Приложение к приказу

АО «ЛЭСР»
от «14» марта 2023 № 268

АКЦИОНЕРНОЕ ОБЩЕСТВО «ЛЕНЭНЕРГОСПЕЦРЕМОНТ»

ПРАВИЛА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АКЦИОНЕРНОГО ОБЩЕСТВА «ЛЕНЭНЕРГОСПЕЦРЕМОНТ»

Редакция 1

Санкт-Петербург
2023

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 26.072017 № 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 Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).
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 Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).
Общество	АО «ЛЭСР»
Подразделение ИБ	Подразделение, ответственное за планирование, организацию, реализацию и контроль мероприятий по обеспечению информационной безопасности.
Удостоверяющий центр	Подразделение, обеспечивающее создание, выдачу и обслуживание сертификатов электронной подписи.
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.
Многофункциональное устройство (МФУ)	Устройство, сочетающее в себе функции принтера, сканера, факсимильного устройства, копировального модуля.
BIOS, UEFI	Набор микропрограмм, реализующих интерфейс для работы с аппаратурой компьютера и подключенными к нему устройствами.

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
ПО	Программное обеспечение
Правила	Правила информационной безопасности АО «ЛЭСР»
Service Desk	Служба технической поддержки пользователей
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 критической информационной инфраструктуры, действия при возникновении компьютерных инцидентов и иных нештатных ситуаций Работников Общества, а также третьих лиц, получивших доступ к информации конфиденциального характера, объектам критической информационной инфраструктуры АО «ЛЭСР» на основании заключенных соглашений и договоров.

1.2. Корпоративный центр кибербезопасности

В ПАО «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 АО «ЛЭСР»;
- физические лица, с которыми Обществом заключены договоры гражданско-правового характера;
- физические лица, выполняющие действия в отношении информационной инфраструктуры, зданий и (или) сооружений Общества с размещенными объектами информационной инфраструктуры, включая проведение аудита, стажировок, уборки помещений;
- работники юридических лиц, выполняющих работы на объектах информационной инфраструктуры или в отношении объектов информационной инфраструктуры АО «ЛЭСР» в соответствии с условиями заключенных договоров, иных законных основаниях.

2.2. Объектами защиты в контексте обеспечения безопасности информационной инфраструктуры АО «ЛЭСР» и информации конфиденциального характера являются:

- 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;
- 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;
- 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;
- цифровые устройства и периферийное оборудование (в том числе принтеры, сканеры, ф-телефоны, цифровые камеры, смартфоны);
- сети электросвязи, используемые для организации взаимодействия объектов и передачи информации, места выхода в сеть Интернет;
- архитектура и конфигурация информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, 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 информационными системами, автоматизированными системами управления, информационно-телекоммуникационными сетями, включая их элементы (автоматизированные рабочие места, 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 критической информационной инфраструктуры и обрабатываемой информации конфиденциального характера, а также другие меры, не противоречащие действующему законодательству Российской Федерации.

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 критической информационной инфраструктуры (приложение к настоящим Правилам).

3. Правила работы с информацией конфиденциального характера

3.1. Информация, обрабатываемая в АО «ЛЭСР», делится на:

- общедоступная информация;
- публичная информация;
- служебная информация;
- информация ограниченного доступа;
- сведения конфиденциального характера;
- сведения, составляющие коммерческую тайну;
- персональные данные;
- информация, содержащая сведения, составляющие государственную тайну;
- иная информация, в отношении которой АО «ЛЭСР» принято решение о необходимости ее защиты.

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 АО «ЛЭСР».

3.3. Информация, обрабатываемая на объектах критической информационной инфраструктуры АО «ЛЭСР», относится к охраняемой компьютерной информации.

3.4. Информация в АО «ЛЭСР» обрабатывается в электронном виде и на бумажных носителях.

3.5. Порядок обработки информации конфиденциального характера определяется локальными нормативными актами (далее – ЛНА) и ОРД АО «ЛЭСР».

4. Правила безопасной работы на объектах критической информационной инфраструктуры

4.1. Пользователям запрещено:

1) осуществлять фотовидеофиксацию 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;

2) осуществлять скрытую аудио и/или видеозапись совещаний и переговоров;

3) выбрасывать информацию, содержащую конфиденциальные данные в печатном виде, в мусорные корзины (бумажные носители должны уничтожаться с применением устройств по измельчению бумаги — «шредер»);

4) 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);

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

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

7) осуществлять попытки самостоятельного внесения изменений в настройки операционных систем и параметров безопасности средств защиты информации, установленных на АРМ.

4.2. Работник обязан незамедлительно сообщать в подразделение ИБ по электронной почте **oib@lenenergo.ru** или телефону +7 (812) 595-87-88 вн. 5-87-88 информацию о следующих фактах:

- выявлении подозрительной активности на АРМ;
- выявлении вирусной активности;
- утрате носителей служебной информации и мобильных АРМ;
- 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, информационных систем и автоматизированных систем управления;
- обнаружении ошибок в настройке и работе информационных систем и автоматизированных систем управления, 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 АО «ЛЭСР».

5. Правила работы с учетными записями

5.1. В АО «ЛЭСР» 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 информационным системам, включая системы электронного документооборота, системы планирования и ведения финансово-хозяйственной деятельности, иным ресурсам, необходимым для выполнения производственных задач, предоставляется по заявке руководителя структурного подразделения в Service Desk посредством создания отдельной учетной записи (логина) и одноразового пароля.

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

5.5. Доступ к АРМ, корпоративному персонифицированному ящику электронной почты, сетевым папкам и сети Интернет для лиц, не являющихся работниками АО «ЛЭСР», предоставляется по заявке руководителя структурного подразделения Общества (куратора соглашения, договора) в Service Desk после согласования заявки с подразделением ИБ.

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

5.7. Все учетные записи должны быть персонифицированы, за исключением случаев, когда необходимость работы под обезличенной учетной записью обусловлена техническими требованиями информационной системы, автоматизированной системы управления или оборудования информационно-телекоммуникационной сети.

5.8. В случае необходимости использования одной учетной записи несколькими Пользователями, подразделением - владельцем информационной системы должен быть разработан и утвержден ОРД с перечнем лиц, допущенных к работе в информационной системе (автоматизированной системе управления, оборудования информационно-телекоммуникационной сети) под указанной учетной записью.

5.9. Учетные записи, неиспользовавшиеся более 45 рабочих дней, должны быть автоматически заблокированы.

5.10. В случае прекращения трудовых отношений с работником, а также при достижении целей, указанных в пункте 5.9 настоящих Правил, учетные записи, принадлежащие работнику, должны быть заблокированы.

5.11. Разблокирование учетных записей, сброс пароля на действующих учетных записях, предоставление доступа к учетной записи уволенного работника, иные действия с учетными записями осуществляются отделом информационно – программного обеспечения АО «ЛЭСР» по согласованию с заместителем генерального директора по безопасности АО «ЛЭСР» с обязательным информированием подразделения ИБ.

5.12. В случае применения механизмов двухфакторной аутентификации с использованием связанного с учетной записью телефонного номера номер, используемый для получения второго фактора, должен принадлежать работнику или быть закрепленным за работником (в случае использования корпоративных телефонных номеров АО «ЛЭСР»).

6. Правила работы с паролями

6.1. Пароль должен содержать (требования к сложности пароля):

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

6.2. Пароли не должны основываться на типовых шаблонах и идущих подряд на клавиатуре или в алфавите символов (qwerty, 1234567, abcdefgh и т.д.), а также не должны основываться на каком-либо одном

слове, выданном идентификаторе, имени, кличке, паспортных данных, номерах страховок.

6.3. Требования к длине пароля:

- для Пользователей с учетной записью «пользователь» длина пароля должна составлять не менее 8 символов;

- для Пользователей с учетной записью «администратор» (локального/доменного) длина пароля должна составлять не менее 15 символов;

- для «сервисных» идентификаторов, разделяемых ключей (shared keys) длина пароля должна составлять не менее 14 символов;

- для SNMP Community Strings длина пароля должна составлять не менее 10 символов.

6.4. Периодичность обязательной смены пароля:

1) административных учетных записей — каждые 60 дней;

2) пользовательских учетных записей — каждые 90 дней;

3) сервисных учетных записей — не реже двух раз в год;

4) shared keys SNMP Community Strings не реже одного раза в год.

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

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

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

6.8. При использовании паролей запрещено:

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

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

3) 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);

4) регистрировать третьих лиц под своим паролем;

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

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

7) использовать одни и те же пароли для разных информационных систем (автоматизированных систем управления, оборудования информационно-телекоммуникационной сети);

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

9) использовать функцию «Запомнить пароль» в программном обеспечении.

6.9. 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 АО «ЛЭСР».

7.3. В случае необходимости организации АРМ для лиц, не являющихся работниками Общества, АРМ создается по обращению руководителя структурного подразделения АО «ЛЭСР» после согласования с заместителем генерального директора по безопасности АО «ЛЭСР» при наличии положительного заключения (согласии) подразделения ИБ ПАО «Россети Ленэнерго».

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 ПАО «Россети Ленэнерго».

7.7. Удаленное подключение к АРМ допускается:

- в случаях, предусмотренных эксплуатационной или проектной документацией на эксплуатируемую систему;
- в случаях введения приказом по АО «ЛЭСР» удаленного режима работы, за исключением подключения к АРМ, входящим в состав автоматизированных систем управления, 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 информационным системам с использованием механизмов двухфакторной аутентификации посредством носителя и сертификата не допускается передача носителя и сертификата третьим лицам, в том числе родственникам или знакомым Пользователя, а также коллегам.

7.11. Организация удаленного подключения подрядных организаций к корпоративным АРМ осуществляется по согласованию с заместителем генерального директора по безопасности.

7.12. По окончании сеанса работы на АРМ или при необходимости оставления рабочего места Пользователь должен заблокировать экран средств вычислительной техники (блокирование экрана на персональном компьютере 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:

1) эксплуатировать средства вычислительной техники при отключенных или неустановленных средствах антивирусной защиты и встроенных в операционную систему средствах обеспечения безопасности (MS Windows Defender);

2) оставлять рабочее место без блокирования экрана средств вычислительной техники;

3) использовать АРМ в нерабочее время не по прямому назначению;

4) осуществлять работу на АРМ, не удовлетворяющих требованиям информационной безопасности;

5) допускать к работе на своем АРМ третьих лиц, за исключением работников службы технической поддержки, работников отдела информационно-программного обеспечения АО «ЛЭСР» и работников подразделения ИБ ПАО «Россети Ленэнерго»;

6) срывать пломбы или печати, вскрывать корпус персонального компьютера, осуществлять самостоятельную сборку и разборку средств вычислительной техники;

7) использовать уязвимости и недокументированные возможности установленного ПО;

8) вносить изменения в аппаратную и программную конфигурацию АРМ;

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

10) производить загрузку АРМ с внешних и сетевых носителей;

11) получать доступ к BIOS или UEFI персонального компьютера;

12) использовать АРМ с локальными учетными записями;

13) препятствовать работе средств защиты информации или обходить их;

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

- принтеры, сканеры и многофункциональные устройства;
- модемы и адаптеры связи;
- мобильные телефоны, планшеты и другие подобные устройства;
- личные носители информации;
- устройства двойного назначения скрывающие встроенный функционал;

15) использовать АРМ с одновременным подключением к ЛВС и другим сетям;

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

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

18) производить самостоятельное удаление/установку программного обеспечения на АРМ.

7.14. При увольнении работника информация на жестком диске персонального компьютера работника и сетевых ресурсах подлежит передаче непосредственному руководителю работника, после чего персональный компьютер и другие средства вычислительной техники, полученные работником, должны быть сданы в структурное подразделение, осуществляющее выдачу средств вычислительной техники.

7.15. При приемке АРМ уволенного работника должна быть выполнена процедура удаления всей 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 ПАО «Россети Ленэнерго».

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 несанкционированный 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 являющимися работниками Общества (в том числе с целью уборки помещений, выполнения работ по техническому обслуживанию, проведения аудита, прохождения стажировки и т.д.), предоставляется только по согласованию с заместителем генерального директора по безопасности Общества при обязательном присутствии работника АО «ЛЭСР», осуществляющего функции ИБ в Обществе, и/либо работника отдела информационно-программного обеспечения АО «ЛЭСР».

7.21. Доступ в помещения с АРМ, серверами, коммутационным оборудованием, осуществляющими обработку информации технологического характера (в том числе информации о значимых объектах критической информационной инфраструктуры), третьим лицам предоставляется только при непосредственном сопровождении работника АО «ЛЭСР», осуществляющего функции ИБ в Обществе, и/либо работника отдела информационно-программного обеспечения АО «ЛЭСР».

8. Правила работы с информационными системами

8.1. При работе с информационными системами (автоматизированными системами управления, оборудовании информационно-телекоммуникационной сети) запрещено:

1) использовать уязвимости и недокументированные возможности программного и аппаратного обеспечения;

2) использовать (в любых целях) ошибки системы;

3) осуществлять деструктивные воздействия на программное обеспечение и данные в информационных системах (автоматизированных системах управления);

4) несанкционированно изменять или уничтожать данные в информационных системах или на внешних (отчуждаемых) носителях;

5) несанкционированно устанавливать на автоматизированные рабочие места любые дополнительные программные и аппаратные компоненты и устройства;

6) осуществлять доступ под чужими учетными данными;

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

8) публиковать в открытом доступе информацию об архитектуре и конфигурации корпоративных и технологических информационно-телекоммуникационных сетей, 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 автоматизированными системами управления) 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 локальной вычислительной сети

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

9.2. Удаленный доступ к внутрикорпоративным web-сервисам и информационным системам, 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 удостоверяющим центром Общества.

9.3. К средствам вычислительной техники (персональный компьютер, ноутбук, планшет), с которых осуществляется удаленный доступ к информационным системам, 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 АО «ЛЭСР», 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 АО «ЛЭСР».

9.5. При работе в ЛВС без предварительного согласования с заместителем генерального директора по безопасности АО «ЛЭСР» не допускается:

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

2) осуществлять доступ к ЛВС с личных устройств;

3) осуществлять сетевой доступ к другим АРМ;

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

5) подключать АРМ к беспроводным сетям.

9.6. При работе в ЛВС запрещено:

1) подключать к ЛВС средства вычислительной техники с отключенными или неустановленными средствами зашиты, а также с настройками, неудовлетворяющими требованиям информационной безопасности;

2) проводить сканирование и анализ ЛВС и сетевых узлов;

3) осуществлять перехват трафика в ЛВС;

4) осуществлять атаки на АРМ, ЛВС, серверы, коммутационное и иное оборудование включая информационные системы и автоматизированные системы управления;

5) использовать уязвимости протоколов и конфигураций сетевого оборудования в ЛВС;

6) организовывать точки входа и шлюзы для внешних сетей;

7) создавать точки беспроводного доступа в административных помещениях и занимаемой территории АО «ЛЭСР».

10. Правила работы в сети Интернет

10.1. Доступ к ресурсам сети Интернет предоставляется работникам для выполнения ими трудовых функций.

10.2. Отдел информационно-программного обеспечения АО «ЛЭСР» через подразделение ИБ ПАО «Россети Ленэнерго» постоянно поддерживает в актуальном состоянии список запрещенных Интернет-ресурсов и блокирует доступ к ним на различных уровнях.

10.3. При работе в сети Интернет запрещено:

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

2) организовывать туннелирование внешних сетей;

3) переходить по баннерам и рекламным объявлениям;

4) переходить по подозрительным ссылкам;

5) использовать ресурсы:

- непристойного содержания;
- не связанных с исполнением трудовых функций работников;
- нарушающих требования действующего законодательства Российской Федерации;

6) распространять информацию, запрещенную действующим 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;

7) игнорировать системные сообщения АРМ и предупреждения об ошибках;

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

9) использовать внешние адреса электронной почты для ведения служебной переписки;

10) публиковать в сети Интернет корпоративные адреса электронной почты и телефонов работников АО «ЛЭСР»;

11) приобретать, хранить и распространять информацию, запрещенную законодательством РФ или способную причинить вред имиджу АО «ЛЭСР», или нанести материальный ущерб Обществу;

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

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

14) использовать ресурсы*:

- игрового и развлекательного характера;
- социальных сетей;
- пиринговых сетей;
- почтовых сервисов;
- файлообменных сервисов и облачных хранилищ, за исключением файлообменных сервисов ПАО «Россети» и ПАО «ФСК ЕЭС» (https://exflle.rosseti.ru/ и https://data.fsk-ees.ru) и 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 (Пот, 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 и др.);

*Для получения исключительного доступа в случае производственной необходимости необходимо сформировать в службу технической поддержки заявку на получение доступа с обоснованием необходимости использования данных сервисов и согласовать эту заявку с заместителем генерального директора по безопасности.

15) снижать установленный уровень защиты информации;

16) 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. Работник должен проверять вложения в сообщениях электронной почты на наличие исполняемых файлов (exe, bat, cmd, msi и другие), при их наличии — не запускать исполняемый файл и сообщить о получении такого письма в службу технической поддержки Service Desk. Рекомендуется открывать только вложения, имеющие следующий формат: документы (Word, Excel, PDF, txt и т.д.), изображения (JPG, PNG и т.д.).

11.4. Рекомендуется подтверждать отправку отправителем писем.

11.5. При работе с электронной почтой запрещено:

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

2) 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;

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

4) снижать установленный уровень защиты информации сообщений;

5) открывать письма, поступившие от неизвестных адресатов с неизвестными вложениями;

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

7) регистрировать учетные записи, профили на сторонних Интернет-ресурсах (включая социальные сети) с указанием корпоративного адреса электронной почты.

11.6. При получении массовой рассылки от подразделения ИБ ПАО «Россети Ленэнерго» или отдела информационно-программного обеспечения АО «ЛЭСР» о наличии информационных угроз на ресурсах Общества работники обязаны усилить бдительность к получаемой электронной почте.

11.7. При получении подозрительного письма работник должен:

1) при наличии 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;

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

3) сообщить в подразделение ИБ ПАО «Россети Ленэнерго» и/либо отдел информационно-программного обеспечения АО «ЛЭСР» о факте получения и открытия вложения подозрительного письма;

4) выполнить следующие действия при подтверждении, что данное письмо является SPAM рассылкой:

- нажать на данное письмо правой кнопкой мыши;
- выбрать пункт нежелательная почта;
- выбрать пункт заблокировать отправителя.

12. Правила работы с носителями информации

12.1. Использование внешних носителей информации «по умолчанию» допускается на АРМ руководителя в должности заместителя

начальника отдела и выше, а также на АРМ помощников руководителей структурных подразделений.

12.2. При необходимости использования внешнего носителя для записи (копирования) информации на АРМ работником должна быть направлена заявка в службу поддержки Service Desk с описанием причин такой необходимости.

12.3. Работники подразделения ИБ ПАО «Россети Ленэнерго» и/или отдела информационно-программного обеспечения АО «ЛЭСР» могут блокировать порты подключения внешних носителей информации в случаях нарушения Пользователем требований при работе с носителями информации, при угрозе распространения вредоносного программного обеспечения, 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 АО «ЛЭСР», осуществляющего обработку данной информации.

12.6. По достижении целей обработки информации (в том числе конфиденциальной) на носителе 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 **строго запрещено**:

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

2) подключать личные носители информации к АРМ;

3) использовать корпоративные носители информации АО «ЛЭСР» 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:

- усиленная квалифицированная электронная подпись;
- неквалифицированная электронная подпись.

13.2. Усиленная квалифицированная электронная подпись используется для:

- организации юридически значимого электронного документооборота;
- акцепта заявок на платеж в информационных системах АО «ЛЭСР» (АСУ Казначейство);
- дистанционного банковского обслуживания;
- организации подключения к ГИС;
- организации подключения к государственным порталам услуг;
- передачи отчетности по телекоммуникационным каналам связи;
- в иных случаях, предусмотренных действующим законодательством Российской Федерации и ОРД АО «ЛЭСР».

13.3. Неквалифицированная электронная подпись используется для:

- шифрования информации, в том числе сообщений электронной почты;
- организации доступа к информационным системам АО «ЛЭСР»;
- организации защищенного удаленного доступа;
- в иных случаях, предусмотренных ОРД Общества.

13.4. Выпуск сертификатов ключа проверки электронной подписи осуществляется в порядке, предусмотренным соответствующим ОРД АО «ЛЭСР».

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

1) извлечение закрытого ключа из контейнера;
2) передача носителя и (или) пароля на контейнер третьим лицам;
3) использование чужих носителей сертификата ключа проверки электронной подписи;
4) оставление носителя в АРМ по окончании сеанса работы с электронной подписью, за исключением случаев, когда постоянное присутствие носителя обусловлено требованиями информационной системы и/или эксплуатационной документацией на информационную систему.

13.6. При прекращении трудовых отношений с АО «ЛЭСР», работник должен сдать имеющиеся у него носители сертификата ключа проверки электронной подписи в подразделение ИБ с уведомлением заместителя генерального директора по безопасности АО «ЛЭСР».

14. Правила работы с системами дистанционного банковского обслуживания

14.1. Доступ к АРМ, на котором установлены системы ДБО, предоставляется только уполномоченным соответствующим ОРД работникам АО «ЛЭСР».

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 ЭП 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 АО «ЛЭСР» настоящих Правил осуществляется заместителем генерального директора по безопасности АО «ЛЭСР» при непосредственном участии отдела информационно-

программного обеспечения Общества и подразделения ИБ ПАО «Россети Ленэнерго».

15.2. Подразделением ИБ ПАО «Россети Ленэнерго» должны применяться автоматизированные и автоматические средства для контроля и предотвращения утечки информации на АРМ Пользователей и в ЛВС, контроля доступа к информационным системам (включая удаленный доступ), а также противодействия компьютерным атакам на информационные активы АО «ЛЭСР».

15.3. С целью контроля и противодействия попыткам несанкционированного доступа к конфиденциальной информации и информационным системам, в том числе автоматизированным системам управления, оборудования информационно-телекоммуникационной сети, работники подразделения ИБ ПАО «Россети Ленэнерго» по согласованию с заместителем генерального директора АО «ЛЭСР» могут:

1) привлекать сотрудников охранного предприятия в случае оказания противодействия со стороны нарушителей;

2) блокировать без предупреждения с обязательным уведомлением по электронной почте в службу технической поддержки доступ Пользователя к:

- ЛВС,
- АРМ;
- сети Интернет;
- ИТС;
- информационным системам;

3) приостанавливать действие сертификата ключа проверки электронной подписи Пользователя;

4) В случае выявления фактов нарушений настоящих Правил направить информацию в АО «ЛЭСР» и инициировать проведение служебной проверки, в рамках которой с согласия руководителя АО «ЛЭСР» в соответствии со ст. 193 ТК РФ истребовать от Пользователя предоставления объяснения;

5) требовать от Пользователя прекращения работы с АРМ через непосредственного руководителя Пользователя;

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

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

8) получать доступ к информации, обрабатываемой на АРМ Пользователя и сетевых ресурсах, в том числе сетевых папках структурных

подразделений АО «ЛЭСР» без уведомления Пользователя и (или) руководителя структурного подразделения — владельца сетевого ресурса;

9) осуществлять изъятие средств вычислительной техники и носителей информации, числящихся за Пользователем и принадлежащих АО «ЛЭСР».

15.4. В целях совершенствования мер по обеспечению информационной безопасности работники отдела информационно-программного обеспечения АО «ЛЭСР» с участием подразделения ИБ ПАО «Россети Ленэнерго» должны постоянно тестировать действие технических средств защиты информации, направленных на выявление угроз и блокирование несанкционированного доступа к конфиденциальной информации.

15.5. Работники отдела информационно-программного обеспечения АО «ЛЭСР» и подразделения ИБ ПАО «Россети Ленэнерго», в случае выявления действий противоречащих действующему законодательству Российской Федерации в области обеспечения информационной безопасности, должны фиксировать их, первоочередно ставить в известность руководство АО «ЛЭСР», по согласованию с генеральным директором АО «ЛЭСР» уведомлять правоохранительные органы и оказывать им всестороннее содействие в рамках своей компетенции при возбуждении административных и уголовных дел по фактам выявленных правонарушений.

16. Ответственность

16.1. Работники АО «ЛЭСР» несут персональную ответственность за соблюдение настоящих Правил.

16.2. По представлению отдела информационно-программного обеспечения АО «ЛЭСР» или подразделения ИБ ПАО «Россети Ленэнерго» на имя заместителя генерального директора по безопасности АО «ЛЭСР» к работнику могут быть применены дисциплинарные взыскания в порядке, установленном действующим законодательством Российской Федерации.

16.3. При принятии решения о привлечении работника АО «ЛЭСР» к дисциплинарной ответственности в соответствии со ст. 192 ТК РФ должна учитываться тяжесть совершенного проступка и обстоятельства, при которых проступок был совершен.