD.Фамилия администратора»;

– имя учетной записи должно соответствовать стандартам и рекомендациям, установленным для ИС или ПАК, в которых она используется;

– имя учетной записи должно применяться для быстрой идентификации учетной записи и ее владельца;

– имя учетной записи не должно содержать конфиденциальную информацию.

6. Правила работы с паролями

6.1. Требования к содержанию, длине, периодичности и порядку смены паролей устанавливаются в соответствии с Политикой управления доступом АО «ЛЭСР».

6.2. Пароли не должны храниться и передаваться в незашифрованном виде по публичным сетям (локальная вычислительная сеть, интернет, электронная почта).

6.3. В ходе работы не должны использоваться пароли по умолчанию. Должны быть назначены пароли, отличные от установленных производителем.

6.4. При компрометации пароля владелец учетной записи должен незамедлительно сменить все пароли.

6.5. При использовании паролей запрещено:

– хранить и записывать пароли на бумаге, в том числе на предметах, а также в местах, доступных третьим лицам;

– хранить и записывать пароли в электронном виде без использования криптографической защиты;

– передавать и сообщать третьим лицам личный пароль (за исключением случаев хранения руководителями или ответственными Работниками подразделений паролей в соответствии с обязанностями, указанными в положении о подразделении и (или) должностных инструкциях);

– регистрировать третьих лиц под своим паролем;

– передавать парольные фразы пользователям при помощи почтовых сообщений либо иным открытым способом через Интернет без использования парольной или криптографической защиты;

– вводить свой пароль в случае, если он может быть подсмотрен случайно или намеренно третьим лицами;

– использовать одни и те же пароли для разных ИС (АСУ, оборудования ИТС);

– создавать учетные записи, профили на сторонних интернет-сервисах и ИС (включая общедоступные сервисы электронной почты) с использованием пароля от корпоративного АРМ;

– использовать функцию «Запомнить пароль» в программном обеспечении.

6.6. В случае отсутствия технической возможности использования паролей, соответствующих требованиям настоящего раздела, требования к паролям устанавливаются на этапе проектирования или разработке эксплуатационной документации на ИС, АСУ, ИТС.

7. Правила работы на АРМ

7.1. Пользователи должны обладать необходимыми навыками работы с используемым аппаратным и программным обеспечением.

7.2. Для выполнения производственных задач Работнику предоставляется корпоративное АРМ, включающее в себя средства вычислительной техники (персональный компьютер), виртуальные ресурсы вычислительной сети, периферийное, мобильное и иное оборудование, предусмотренное должностными обязанностями Работника и соответствующими ОРД Общества.

7.3. В случае необходимости организации АРМ для лиц, не являющихся Работниками Общества, АРМ создается по обращению в Service Desk руководителя структурного подразделения Общества, куратора соглашения, договора после согласования с Подразделением ИБ.

7.4. К ИТС Общества запрещено подключать личные средства вычислительной техники (персональный компьютер, ноутбук, смартфон, планшет, модем, роутер, точку доступа, ip видеокамеру, цифровую приставку для ТВ и т.д.).

7.5. Доступ Пользователя к АРМ осуществляется:

– с применением персональной доменной учетной записи;

– с применением локальной персонифицированной или общей учетной записи;

– с применением средств защищенного удаленного доступа.

7.6. Использование локальных учетных записей допускается:

– в случаях, предусмотренных эксплуатационной или проектной документацией на эксплуатируемую систему;

– в случаях проведения работ по техническому обслуживанию АРМ (для Работников технической поддержки);

– в отдельных случаях, после получения согласования со стороны Подразделения ИБ.

7.7. Удаленное подключение к АРМ допускается:

– в случаях, предусмотренных эксплуатационной или проектной документацией на эксплуатируемую систему;

– в случаях введения приказом по Обществу удаленного режима работы, за исключением подключения к АРМ, входящим в состав АСУ, иных технологических систем;

– в отдельных случаях, после получения согласования со стороны Подразделения ИБ.

7.8. Все АРМ (включая виртуальные) должны быть оснащены средствами антивирусной защиты.

7.9. Доступ к настройкам BIOS АРМ, настройкам МФУ, сетевого и коммутационного оборудования должен быть заблокирован паролем.

7.10. При организации защищенного удаленного доступа к АРМ или ИС с использованием механизмов двухфакторной аутентификации посредством отправки SMS-кодов, носителя и сертификата не допускается использование телефонных номеров третьих лиц, передача носителя и сертификата третьим лицам, в том числе родственникам или знакомым Пользователя, коллегам.

7.11. Организация удаленного подключения подрядных организаций к корпоративным АРМ осуществляется по согласованию с Подразделением ИБ.

7.12. По окончании сеанса работы на АРМ или при необходимости оставления рабочего места Пользователь должен заблокировать экран средств вычислительной техники (блокирование экрана на АРМ осуществляется нажатием сочетания клавиш Win + L или нажатием сочетания клавиш Ctrl + Alt + Del и выбором опции «Блокировать компьютер»).

7.13. При работе на АРМ запрещено:

– эксплуатировать средства вычислительной техники при отключенных или неустановленных средствах антивирусной защиты и встроенных в операционную систему средствах обеспечения безопасности;

– оставлять рабочее место без блокирования экрана АРМ;

– использовать АРМ в нерабочее время не по прямому назначению;

– осуществлять работу на АРМ, не удовлетворяющих требованиям ИБ;

– допускать к работе на своем АРМ третьих лиц, за исключением Работников службы технической поддержки и Работников Подразделения ИБ;

– срывать пломбы или печати, вскрывать корпус АРМ, осуществлять самостоятельную сборку и разборку средств вычислительной техники;

– использовать уязвимости и недокументированные возможности установленного ПО;

– вносить изменения в аппаратную и программную конфигурацию АРМ;

– хранить личную, не имеющую отношения к выполнению должностных обязанностей, информацию на АРМ и сетевых ресурсах;

– производить загрузку АРМ с внешних и сетевых носителей;

– получать доступ к BIOS или UEFI АРМ;

– использовать АРМ с локальными учетными записями;

– препятствовать работе средств защиты информации или обходить их;

– самостоятельно подключать к АРМ периферийные и внешние устройства, в том числе:

– принтеры, сканеры и МФУ,

– модемы и адаптеры связи,

– мобильные телефоны, планшеты и другие подобные устройства,

– личные носители информации,

– устройства двойного назначения – скрывающие встроенный функционал;

– использовать АРМ с одновременным подключением к ЛВС и другим сетям;

– оставлять средства вычислительной техники (ноутбук, смартфон, планшет) в общедоступных местах без присмотра;

– осуществлять подключение (проводное или беспроводное) к АРМ личных мобильных устройств (смартфон, планшет, модем или другие внешние устройства), в том числе с целью зарядки;

– производить самостоятельное удаление/установку программного обеспечения на АРМ.

7.14. При увольнении Работника информация на жестком диске АРМ Работника и сетевых ресурсах подлежит передаче непосредственному руководителю Работника, после чего АРМ и другие средства вычислительной техники, полученные Работником, должны быть сданы в структурное подразделение, осуществляющее выдачу средств вычислительной техники, до момента его увольнения.

7.15. При приемке АРМ уволенного Работника должна быть выполнена процедура удаления информации и установлена новая копия операционной системы и прикладного ПО.

7.16. При передаче средств вычислительной техники в ремонт, в иных случаях передачи средств вычислительной техники третьим лицам (включая списание и утилизацию) жесткие диски должны быть демонтированы.

7.17. Передача средств вычислительной техники с жесткими дисками, передача жестких дисков в ремонт осуществляется после согласования с Подразделением ИБ.

7.18. При списании, утилизации жестких дисков, иных носителей информации должна быть выполнена процедура удаления информации без возможности ее восстановления.

7.19. Физический доступ в помещения с АРМ должен обеспечиваться с использованием средств контроля и управления доступом или иными способами контроля, позволяющими исключить несанкционированным доступ в помещение посторонних лиц.

7.20. Доступ в помещения с АРМ, серверные и кроссовые помещения, иные помещения с размещенными элементами информационной инфраструктуры представителям подрядных организаций, контрагентов и иным лицам, не являющимся Работниками Общества (в том числе с целью уборки помещений, выполнения работ по техническому обслуживанию, проведения аудита, прохождения стажировки и т.д.), предоставляется по согласованию с департаментом безопасности Общества.

7.21. Доступ в помещения с АРМ, серверами, коммутационным оборудованием, осуществляющими обработку информации технологического характера (в том числе информации о значимых объектах КИИ), третьим лицам предоставляется только при непосредственном сопровождении Работника Подразделения ИБ Общества.

7.22. Настройка нового АРМ, замена или передача другому Работнику, а также перенос АРМ из одного подразделения или сетевого сегмента в другой должны выполняться с удалением имеющейся информации на жестких дисках и установкой новой копии операционной системы и прикладного ПО.

8. Правила работы с ИС

8.1. При работе с ИС (АСУ, оборудовании ИТС) запрещено:

– использовать уязвимости и недокументированные возможности программного и аппаратного обеспечения;

– использовать (в любых целях) ошибки системы;

– осуществлять деструктивные воздействия на ПО и данные в ИС (АСУ);

– несанкционированно изменять или уничтожать данные в ИС или на внешних (отчуждаемых) носителях;

– несанкционированно устанавливать на АРМ любые дополнительные программные и аппаратные компоненты и устройства;

– осуществлять доступ под чужими учетными данными;

– выполнять резервное копирование информации на личные носители, облачные сервисы, внешние сервисы электронной почты;

– публиковать в открытом доступе информацию об архитектуре и конфигурации корпоративных и технологических ИТС, сетей электросвязи, используемых для организации взаимодействия объектов и передачи информации, в том числе для выхода в сеть Интернет.

8.2. При работе с технологическими системами (в том числе АСУ) Пользователь должен уделять особое внимание безопасности информации.

8.3. Порядок работы с технологическими системами указывается в эксплуатационной или проектной документации на данные системы.

9. Правила работы в ЛВС

9.1. Работнику для выполнения служебных обязанностей предоставляется доступ в ЛВС со стационарного АРМ.

9.2. Удаленный доступ к внутрикорпоративным web-сервисам и ИС, в том числе с использованием сторонних средств вычислительной техники, должен осуществляться через «единое окно» по защищенному каналу связи с применением средств терминального доступа или VPN шлюза по протоколу

HTTPS с применением двухфакторной аутентификации, в том числе с применением персональных сертификатов, выдаваемых подразделением Общества, обеспечивающим создание, выдачу и обслуживание сертификатов электронной подписи.

9.3. К средствам вычислительной техники (персональный компьютер, ноутбук, планшет), с которых осуществляется удаленный доступ к ИС, в том числе к корпоративным АРМ, применяются все требования настоящих Правил.

9.4. В случае осуществления удаленного или локального доступа к ЛВС Общества с АРМ организаций, выполняющих работы/оказывающих услуги в интересах Общества, доступ предоставляется только при условии наличия с указанной организацией соглашения об охране и передаче информации и соглашения/условий договора о соблюдении требований настоящих Правил работниками указанной организации, а также при наличии в указанном соглашении/договоре ответственности за нарушение требований настоящих Правил. При этом АРМ указанной организации должны удовлетворять требованиям и мерам защиты информации, принятым в Обществе.

9.5. При работе в ЛВС без предварительного согласования с Подразделением ИБ не допускается:

– устанавливать удаленный доступ к АРМ и ЛВС, подключать любые устройства к ЛВС;

– осуществлять доступ к ЛВС с личных устройств;

– осуществлять сетевой доступ к другим АРМ;

– подключать средства вычислительной техники, имеющие встроенные и внешние устройства беспроводной связи к ЛВС;

– подключать АРМ к беспроводным сетям.

9.6. При работе в ЛВС запрещено:

– подключать к ЛВС средства вычислительной техники с отключенными или неустановленными средствами зашиты, а также с настройками, неудовлетворяющими требованиям ИБ;

– проводить сканирование и анализ ЛВС и сетевых узлов;

– осуществлять перехват трафика в ЛВС;

– осуществлять атаки на АРМ, ЛВС, серверы, коммутационное и иное оборудование, включая информационные системы и АСУ;

– использовать уязвимости протоколов и конфигураций сетевого оборудования в ЛВС;

– организовывать точки входа и шлюзы для внешних сетей;

– создавать точки беспроводного доступа на территории Общества.

10. Правила работы в сети Интернет

10.1. Доступ с АРМ к ресурсам сети Интернет предоставляется через защищенную схему в соответствии с ОРД Общества.

10.2. Доступ к ресурсам сети Интернет предоставляется:

– работникам для выполнения ими трудовых функций;

– работникам организаций, в рамках заключенного договора между Обществом и организацией, условиями которого является выполнение действий в информационной инфраструктуре на территории Общества (по согласованию с руководителем структурного подразделения – куратором договора);

– физическим лицам, в рамках заключенного договора гражданско-правового характера, условиями которого является выполнение действий в информационной инфраструктуре на территории Общества (по согласованию с руководителем структурного подразделения – куратором договора);

– физическим лицам, проходящим практику или стажировку (по согласованию с руководителем практики или стажировки);

– иным физическим лицам, выполняющим действия в информационной инфраструктуре на территории Общества в соответствии с ОРД Общества

10.3. При работе в сети Интернет запрещено:

– обходить механизмы фильтрации запрещенных Интернет-ресурсов с помощью специализированных интернет-сервисов (анонимайзеры, прокси-серверы, VPN-серверы);

– организовывать туннелирование внешних сетей;

– переходить по баннерам и рекламным объявлениям;

– переходить по подозрительным ссылкам;

– распространять информацию, запрещенную законодательством Российской Федерации, включая материалы террористического, национального, расистского, сексуального, религиозного, развлекательного и другого характера, а также информацию, оскорбляющую честь, достоинство и деловую репутацию юридических и физических лиц;

– игнорировать системные сообщения АРМ и предупреждения об ошибках;

– несанкционированно размещать от имени Общества любую информацию, в том числе публиковать информацию в социальных сетях, Интернет-мессенджерах, форумах;

– использовать внешние адреса электронной почты для ведения служебной переписки;

– публиковать в сети Интернет корпоративные адреса электронной почты и телефонов Работников Общества;

– приобретать, хранить и распространять информацию, запрещенную законодательством либо способную причинить вред имиджу Общества или нанести материальный ущерб Обществу;

– предпринимать самостоятельные действия по устранению неполадок при подключении к сети Интернет при их возникновении;

– осуществлять работу в сети Интернет с использованием учетных записей с административными правами доступа;

– использовать ресурсы:

– непристойного содержания,

– не связанные с исполнением трудовых функций Работников,

– нарушающие требования действующего законодательства,

– игрового и развлекательного характера,

– социальных сетей,

– пиринговых сетей,

– почтовых сервисов,

– файлообменных сервисов и облачных хранилищ, за исключением файлообменных сервисов Общества,

– форумов и конференций (в части публикации сообщений),

– сервисов коммуникаций (Telegram, WhatsApp, Instagram, Skype (за исключением корпоративной версии) и иных сервисов), за исключением случаев, когда использование такого сервиса необходимо в рамках исполнения должностных обязанностей в соответствии с положением о структурном подразделении, должностной инструкцией или другими нормативными документами общества,

– сервисов видеотелефонной связи (Zoom, Google Meet, TrueConf и др.), за исключением использования корпоративных версий указанного программного обеспечения в рамках исполнения должностных обязанностей,

– удаленных АРМ, находящихся за пределами ЛВС, способами, выходящими за рамки утвержденных проектных решений, в том числе с использованием программ удаленного доступа (rAdmin, TeamViewer, AnyDesk, RemotePC, Chrome Remote Desktop, Ammyy Admin и др.);

– снижать установленный уровень защиты информации;

– сохранять и запускать файлы, полученные из сети Интернет, за исключением случаев, когда использование таких файлов необходимо в рамках исполнения должностных обязанностей в соответствии с положением о структурном подразделении и (или) должностной инструкцией.

10.4. Не допускается организация подключения к сети Интернет на АРМ и серверах технологического сегмента.

11. Правила работы с электронной почтой

11.1. Доступ к корпоративной электронной почте предоставляется Работникам только в целях исполнения трудовых функций.

11.2. Вся служебная переписка должна осуществляться только с использованием персонального адреса корпоративной электронной почты.

11.3. Допускаются к передаче по электронной почте только сообщения, которые могут быть успешно проверены средствами антивирусной защиты.

11.4. Не допускаются к передаче сообщения электронной почты с исполняемыми файлами (exe, bat, cmd, msi и т.п.) и архивами, защищенными паролем. Для передачи подобных файлов применяется корпоративная Система обмена данными ПАО «Россети Леэнерго».

11.5. При работе с электронной почтой запрещено:

– осуществлять массовую и адресную рассылку информации, не связанной со служебной необходимостью и с выполнением должностных обязанностей (спам-рассылка);

– направлять конфиденциальную информацию без применения средств криптографической защиты информации по открытым (незащищенным) каналам передачи данных, в том числе через сети общего пользования и сеть Интернет;

– использовать любые другие сервисы электронной почты, кроме корпоративных, если иное не предусмотрено исполнением должностных обязанностей;

– снижать установленный уровень защиты информации сообщений;

– открывать письма, поступившие от неизвестных адресатов с неизвестными вложениями;

– переходить по внешним ссылкам, указанным в электронных письмах, в случае если получение такого письма не связано с выполнением должностных обязанностей;

– регистрировать учетные записи, профили на сторонних Интернет-ресурсах (включая социальные сети) с указанием корпоративного адреса электронной почты, за исключением случаев, связанных с выполнением должностных обязанностей.

11.6. При получении массовой рассылки от ОИПО Работники обязаны усилить бдительность к получаемой электронной почте.

11.7. При получении подозрительного письма Работник должен:

– при получении письма сомнительного содержания и/или от неизвестного пользователя с вложением не открывать его, в случае открытия – не открывать вложения, не переходить по указанным в письме ссылкам;

– при случайном открытии письма и подозрительном поведении АРМ запрещается отключать АРМ от питания;

– сообщить в ОИПО о факте получения и открытия вложения подозрительного письма;

– выполнить следующие действия при подтверждении, что данное письмо является нежелательной почтой (спам-рассылкой):

- для Microsoft Office:
  - нажать на данное письмо правой кнопкой мыши;
  - выбрать пункт «Нежелательная почта»;
  - выбрать пункт «Заблокировать отправителя»;
- для Evolution:
  - нажать на данное письмо правой кнопкой мыши;
  - выбрать пункт «Пометить как спам»;
- для Р7 органайзер:
  - нажать на данное письмо правой кнопкой мыши;
  - выбрать раздел «Отметить»;
  - выбрать пункт «Как спам».

12. Правила работы с носителями информации

12.1. Использование внешних носителей информации, включая носители USB, съемные диски, карты памяти и оптические диски CD/DVD, запрещено без согласования с ОИПО.

12.2. При необходимости использования внешнего носителя для записи (копирования) информации на АРМ руководитель подразделения или Подразделения, обслуживающего корпоративные и технологические системы филиала, должен направить консолидированный запрос в службу поддержки Service Desk с обоснованием производственной необходимости, Ф.И.О., сетевыми именами АРМ и контактными телефонами Работников, которым необходимо предоставить доступ.

12.3. Работники Подразделения ИБ могут блокировать порты подключения внешних носителей информации в случаях нарушения Пользователем требований при работе с носителями информации, при угрозе распространения вредоносного ПО, иных случаях, связанных с рисками нарушения конфиденциальности, целостности и доступности информации.

12.4. В случае использования внешнего носителя для передачи конфиденциальной информации такой носитель должен быть промаркирован, а вся информация на носителе должна быть зашифрована. При шифровании должны использоваться криптоалгоритмы, разрешенные к применению на территории Российской Федерации.

12.5. Учет и маркировка носителей, содержащих конфиденциальную информацию (в том числе персональные данные), осуществляются

уполномоченным Работником структурного подразделения Общества, осуществляющего обработку данной информации.

12.6. По достижении целей обработки информации (в том числе конфиденциальной) вся информация на носителе должна быть уничтожена без возможности ее восстановления.

12.7. Подключение внешних носителей информации к АСУ, АРМ и серверам (в том числе коммутационному оборудованию) технологического сегмента допускается только для Пользователей, осуществляющих эксплуатационную и техническую поддержку указанного оборудования. Используемый носитель информации должен быть промаркирован и подлежать учету.

12.8. В случае необходимости подключения внешнего носителя информации к АРМ или серверам, размещенным в технологическом сегменте и не оснащенным средствами антивирусной защиты, необходимо предварительно выполнить проверку носителя на отдельном (изолированном от технологического сегмента и сети Интернет) АРМ, с установленным АВПО с актуальными антивирусными базами.

12.9. При работе с носителями информации запрещено:

– несанкционированно подключать и использовать внешние носители информации как к АРМ и серверам, так и к другому оборудованию;

– использовать личные носители информации в производственных целях;

– использовать корпоративные носители информации Общества в личных целях, в том числе для удаленной работы на личных персональных компьютерах.

13. Правила работы с носителями ключевой информации

13.1. В Обществе применяются следующие виды ключевой информации:

– квалифицированная электронная подпись;

– неквалифицированная электронная подпись.

13.2. Квалифицированная электронная подпись используется для:

– организации юридически значимого электронного документооборота;

– акцепта заявок на платеж в ИС Общества (Подсистема ЕИС «Альфа» ИС Казначейство);

– ДБО;

– организации подключения к ГИС;

– организации подключения к государственным порталам услуг;

– в иных случаях, предусмотренных законодательством Российской Федерации и ОРД Общества.

13.3. Неквалифицированная электронная подпись используется для:

– шифрования информации, в том числе сообщений электронной почты;

– организации доступа к ИС Общества;

– организации защищенного удаленного доступа;

– в иных случаях, предусмотренных ОРД Общества.

13.4. Выпуск сертификатов ключа проверки электронной подписи осуществляется в порядке, предусмотренным соответствующим ОРД Общества.

13.5. При работе с носителями сертификата ключа проверки электронной подписи (токенами) не допускается:

– извлечение закрытого ключа из контейнера;

– передача носителя и (или) пароля на контейнер третьим лицам;

– оставление носителя в АРМ по окончании сеанса работы с электронной подписью, за исключением случаев, когда постоянное присутствие носителя обусловлено требованиями ИС и/или эксплуатационной документацией на ИС.

13.6. При прекращении трудовых отношений с Обществом Работник должен сдать имеющиеся у него носители сертификата ключа проверки электронной подписи в Подразделение ИБ.

14. Правила работы с системами ДБО

14.1. Доступ к АРМ, на котором установлены системы ДБО, предоставляется только уполномоченным соответствующим ОРД Работникам Общества.

14.2. АРМ, на котором установлены системы ДБО, должно размещаться в отдельном помещении, обеспеченном средствами контроля физического доступа в помещение.

14.3. Не допускается использование сети Интернет на АРМ с установленными системами ДБО, за исключением использования соединения банк-клиент.

14.4. Не допускается удаленное подключение к системам ДБО, в том числе к АРМ с установленными системами ДБО.

14.5. На АРМ должны быть установлены и настроены необходимые средства защиты информации в соответствии с условиями банковского обслуживания.

14.6. При увольнении указанного в пункте 14.1 настоящих Правил Работника все учетные записи, принадлежащие данному Работнику, должны быть блокированы. В случае использования неперсонифицированной учетной записи в системе ДБО должна быть произведена смена паролей такой учетной записи, а также смена пароля к контейнеру сертификата электронной подписи

и (или) блокирование (отзыв) сертификата электронной подписи, принадлежащий данному Работнику.

14.7. Для размещения закрытых ключей электронных подписей должны использоваться только внешние извлекаемые носители информации.

14.8. Ключевой носитель должен храниться в недоступном для посторонних лиц месте, например, металлическом шкафу, сейфе.

14.9. Не допускается использовать ключевой носитель для иных, кроме работы с системой ДБО, целей, в том числе для хранения файлов, электронных документов.

15. Контроль

15.1. Контроль за соблюдением настоящих Правил осуществляется ОИПО.

15.2. С целью контроля и противодействия попыткам несанкционированного доступа к конфиденциальной информации и ИС, в том числе АСУ, оборудования ИТС, Работники ОИПО могут:

– привлекать сотрудников охраны в случае оказания противодействия со стороны нарушителей;

– блокировать без предупреждения с обязательным уведомлением по электронной почте в службу технической поддержки доступ Пользователя к ЛВС, АРМ, сети Интернет, ИТС, ИС;

– приостанавливать действие сертификата ключа проверки электронной подписи Пользователя;

– требовать от Пользователя лично (с уведомлением руководителя Пользователя) или через непосредственного руководителя Пользователя предоставления объяснений по выявленным фактам нарушений настоящих Правил;

– требовать от Пользователя прекращения работы с АРМ через непосредственного руководителя Пользователя;

– требовать от Пользователя предоставления носителей информации и средств вычислительной техники, вверенных ему Обществом;

– подготавливать представление для привлечения Пользователя к ответственности за нарушение настоящих Правил;

– получать доступ к информации, обрабатываемой на АРМ Пользователя и сетевых ресурсах, в том числе сетевых папках структурных подразделений Общества, без уведомления Пользователя и (или) руководителя структурного подразделения – владельца сетевого ресурса;

– осуществлять изъятие средств вычислительной техники и носителей информации, числящихся за Пользователем и принадлежащих Обществу.

15.3. В целях совершенствования мер по обеспечению ИБ Работники ОИПО должны постоянно тестировать действие технических средств защиты информации, направленных на выявление угроз и блокирование несанкционированного доступа к конфиденциальной информации.

15.4. Работники ОИПО, в случае выявления действий, противоречащих законодательству Российской Федерации в области обеспечения ИБ, должны фиксировать их, уведомлять правоохранительные органы, оказывать содействие правоохранительным органам, в том числе при возбуждении административных и уголовных дел по фактам выявленных правонарушений.

16.Ответственность

16.1. Работники Общества несут персональную ответственность за соблюдение настоящих Правил.

16.2. По представлению ОИПО на имя заместителя генерального директора по безопасности и директора по управлению персоналом и организационному проектированию – начальника департамента управления персоналом и организационного проектирования к Работнику могут быть применены дисциплинарные взыскания в порядке, установленном законодательством Российской Федерации.

16.3. При принятии решения о привлечении Работника к дисциплинарной ответственности должна учитываться тяжесть совершенного проступка и обстоятельства, при которых проступок был совершен.

Приложение 2.
Обязательство

ОБЯЗАТЕЛЬСТВО

Я, _____
(фамилия, имя, отчество)

_____
(должность, организация)

в результате получения доступа к объектам информационной инфраструктуры АО «ЛЭСР», а также к информационно-телекоммуникационной сети АО «ЛЭСР», а также при использовании сети Интернет посредством информационной инфраструктуры АО «ЛЭСР» ознакомлен и обязуюсь:

1. Соблюдать установленный режим работы с информацией, составляющей коммерческую тайну АО «ЛЭСР».
2. Соблюдать Положение о порядке обработки персональных данных работников АО «ЛЭСР».
3. Соблюдать Правила информационной безопасности АО «ЛЭСР».
4. Не разглашать ставшую мне известной информацию, составляющую коммерческую тайну, и иную конфиденциальную информацию, обладателем которой является АО «ЛЭСР», без согласия АО «ЛЭСР», не использовать эту информацию в личных целях в течение пяти лет после прекращения доступа к такой информации.
5. Возместить в соответствии с законодательством Российской Федерации причиненные АО «ЛЭСР» убытки, возникшие в результате разглашения по моей вине информации, составляющей коммерческую тайну и иной конфиденциальной информации, обладателем которой является АО «ЛЭСР», и ставшей мне известной в связи с получением доступа к объектам информационной инфраструктуры АО «ЛЭСР» и/или к информационно-телекоммуникационной сети АО «ЛЭСР».
6. Передать АО «ЛЭСР» при прекращении или расторжении отношений имеющиеся в моем пользовании и принадлежащие АО «ЛЭСР» материальные носители информации, содержащие информацию, составляющую коммерческую тайну, и иную конфиденциальную информацию, обладателем которой является АО «ЛЭСР».

_____ _____ / _____
дата Ф. И. О. подпись