Акционерное общество
«Ленэнергоспецремонт» (АО «ЛЭСР»)

ПРИКАЗ

08.08.2025 г. Санкт-Петербург № 957

Об утверждении Политики
управления доступом АО «ЛЭСР»

В дополнение к Политике информационной безопасности АО «ЛЭСР», утвержденной приказом АО «ЛЭСР» от 14.03.2023 № 268

ПРИКАЗЫВАЮ:

1. Ввести в действие Политику управления доступом АО «ЛЭСР» (далее – Политика) согласно приложению, к настоящему приказу.

2. Первому заместителю генерального директора, главному инженеру, заместителям генерального директора, руководителям прямого подчинения генеральному директору:

2.1. Принять положение Политики к руководству и исполнению.

2.2. Определить руководителей структурных подразделений, ответственных за реализацию пункта 5.2. Политики, в соответствии с приложением 1 к Политике.

Срок: не позднее 1 месяца с даты выхода настоящего приказа.

2.3. Направить информацию о владельцах объектов критической информационной инфраструктуры (далее – КИИ) по результатам выполнения пункта 2.2. настоящего приказа в отдел информационной безопасности по форме приложения 4 к Политике.

Срок: не позднее 1 месяца с даты выхода настоящего приказа.

2.4. В соответствии с разделом 6 Политики, определить пользователей с привилегированными учетными записями (администраторов объектов КИИ) и направить их на регистрацию в отдел информационной безопасности с прохождением инструктажа.

Срок: не позднее 1 месяца с даты выхода настоящего приказа.

2.5. Организовать работу по приведению действующих организационно-распорядительных документов АО «ЛЭСР», регламентирующих предоставление доступа к информационным ресурсам (объектам КИИ) Общества, в соответствии с требованиями Политики.

2.6. Считать Политику верхнеуровневым документом по вопросам управления доступом в инфраструктуру АО «ЛЭСР».

Срок: не позднее 24.08.2025.

3. Начальнику отдела управления персоналом Румянцевой Е.Р. включить Политику в перечень документов, обязательных для ознакомления вновь принимаемых работников.

Срок: не позднее 1 месяца с даты выхода настоящего приказа.

4. Исполнение положений Политики является обязательным для всех работников Общества.

5. Исполняющему обязанности начальника информационно-программного обеспечения Мурадяну А.Г. обеспечить координацию деятельности Общества по реализации комплекса мер, предусмотренных Политикой.

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
к приказу АО «ЛЭСР»
от 08.08.2025 № 957

ПОЛИТИКА
Управления доступом АО «ЛЭСР»

Санкт-Петербург
2025

Содержание

1. Термины, определения и сокращения

В настоящей Политике использованы термины и следующие сокращения:

Авторизация	- определение и предоставление субъекту доступа соответствующих прав доступа;
Объект КИИ	- корпоративные информационные системы, обеспечивающие устойчивость финансово-хозяйственной деятельности, в том числе ИСУ; автоматизированные системы управления, обеспечивающие надежное снабжение потребителей электроэнергией; корпоративные и технологические информационно-телекоммуникационные сети, формирующие единое информационное пространство и цифровую среду взаимодействия; сети электросвязи, используемые для организации взаимодействия объектов;
Аутентификация	- проверка принадлежности субъекту доступа предъявленного им идентификатора; проверка подлинности субъекта доступа;
Безопасность информации	- состояние защищенности информации, обрабатываемой средствами вычислительной техники, от внутренних или внешних угроз
Владелец (Объекта КИИ)	- должностное лицо организации, назначаемый руководителем организации, ответственный за функционирование бизнес-процесса, обеспечивающего объектом КИИ, а также эксплуатацию и развитие функционала объекта КИИ. Термин «владелец» не означает наличие имущественных (и иных, не указанных в настоящей Политике) прав на объект Общества.
Доступ к информации	- ознакомление с информацией, её обработка, в частности, копирование модификация или уничтожение информации;
Доступность (информации)	- свойство безопасности информации, при котором субъекты доступа, имеющие права доступа, могут беспрепятственно их реализовать.
Идентификатор (доступа)	- уникальный признак субъекта доступа;
Идентификация (пользователей)	- присвоение субъектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов;
Конфиденциальность (информации)	- свойство безопасности информации, при котором доступ к ней осуществляют только субъекты доступа, имеющие на него право. Обязательное для выполнения лицом, получившем доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.
Несанкционированный доступ	- доступ к объекту, полученный в нарушении правил разграничения доступа;
Матрица доступа	- таблица, отображающая правила разграничения доступа;
Многофакторная (двухфакторная) аутентификация	- аутентификация с использованием двух (двухфакторная) или более различных факторов аутентификации;

Объект доступа	- компонент (единица) ИТ-инфраструктуры АО «ЛЭСР» или любой другой объект, доступ к которым регламентируется правилами разграничения доступа;
Правила разграничения доступа	- совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа;
Рекомендация	- описание, поясняющее действия и способы их выполнения, необходимые для достижения целей, изложенных в политике.
Роль (доступа)	- предопределённая совокупность правил, устанавливающих допустимое взаимодействие между пользователем и информационной системой;
Санкционированный доступ	- доступ к объекту, полученный строго в рамках правил разграничения доступа;
СЗИ	- средства защиты информации;
СКЗИ	- средства криптографической защиты информации;
Средства обработки информации	- любая система обработки информации, услуга или инфраструктура, или их фактическое месторасположение.
Субъект доступа	- лицо или процесс, действия которого в отношении объектов доступа регламентируются правилами разграничения доступа;
Управление доступом	- ограничение, предоставление и контроль доступа субъектов доступа к объектам доступа в информационной системе в соответствии с установленными правилами разграничения доступа;
Целостность (информации)	- свойство безопасности информации, при котором отсутствует любое её изменение либо изменение субъектами доступа, имеющими на него право;
АСУ, АСТУ	автоматизированные системы управления (в том числе автоматизированные рабочие места, 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 программное обеспечение), обеспечивающие надежное снабжение потребителей электроэнергией, а также САЦ, ЦУС
КИИ	Критическая информационная инфраструктура
ЗОКИИ	Значимый ОКИИ, объекту КИИ присвоена категория значимости
КИС	корпоративные информационные системы (в том числе машинные носители информации, автоматизированные рабочие места, серверы, средства обработки буквенно-цифровой, графической, видео- и речевой информации, микропрограммное, общесистемное, прикладное программное обеспечение), обеспечивающие устойчивость финансово-хозяйственной деятельности
ИТС	корпоративные и технологические информационно-телекоммуникационные сети (в том числе телекоммуникационное оборудование, программное обеспечение, система управления, линии связи), формирующие единое информационное пространство и цифровую среду взаимодействия

ИСУ	интеллектуальные системы учета электроэнергии, системы автоматизации процессов формирования балансов и объемов услуг по передаче электрической энергии, системы планирования работ и управляемые устройства, личный кабинет потребителя
Средства обеспечения жизнедеятельности объектов	гарантированные и бесперебойные системы электропитания и заземления объектов, системы пожарной и охранной сигнализации, электронные системы контроля и управления доступом на территорию и в помещения, системы громкоговорящей связи и оповещения, системы кондиционирования, отопления, вентиляции и пожаротушения, видеонаблюдение
ОРД	Организационно-распорядительная документация

2. Общие положения

2.1. Настоящая Политика определяет цели и задачи в области обеспечения защиты информации, а также общие намерения и направления при управлении доступом к объектам критической информационной инфраструктуры АО «ЛЭСР» (далее – объект КИИ).

2.2. К объектам защиты в контексте обеспечения безопасности критической информационной инфраструктуры относятся:

- корпоративные информационные системы, обеспечивающие устойчивость финансово-хозяйственной деятельности, в том числе ИСУ;
- автоматизированные системы управления, обеспечивающие надежное снабжение потребителей электроэнергией;
- корпоративные и технологические информационно-телекоммуникационные сети, формирующие единое информационное пространство и цифровую среду взаимодействия;
- сети электросвязи, используемые для организации взаимодействия объектов;
- информация конфиденциального характера, в том числе технологическая информация, представляющая коммерческую ценность в силу неизвестности третьим лицам.

2.3. Настоящая политика является элементом Политики информационной безопасности АО «ЛЭСР» и содержит:

- политику учета объектов КИИ (Раздел 5);
- политику управления доступом (Раздел 6);
- политику идентификации и аутентификации пользователей (Раздел 7);
- парольную политику (Раздел 8);
- политику использования мобильной вычислительной техники (Раздел 9).

2.4. В рамках настоящей Политики в качестве получателей прав доступа к объектам КИИ (субъектов доступа, пользователей) рассматриваются:

- работники АО «ЛЭСР»;

- администраторы, осуществляющие системное и прикладное администрирование объектов критической информационной инфраструктуры, являющиеся работниками АО «ЛЭСР»;
- администраторы, осуществляющие системное и прикладное администрирование объектов критической информационной инфраструктуры, являющиеся работниками подрядчиков АО «ЛЭСР»;
- работники аффилированных структур, имеющие доступ к объектам критической информационной инфраструктуры АО «ЛЭСР»;
- граждане, которым предоставляется доступ к объектам критической информационной инфраструктуры АО «ЛЭСР».

2.5. Настоящая Политика разработана на основании и в развитие:

- Политики информационной безопасности АО «ЛЭСР»
- приказа АО «ЛЭСР» «Об утверждении Политики информационной безопасности АО «ЛЭСР»

Настоящая Политика создана и должна пересматриваться с учетом требований технологических процессов АО «ЛЭСР» и задач информационной безопасности.

3. Цели политики управления доступом

Целями настоящей Политики являются:

- предотвращение несанкционированного доступа к объектам КИИ АО «ЛЭСР»;
- предотвращение нарушений прав субъектов данных при обработке информации;
- недопущение деструктивного воздействия на технические средства обработки информации;
- недопущение деструктивного информационного воздействия на информацию.

4. Основные принципы управления доступом

4.1. Обоснованность доступа: должны существовать объективные причины, зафиксированные установленным порядком в соответствующих документах (соглашениях, регламентах, порядках, должностных инструкциях и др.), обуславливающие необходимость предоставления конкретному пользователю доступа к объекту с определёнными полномочиями.

4.2. Разграничение прав доступа: субъектам доступа предоставляются только те права, которые необходимы ему для выполнения возложенных на него функциональных обязанностей.

4.3. Однозначность управления доступом: перечень объектов и прав к ним, доступных пользователю, определяется набором типовых ролей (полномочий, шаблонов, профилей), описанных в эксплуатационной или иной документации на соответствующий объект КИИ.

4.4. Документированность: управление (предоставление, изменение, блокировка, аннулирование) правами доступа к объектам осуществляется исключительно на основании документа (заявки, иного обращения установленной формы на предоставление/изменение прав доступа), содержащей всю необходимую информацию для её однозначного и правильного выполнения.

4.5. Требования к мерам защиты информации, реализуемые при осуществлении доступа (требования к применяемым средствам защиты информации и организационным мероприятиям), должны соответствовать законодательству Российской Федерации.

5. Объект КИИ как объекты доступа (политика учета объектов КИИ)

5.1. Настоящая Политика регулирует процессы управления доступом к объектам КИИ АО «ЛЭСР».

5.2. Все объекты КИИ должны учитываться, иметь назначенного владельца (рекомендации по определению владельца для различных объектов определены в приложении 1 к настоящей Политике), а информация, обрабатываемая с использованием объекта, должна быть классифицирована (пример приложение 4). При необходимости (обязательно для объектов централизованных компонентов критической информационной инфраструктуры АО «ЛЭСР» – ЦОДов) должны быть определены ограничения – определение групп субъектов доступа.

5.3. В рамках учета объектов КИИ требуется определить ответственного за поддержку соответствующих мер и средств контроля и управления. Реализация определённых мер и средств контроля и управления при необходимости может быть делегирована ответственным, но ответственность за надлежащую защиту объектов при этом не снимается.

5.4. В отношении объектов КИИ, реализующих предоставление доступа в соответствии с ролями доступа, определение владельца, классификация информации и определение ограничений проводится в отношении каждой из ролей доступа.

5.5. Владелец объекта несет ответственность за:

- классификацию информации, в том числе в объектах КИИ, связанных со средствами обработки информации;
- определение и периодический пересмотр ограничений и классификаций доступа, принимая в расчет применимые политики управления доступом.

5.6. При учете объектов допускается обозначать группы объектов, действующих вместе, для обеспечения функции, такой как «услуга». В данном случае владелец «услуги» является ответственным за поставку «услуги» и функционирование объектов, которые обеспечивают данную «услугу».

5.7. Информация объекта КИИ должна быть классифицирована, чтобы определить необходимость, приоритеты и предполагаемую степень защиты при обработке информации.

5.8. Информация в критической информационной инфраструктуре АО «ЛЭСР» подразделяется исходя из законодательных требований как:

- общедоступная информация:
  - публичная информация;
  - служебная информация;
- информация ограниченного доступа:
  - сведения конфиденциального характера;
  - сведения, составляющие коммерческую тайну;
  - персональные данные;
- иная информация, в отношении которой Обществом принято решение о необходимости ее защиты.

6. Правила управления доступом (политика управления доступом)

6.1. Доступ к объектам КИИ предоставляется субъектам доступа (в том числе процессам), прошедшим этапы идентификации и аутентификации, в соответствии с разделом 7 настоящей Политики. Исключение могут составлять действия, указанные в Перечне действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификация (Приложение 3).

6.2. Доступ к информации, относящейся к информации ограниченного распространения и информации ограниченного доступа, а также к объектам, являющимся средствами обработки информации такой классификации, допускается только для авторизованных субъектов доступа.

6.3. Необходимость авторизации доступа может быть определена владельцем и в отношении общедоступной информации и объектов, являющихся средствами обработки информации указанной классификации. Данная необходимость должна быть определена в отношении объектов в случае необходимости обеспечения целостности и доступности информации.

6.4. Настоящая Политика предусматривает следующие стандартные категории учетных записей (пользователей):

- Непривилегированные учетные записи – по умолчанию для всех пользователей (субъектов доступа) к объектам критической информационной инфраструктуры АО «ЛЭСР», которым не делегированы права привилегированных учетных записей;
- Привилегированные учетные записи – для администраторов объектов критической информационной инфраструктуры АО «ЛЭСР» и системных компонентов:

- Учетные записи системных администраторов – для пользователей, уполномоченных на выполнение действий по управлению (администрированию) инфраструктурой системы;
- Учетные записи администраторов учетных записей (доступа) – для пользователей, уполномоченных на выполнение действий по управлению учетными записями и их правами в критической информационной инфраструктуре АО «ЛЭСР»;
- Учетные записи администраторов безопасности – для пользователей, уполномоченных на выполнение действий по управлению средствами защиты информации;
- Технологические (сервисные) учетные записи – для общесистемных компонентов критической информационной инфраструктуры АО «ЛЭСР»

6.5. Использование привилегированных учетных записей разрешается только для исполнения административных функций. Использование административных учетных записей при выполнении работ не связанных с выполнением административных функций запрещено.

6.6. Должно быть обеспечено разграничение между отдельными должностными лицами следующих полномочий:

- по обработке информации (пользователей);
- по администрированию объекта КИИ (системные администраторы);
- по управлению системой защиты информации (администратор безопасности);
- по контролю (мониторингу) за обеспечением уровня защищённости информации;
- по обеспечению функционирования объектов критической информационной инфраструктуры АО «ЛЭСР».

6.7. Администратором, имеющим права по передаче полномочий по администрированию объектов КИИ и систем защиты информации другим лицам и осуществляющим контроль за использованием переданных полномочий в критической информационной инфраструктуре АО «ЛЭСР», является структурное подразделение ИА АО «ЛЭСР», в полномочия которого входит организация и координация процессов управления информационной безопасностью.

6.8. Процессы предоставления доступа к объектам КИИ, требующим авторизации субъектов доступа, осуществляются с учетом разделения следующих полномочий:

- по запросу доступа;
- по авторизации доступа;
- по администрированию доступа.

6.9. Запрос доступа:

- в отношении привлекаемых в рамках договоров специалистов и экспертов запрос доступа осуществляется руководителем (уполномоченном лицом) организации, с которой непосредственно заключен контракт или договор;
- в отношении компонента критической информационной инфраструктуры (процесса) запрос доступа осуществляется начальником структурного подразделения – инициатором запроса, с согласованием владельца объекта КИИ, к которому относится данный компонент.

6.10. Авторизация (подтверждение) доступа:

- в отношении работников АО «ЛЭСР» подтверждение доступа осуществляется совместно:
  - начальником структурного подразделения ИА АО «ЛЭСР», к которому относится пользователь;
  - начальником структурного подразделения ИА АО «ЛЭСР», в функции которого входит организация обеспечения выполнения нормативно-правовых документов по защите ОКИИ, конфиденциальных сведений и персональных данных;
  - начальником структурного подразделения ИА АО «ЛЭСР», являющимся владельцем объекта (объекта доступа);
- в отношении привлекаемых в рамках договоров специалистов и экспертов подтверждение доступа осуществляется совместно:
  - руководителем или уполномоченным лицом АО «ЛЭСР», заключившей соответствующий контракт (договор);
  - начальником структурного подразделения, являющимся владельцем объекта (объекта доступа);
  - начальником структурного подразделения АО «ЛЭСР», в функции которого входит организация обеспечения выполнения нормативно-правовых документов по защите ОКИИ, конфиденциальных сведений и персональных данных.

6.11. Администрирование доступа осуществляется пользователями критической информационной инфраструктуры АО «ЛЭСР», уполномоченными на выполнение действий по управлению правами доступа к соответствующему объекту (администраторы доступа).

6.12. Пользователи с привилегированными учетными записями (администраторы объектов КИИ) при выполнении свои функциональных обязанностей должны руководствоваться действующим законодательством РФ и организационно-распорядительными документами АО «ЛЭСР». Ознакомление данных пользователей с руководящими документами осуществляется работниками департамента информационной безопасности в соответствии с Порядком проведения инструктажей по информационной

безопасности пользователей привилегированных учетных записей АО «ЛЭСР» (приложение 6).

6.13.Возможности администратора доступа администрировать собственные права доступа должны быть ограничены в случае наличия такой технической возможности.

6.14.Запрос, авторизация и администрирование доступа осуществляются при условии заверения всеми ответственными лицами указанных действий личной подписью, электронной подписью или при помощи информационных систем. Хранение указанных подписей должно обеспечиваться администраторами доступа на срок не менее двух лет после отзыва (окончания) прав доступа.

6.15.Запрос и авторизация доступа могут быть оформлены как заявка, матрица доступа (допускается использование должностей и категорий пользователей вместо конкретных идентификаторов пользователей) или как иной документ при условии соблюдения принципов документированности в соответствии с утвержденным в обществе ОРД. Допускается объединение учетных записей в группу пользователей.

6.16.Права доступа в отношении пользователей, у которых изменились должностные обязанности (переведенных на другую должность) или уволившихся, должны быть немедленно пересмотрены (отменены – в случае увольнения) администраторами доступа.

6.17.Права доступа в отношении привилегированных учетных записей должны регистрироваться администраторами доступа в соответствующих журналах и пересматриваться не менее двух раз в три месяца.

6.18.Должна быть обеспечена блокировка попыток несанкционированной загрузки нештатной среды (операционной системы) на объектах КИИ, а также контроль целостности системного программного обеспечения и аппаратных компонент объектов.

6.19.В случае неактивности пользователя при доступе к объекту более 1 (одного) часа в рамках одного сеанса (в случае технической возможности для реализации), данный сеанс доступа должен быть заблокирован.

6.20.В централизованном сегменте критической информационной инфраструктуры АО «ЛЭСР» рекомендуется осуществлять управление информационными потоками при передаче информации между устройствами, сегментами, включающее в себя:

- фильтрацию информационных потоков в соответствии с установленными правилами управления потоками;
- разрешение передачи информации только по установленным маршрутам (профилям приложений);
- изменение (перенаправление) маршрута передачи информации;
- запись во временное хранилище информации для анализа и принятия решения о возможности ее дальнейшей передачи.

6.21. Управление информационными потоками в рамках пункта 6.18. настоящей Политики должно осуществляться на основе атрибутов (меток) безопасности, связанных с передаваемой информацией, источниками и получателями информации.

7. Правила управления учетными записями пользователей (политика идентификации и аутентификации)

7.1. При идентификации пользователей должны использоваться уникальные идентификаторы, позволяющие отследить действия конкретных пользователей в конкретный момент времени (повторное использование одного идентификатора различными субъектами доступа должно быть исключено).

7.2. Использование общих учетных записей (учетных записей, которыми пользуется несколько пользователей) в корпоративном сегменте сети запрещено. В технологическом сегменте использование общих учетных записей должно быть минимизировано и обосновываться особенностью выполнения технологических процессов.

7.3. Аутентификация пользователей в критической информационной инфраструктуре АО «ЛЭСР» допускается (набор мер аутентификации определяется исходя из требований к объекту КИИ):

- с использованием пароля, соответствующего разделу 8 настоящей Политики;
- с использованием средств криптографической защиты информации и усиленной электронной подписи с применением сертификата ключа проверки электронной подписи, используемые в АО «ЛЭСР»;
- исключительно для доступа к общедоступной информации и объектам, являющимся средствами обработки информации указанной классификации, допускается по согласованию с владельцем использование для аутентификации иной информации в электронном виде (например, в виде файла или ссылки в электронном сообщении);
- с использованием сертифицированных по требованиям ИБ электронных идентификаторов;
- с одновременным использованием нескольких вышеперечисленных способов (многофакторная аутентификация).

7.4. Процедуры регистрации и блокировки учетных записей пользователей (и других пользовательских идентификаторов) должны быть формально учтены. В организации должен быть назначен ответственный за создание, присвоение и блокировку идентификаторов, а также за временное хранение, выдачу и инициализацию аутентификационной информации.

7.5. Для корпоративного сегмента сети соответствующими администраторами учетных записей должна проводиться периодическая (не менее двух раз в три месяца) проверка и блокирование избыточных пользовательских идентификаторов (учетных записей). Под избыточными

пользовательскими идентификаторами понимаются неиспользуемые более 45 дней либо задублированные (при использовании в одной системе учетных записей нескольких идентификаторов, связанных с одним субъектом доступа). В технологическом сегменте проводится проверка и блокировка неиспользуемых учетных записей не реже 1 раза в год, в рамках планово-профилактического обслуживания.

7.6. Пользователи критической информационной инфраструктуры АО «ЛЭСР» при получении аутентификационной информации в обязательном порядке должны под подпись ознакомиться с настоящей Политикой. При этом особое внимание пользователя необходимо обратить на обязанности пользователя (приложение 2).

7.7. Число разрешенных неудачных попыток аутентификации должно быть ограничено:

- для учетных записей пользователей – не более 3 в час;
- для привилегированных учётных записей – не более 3 в сутки.

7.8. После превышения, указанного в пункте 7.7 настоящей Политики количества попыток аутентификации устройство, с которого осуществлялись попытки аутентификации, должно быть заблокировано (при наличии технической возможности). И может быть разблокировано по решению департамента информационной безопасности

7.9. Попытки аутентификации и инициируемых ими процессов в критической информационной инфраструктуре АО «ЛЭСР» должны записываться и храниться.

7.10.Процедура регистрации (создания идентификационной информации) в системе должна быть спроектирована так, чтобы свести к минимуму возможность несанкционированного доступа.

7.11.Необходимо, чтобы процедура начала сеанса раскрывала минимум информации о системе, во избежание оказания какой-либо ненужной помощи неавторизованному пользователю.

7.12.При вводе паролей в информационной системе они не должны отображаться на экране.

7.13.Многократное использование одного идентификатора и параллельных сеансов доступа к одному объекту должно быть ограничено.

7.14.При аутентификации пароли (и иная аутентификационная информация) не должны передаваться в открытом виде по сети.

7.15.В случае компрометации аутентификационной информации администраторами учетных записей должны быть приняты все меры по блокированию действий соответствующих учетных записей до проведения процедур по замене аутентификационной информации. По факту компрометации аутентификационной информации должны быть проведены мероприятия по выявлению причин компрометации и ее последствий.

7.16.Для идентификации и аутентификации в критической информационной инфраструктуре АО «ЛЭСР» рекомендуется использовать единый сервис.

7.17.В критической информационной инфраструктуре до начала информационного взаимодействия (передачи защищаемой информации от устройства к устройству) должна осуществляться идентификация и аутентификация устройств (технических средств обработки информации).

7.18.Идентификация устройств осуществляется по логическим именам устройств (доменным именам).

7.19.Аутентификация устройств обеспечивается с использованием протоколов аутентификации.

7.20.В критической информационной инфраструктуре АО «ЛЭСР» рекомендуется осуществлять идентификацию и аутентификацию объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа с использованием свидетельств подлинности информации.

7.21.Внешние пользователи информационной системы должны однозначно идентифицироваться и аутентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации в соответствии с приложением 3 к настоящей Политике.

8. Управление паролями пользователей (парольная политика)

8.1. Выдача паролей пользователю осуществляется исключительно при условии ознакомления пользователя под подпись с обязанностями по соблюдению требований информационной безопасности (приложение 2).

8.2. Должностные лица (администраторы учетных записей), ответственные за хранение, выдачу, инициализацию и блокировку паролей в организациях должны быть назначены приказом.

8.3. Создание (смена) паролей может:

- осуществляться самостоятельно пользователем – предпочтительный вариант;
- осуществляться администратором учетных записей – в случае особенности технологического процесса, в том числе при использовании общих учетных записей.

8.4. В случае самостоятельной смены пользователем личных паролей администратором учетных записей первоначально или повторно (в случае утери) предоставляется временный пароль, который подлежит немедленной принудительной замене пользователем после его первого использования для доступа.

8.5. Регламентами и порядками доступа к объектам должны быть предусмотрены меры проверки личности пользователя, прежде чем ему будет предоставлен новый, заменяющий или временный пароль.

8.6. В случае управления паролями администратором учетных записей администратором обеспечивается запись новых и замещающих паролей на парольной карте и их безопасное хранение в запечатанном виде на всё время использования пароля.

8.7. Пароли следует выдавать пользователям безопасным способом (обеспечивающим их конфиденциальность).

8.8. Пароли должны быть уникальны для каждого пользователя, не должны быть легко угадываемыми. Пароли должны формироваться с учетом следующих требований к сложности пароля (для непривилегированных учетных записей):

- минимальная длина паролей – 8 символов;
- строчные латинские буквы: abcd...xyz;
- прописные латинские буквы: ABCD...XYZ;
- цифры: 123...90;
- специальные символы: !%()+ и т.д.

8.9. Для привилегированных учетных записей должны соблюдаться следующие требования к сложности пароля:

- минимальная длина паролей – 12 символов;
- строчные латинские буквы: abcd...xyz;
- прописные латинские буквы: ABCD...XYZ;
- цифры: 123...90;
- специальные символы: !%()+ и т.д.

8.10. Периодичность обязательной смены пароля:

- в корпоративном сегменте сети пароли непривилегированных учетных записей должны меняться каждые 90 дней, а привилегированных учетных записей каждые - 30 дней.
- в технологическом сегменте смена паролей на оборудовании СДТУ должна проводиться не реже 1-2 раз в год, в рамках планово-профилактического обслуживания.

8.11. Пользователи должны подтверждать получение паролей.

8.12. Хранение (и иная обработка) паролей в критической информационной инфраструктуре АО «ЛЭСР» должно производиться только в защищенной форме (с использованием СКЗИ – в электронной форме, и применением организационных мер – в иных случаях).

8.13. Пароли поставщика (разработчика/изготовителя), установленные по умолчанию, должны быть изменены после инсталляции в критической информационной инфраструктуре АО «ЛЭСР» лицом, осуществившем указанную инсталляцию, после чего на парольной карте переданы соответствующему администратору учётных записей.

8.14.Пользователи обязаны обеспечить конфиденциальность паролей, в том числе избегать запись паролей (например, на бумаге, в файле программного обеспечения или карманных устройствах), если не может быть обеспечено безопасное хранение и способ хранения не утверждён.

8.15.Пользователи обязаны сообщать администратору доступа о всех признаках возможной компрометации пароля.

8.16.Запрещается использование одного и того же пароля для работы в критической информационной инфраструктуре АО «ЛЭСР» и для личных целей (для доступа к личной электронной почте, для доступа к социальным сетям, личным аккаунтам в интернет-магазинах и прочее).

9. Удаленный доступ пользователей (политика использования мобильной вычислительной техники)

9.1. Удаленный доступ пользователей к объектам КИИ, опубликованным в сети общего пользования Интернет, возможен исключительно для объектов, к которым разрешен пользовательский доступ.

9.2. В случае необходимости предоставления удаленного доступа к объектам, требующим авторизации, или объектам, к которым одновременно осуществляется доступ пользователей из пределов информационной системы, должны выполняться следующие требования:

- на мобильной вычислительной технике должны быть реализованы необходимые меры защиты информации;
- удаленный доступ должен осуществляться исключительно по защищенным с использованием сертифицированного СКЗИ каналам связи;
- должна использоваться многофакторная (двухфакторная) аутентификация;
- перечень ip-адресов в сети Интернет с которого предоставляется доступ к объектам, должен быть ограничен.

9.3. При удаленном доступе пользователь обязан обеспечить необходимую защиту места дистанционной работы в отношении, например, хищения оборудования и информации, несанкционированного раскрытия информации, несанкционированного удаленного доступа к внутренним системам организации или неправильного использования оборудования.

9.4. Виды работ, которые могут быть осуществлены удаленно, время работы, классификацию информации, к которой разрешён доступ сотруднику в дистанционном режиме, должны утверждаться руководителем организации.

9.5. Пользователи получают право удаленного доступа к информационным ресурсам общества с учетом их должностных обязанностей и взаимоотношений с организацией.

9.6. Сотрудникам, использующим в работе портативные компьютеры организации, может быть предоставлен удаленный доступ к сетевым ресурсам организации в соответствии с правами в корпоративной информационной системе.

9.7. Сотрудникам, работающим удаленно с использованием компьютера, не принадлежащего организации, запрещено копирование данных на компьютер, с которого осуществляется удаленный доступ.

9.8. Сотрудники и третьи лица, имеющие право удаленного доступа к информационным ресурсам организации, должны соблюдать требование, исключающее одновременное подключение их компьютера к VPN сети организации и к каким-либо другим VPN сетям, не принадлежащим Компании.

9.9. Все компьютеры, подключаемые посредством удаленного доступа к информационной сети организации, должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления.

9.10.Каждый сотрудник обязан немедленно уведомить руководителя обо всех случаях предоставления несанкционированного доступа третьих лиц к ресурсам корпоративной сети.

9.11.Доступ третьих лиц к информационным системам Компании должен быть обусловлен производственной необходимостью. В связи с этим порядок доступа к информационным ресурсам Компании должен быть четко определен, контролируем и защищен.

Приложение 1
к Политике Управления доступом АО «ЛЭСР»

Рекомендации по определению владельца объекта КИИ

В общем случае владельцем объекта КИИ определяется руководитель структурного подразделения, ответственный за использование указанного объекта. В отношении конкретных объектов определение владельца рекомендуется осуществлять в соответствии с таблицей:

№	Объект КИИ	Определение владельца
1.	Серверные комплексы	Владельцем определяется структурное подразделение в обязанности которого входит обеспечение функционирования серверных комплексов или владельцы информационного ресурса или информации размещаемого на данном серверном комплексе.
2.	Рабочие станции, технические средства ввода/вывода информации, комплексы сканирования документов, принтеры, средства хранения и архивирования данных	Владельцем определяется структурное подразделение, в пользование которого выдано оборудование.
3.	Активное и пассивное коммуникационное оборудование, система управления, мониторинга и обслуживания сетевой инфраструктуры	Владельцем определяется структурное подразделение в обязанности которого входит обеспечение функционирования телекоммуникационных сетей в организации.
4.	Общесистемное программное обеспечение (операционные системы, системы управления базами данных)	Владельцем определяется структурное подразделение в обязанности которого входит обеспечение функционирования общесистемного программного обеспечения или структурное подразделение, являющееся владельцем оборудования, на котором функционирует общесистемное ПО.
5.	Средства защиты информации	Владельцем объекта определяется структурное подразделение в обязанности которого входит обеспечение информационной безопасности
6.	Средства обеспечения жизнедеятельности объектов	Владельцем объекта определяется структурное подразделение в обязанности которого входит обеспечение работоспособности соответствующего средства
7.	Корпоративные информационные системы, автоматизированные системы управления	Владельцем определяется структурное подразделение ответственное за функционирование бизнес-процесса или руководитель эксплуатирующего подразделения

		(владелец информации/данных). В случае нескольких владельцев разных бизнес-процессов, владелец определяется руководителем (заместителем руководителя) организации.

Приложение 2
к Политике Управления доступом АО «ЛЭСР»

Обязанности пользователя при работе с объектами критической информационной инфраструктуры АО «ЛЭСР»

1. Целью настоящего документа является обеспечение уверенности в том, что работники АО «ЛЭСР», а также подрядчики (исполнители контрактов и договоров) осведомлены об угрозах и проблемах, связанных с информационной безопасностью, о мере их ответственности и обязательствах, что снижает риск человеческого фактора.

2. Пользователь обязан ознакомиться с соответствующей эксплуатационной документацией перед использованием объекта КИИ, понимать свои обязанности при работе с объектами и не использовать объекты для целей, не соответствующих должностным обязанностям.

3. При использовании объектов КИИ пользователи должны обеспечивать сохранность аутентификационной информации, в том числе:

- сохранять конфиденциальность паролей и закрытой ключевой информации;
- избегать записи паролей, если не может быть обеспечено его безопасное хранение и способ хранения не утвержден;
- при появлении любого признака возможной компрометации системы или пароля изменять пароли и сообщать об этом администратору информационной безопасности (oib@lenenergo.ru или по телефону в департамент информационной безопасности);
- изменять временные пароли при первом начале сеанса;
- не включать пароли ни в какой автоматизированный процесс начала сеанса, например, с использованием хранимых макрокоманд или функциональных клавиш;
- не использовать коллективно индивидуальные пользовательские пароли;
- не использовать один и тот же пароль для работы в критической информационной инфраструктуре АО «ЛЭСР» и для личных целей.

4. Пользователь несет исключительную личную ответственность за все действия, осуществленные с использованием его идентификатора (имени учетной записи или др.) и аутентификационной информацией.

5. Все пользователи при работе с объектами КИИ должны обеспечивать возможные процедуры по обеспечению безопасности, в том числе:

- завершать активные сеансы по окончании работы, если отсутствует соответствующий механизм блокировки, например, защищенная паролем экранная заставка;

- завершить сеанс на виртуальной инфраструктуре, серверах и офисных персональных компьютерах, когда работа завершена (т.е. не только выключить экран персонального компьютера или терминал);
- обеспечивать безопасность персональных компьютеров или терминалов от несанкционированного использования с помощью блокировки клавиатуры или эквивалентных средств контроля, например, доступа по паролю, когда оборудование не используется.

6. Необходимо обеспечить политику «чистого стола» в отношении бумажных документов и носителей данных, а также политику «чистого экрана» в отношении средств обработки информации. Политика «чистого стола» и «чистого экрана» должна учитывать классификацию информации, законодательные и договорные требования, а также соответствующие риски. В рамках соблюдения политик «чистого стола» и «чистого экрана» необходимо обеспечить выполнение следующих рекомендаций:

- носители (бумажные или электронные), содержащие информацию ограниченного доступа или ограниченного распространения, а также иной критической информации, когда они не используются, следует убирать и запирать (лучше всего в несгораемый сейф или шкаф), особенно когда помещение пустует;
- компьютеры, когда их оставляют без присмотра, следует выключать или защищать посредством механизма блокировки экрана или клавиатуры, контролируемого паролем, носителем ключевой информации или аналогичным механизмом аутентификации пользователя, а также необходимо применять кодовые замки, пароли или другие меры и средства контроля и управления в то время, когда эти устройства не используются;
- необходимо обеспечить защиту пунктов приема/отправки корреспонденции, а также автоматических факсимильных аппаратов;
- документы, содержащие информацию ограниченного доступа или ограниченного распространения, а также иную критическую информацию, необходимо немедленно изымать из принтеров.

Приложение 3
к Политике Управления доступом АО «ЛЭСР»

Перечень действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификация

№	Наименование действия
1	Доступ к общедоступной информации и иным общедоступным ресурсам (в том числе сетевым ресурсам, файловым хранилищам и прочее)
2	Доступ к веб-сайтам, порталам, содержащим открытую информацию (в том числе корпоративному порталу АО «ЛЭСР»)
3	Доступ к системам информационно-правового обеспечения.
4	Действия привилегированных пользователей (администраторов), направленные на восстановление работоспособности системы и ее отдельных компонентов
5	Действия привилегированных пользователей (администраторов), направленные на восстановление доступности информации в критической информационной инфраструктуре АО «ЛЭСР»

Приложение 4
к Политике Управления доступом АО «ЛЭСР»

Таблица учета Владельца объекта КИИ (системы)

Наименование объекта КИИ (системы)	**ФИО Владельца**	**Должность**	**Классификация, обрабатываемых объектов КИИ (системой) данных**

Приложение 5
к Политике Управления доступом АО «ЛЭСР»

УВЕДОМЛЕНИЕ
Ответственность пользователей при работе с объектами критической информационной инфраструктуры АО «ЛЭСР»

В соответствии с Федеральным законом № 187-ФЗ от 26.07.2017 вся информационная инфраструктура субъектов электроэнергетики (включая информационные системы, автоматизированные системы управления, информационно-телекоммуникационные сети и входящие в них компоненты - персональные компьютеры, сетевое и серверное оборудование, программное обеспечение), а также организаций, которые обеспечивают взаимодействие ИС, АСУ, ИТС или сетей электросвязи субъектов электроэнергетики относится к объектам критической информационной инфраструктуры, независимо от присвоенной категории значимости. Информация, хранящаяся и обрабатываемая объектами критической информационной инфраструктуры и входящими в них компонентами, относится к охраняемой компьютерной информации.

Федеральным законом от 26.05.2021 №141-ФЗ устанавливается административная ответственность за:

- нарушение требований в области обеспечения безопасности критической информационной инфраструктуры (далее - КИИ), в том числе за нарушение требований к созданию систем безопасности значимых объектов КИИ (вступает в силу с 01.09.2021);
- нарушение порядка информирования о компьютерных инцидентах, реагирования на них и принятия мер по ликвидации последствий;
- нарушение порядка обмена информацией о компьютерных инцидентах между субъектами КИИ, между субъектами КИИ и уполномоченными органами иностранных государств, международными, международными неправительственными и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты.

Уголовный кодекс РФ Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. Содержание статьи уголовного кодекса в таблице 1.

Таблица 1

Ч.1	Создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации, -наказываются принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до пяти лет со штрафом в размере от пятисот

	тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.
Ч.2	Неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ, если он повлек причинение вреда критической информационной инфраструктуре Российской Федерации, - наказывается принудительными работами на срок до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет и с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до шести лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.
Ч.3	Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации, -наказывается принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового либо лишением свободы на срок до шести лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.
Ч.4	Деяния, предусмотренные частью первой, второй или третьей настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения, - наказываются лишением свободы на срок от трех до восьми лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.5. Деяния, предусмотренные частью первой, второй, третьей или четвертой настоящей статьи, если они повлекли тяжкие последствия, -наказываются лишением свободы на срок от пяти до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.

В соответствии с частью 2, 3 ст.274.1 УК РФ, уголовно наказуемы:

- неправомерный доступ к информации в КИИ если он повлек причинение вреда критической информационной инфраструктуре;

- нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре либо правил доступа к охраняемой информации, информационным системам, информационно-телекоммуникационным сетям,

автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда критической информационной инфраструктуре.

Согласно имеющейся правоприменительной практики, причинением вреда признается сам факт раскрытия охраняемой компьютерной информации третьим лицам (в том числе внешним почтовым или облачным сервисам).

В соответствии с Правилами информационной безопасности ПАО «Россети» и ПАО «ФСК ЕЭС», утвержденными приказом ПАО «Россети» и ПАО «ФСК ЕЭС» от 24.06.2022 № 289/189, использование сторонних почтовых сервисов, облачных хранилищ для передачи информации не допускается.

Передача материалов (сетевых схем, проектной, рабочей, эксплуатационной документации и иной информации) об объекте КИИ третьим лицам и/или с использованием сторонних электронных сервисов (личной электронной почты, облачных хранилищ, иным незащищенным способом) может быть расценено как деяние, подлежащее привлечению к ответственности по ст.274.1 ч.2 или ст.274.1 ч.3 УК РФ.

Ознакомлен _____ «___» _____ 20___

Приложение 6
к Политике Управления доступом АО «ЛЭСР»

Порядок проведения инструктажей по информационной безопасности пользователей привилегированных учетных записей АО «ЛЭСР»

1. Основанием проведения инструктажа является наличие запроса на предоставление/изменение доступа к ресурсам ОКИИ с указанной в реквизитах электронной почтой получателя доступа (далее – Запрос), оформленного на привилегированную учетную запись, в соответствии с Политикой.

2. Предоставление/изменение прав доступа пользователю с привилегированной учетной записью (далее – Пользователь) к информационным, программным и иным ресурсам осуществляется после проведения инструктажа по информационной безопасности в соответствии с настоящим Порядком.

3. Инструктаж осуществляется работником департамента информационной безопасности (далее – Инструктирующий).

4. При получении Запроса Инструктирующий назначает дату, время и место проведения инструктажа, о чем не позднее 1 (одного) рабочего дня уведомляет Пользователя по указанным в Запросе контактным данным. При невозможности направления сообщения о планируемом инструктаже Пользователю сообщение направляется контактному лицу в соответствии с реквизитами, указанными в Запросе.

5. Пользователь обязан в установленные сроки прибыть в указанное место для прохождения Инструктажа. При невозможности прибытия в установленный срок в установленное место Пользователь обязан заблаговременное сообщить Инструктирующему о данном факте, после чего Инструктирующим назначаются новые дата и время проведения Инструктажа.

6. Инструктаж проводится в устной форме.

7. Результат прохождения Инструктажа фиксируется в журнале в соответствии с приложением 7 к Политике.

Приложение 7
к Политике Управления доступом
АО «ЛЭСР»

ЖУРНАЛ

проведения инструктажей по информационной безопасности пользователей привилегированных учетных записей

АО «ЛЭСР»

Начат « ___ » _____ 202 __ г.

Окончен « ___ » _____ 202 __ г.

Список документов[1]

1. Политика информационной безопасности АО «ЛЭСР»;
2. Правила информационной безопасности АО «ЛЭСР»;
3. Политика управления доступом АО «ЛЭСР»;

[1] Список документов может быть изменен по усмотрению департамента информационной безопасности АО "ЛЭСР"»

Инструкция по ведению журнала

В графе **«Ф.И.О.»** указываются фамилии, имена и отчества получателей прав доступа к ОКИИ.

В графе **«Организация»** указывается место работы получателя прав доступа к ОКИИ. Если получатель является работником АО «ЛЭСР», то в данной графе пишется «АО «ЛЭСР».

В графе **«Контакты»** указываются контакты для связи – номер телефона и/или электронная почта.

В графе **«Система обслуживания»** указывается система, администратором которой является получатель прав доступа к ОКИИ.

В графе **«Номер договора»** указывается номер договора, заключенного между АО «ЛЭСР» и организацией получателя прав доступа к ОКИИ. Если получателем является работник АО «ЛЭСР», то в данной графе ставится прочерк.

В графе «**Срок действия договора**» указывается срок действия договора, заключенного между АО «ЛЭСР» и организацией получателя прав доступа к ОКИИ. Если получателем является работник АО «ЛЭСР», то в данной графе указывается один из видов трудового договора – Срочный или Бессрочный.

В графе «**Дата прохождения инструктажа**» указывается дата прохождения получателем инструктажа в департаменте информационной безопасности.

В графе «**Подпись прохождения инструктажа**» ставится подпись инструктируемого – получателя прав доступа к ОКИИ.

В графе «**Дата ознакомления с ОРД Общества по ИБ**» указывается дата ознакомления получателя инструктажа в департаменте информационной безопасности.

В графе «**Подпись ознакомления с ОРД Общества по ИБ**» ставится подпись инструктируемого – получателя прав доступа к ОКИИ.

№ п/п	Данные получателя прав доступа к ОКИИ				Договор		Прохождение инструктажа		Ознакомление с ОРД Общества по ИБ	
	Ф.И.О.	Организация	Контакты	Система обслуживания	Номер	Срок действия	Дата	Подпись	Дата	Подпись