Акционерное общество «Россети»

**Политика информационной безопасности**

АО «Россети»

г. Москва

2023 г.

**СОДЕРЖАНИЕ**

[**1.Обозначения и сокращения** 3](#_Toc156551893)

[**2.ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ** 3](#_Toc156551894)

[**3.ОБЛАСТЬ ПРИМЕНЕНИЯ** 3](#_Toc156551895)

[**4. НОРМАТИВНЫЕ ССЫЛКИ** 4](#_Toc156551896)

[**5.Общие положения** 4](#_Toc156551897)

[**6. ПОЛОЖЕНИЯ ПО ИНФОРМАЦИННОЙ БЕЗОПАСНОСТИ** 4](#_Toc156551898)

[**7. ЗАДАЧИ СИСТЕМЫ УПРАВЛЕНИЯ ИБ** 5](#_Toc156551899)

[**8. РЕАЛИЗАЦИЯ** 6](#_Toc156551900)

[**8.1 Структура и ответственность** 6](#_Toc156551901)

[**8.2 Осведомленность и информирование** 6](#_Toc156551902)

[**8.3 Реагирование на инциденты безопасности** 6](#_Toc156551903)

[**9. КОНТРОЛЬ** 7](#_Toc156551904)

[**10. СОВЕРШЕНСТВОВАНИЕ** 7](#_Toc156551905)

[**ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ** 8](#_Toc156551906)

[**Положение об Организации парольной защиты** 11](#_Toc156551907)

[2.1. **Назначение и область действия** 11](#_Toc156551908)

[2.2. **Основные требования** 11](#_Toc156551909)

[**3 Роли и ответственность** 13](#_Toc156551910)

# **1.Обозначения и сокращения**

В настоящем документе использованы следующие сокращения:

|  |  |  |
| --- | --- | --- |
| **ИБ** | - | Информационная безопасность |
| **ИС** | - | Информационная система |
| **СУИБ** | - | Система управления информационной безопасностью |

# **2.ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

Термины и определения, используемые в настоящей Политике и рекомендуемые к использованию в нормативных и организационно- распорядительных документах, созданных на ее основе, приведены в Приложении № 1 «Термины и определения».

# **3.ОБЛАСТЬ ПРИМЕНЕНИЯ**

* 1. Настоящая Политика информационной безопасности (далее – «Политика») предназначена для сотрудников АО «Россети» (далее – «Организация»), обеспечивающих безопасность информации организации, сотрудников и клиентов. Находящийся под эксплуатацией и управлением ЦОД.
  2. Система обеспечения ИБ представляет собой совокупность технических, нормативно-правовых и организационных мер для защиты интересов Организации в информационной сфере.
  3. Система управления ИБ является составной частью общей системы управления Организации, обеспечивает поддержку и управление процессами обеспечения ИБ на всех этапах деятельности корпоративной информационной системы.
  4. Организация разрабатывает и внедряет систему управления ИБ, отвечающую требованиям и рекомендациям нормативных документов Российской Федерации.
  5. Основные цели внедрения системы управления ИБ Организации:
     1. Защита конфиденциальных ресурсов.
     2. Оценка защищенности ИС
     3. Оценка соответствия ИС требованиям данной политики
     4. Анализ существующих уязвимостей
     5. Защита целостности информации для обеспечения требуемого качества работ.
     6. Повышение осведомленности работников Организации о рисках и повышение их квалификации.
  6. Положения настоящей Политики распространяются на все виды информации в Организации, хранящейся либо передающейся любыми способами, в том числе информацию, зафиксированную на материальных носителях.
  7. Политика распространяются на средства приема, обработки, передачи, хранения и защиты информации Организации.
  8. Область применения настоящей Политики распространяется на все подразделения Организации, в которых обрабатывается информация, не составляющая государственную тайну.

# **4. НОРМАТИВНЫЕ ССЫЛКИ**

При разработке настоящей Политики учтены требования и рекомендации следующих документов:

* Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
* Документ ФСТЭК России от 11.02.2014 г. «Меры защиты информации в государственных информационных системах».
* ГОСТ Р 50922-2006. Защита информации. Основные термины и определения
* ГОСТ Р ИСО/МЭК 27001–2021 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности».
* ГОСТ Р ИСО/МЭК 27002-2021. Информационные технологии. методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности
* Федеральный закон от 7 июля 2003 г. №126-ФЗ

# **5.Общие положения**

Целью настоящей политики является обеспечение безопасности объектов, ресурсов и иного имущества Организации от всех видов угроз, как внешних, так и внутренних, умышленных и непреднамеренных. Минимизация и локализация ущерба от потенциальных угроз безопасности.

Обеспечение безопасности данных клиентов и партнеров Организации, минимизация возможности утечки и последующей компрометации информации.

# **6. ПОЛОЖЕНИЯ ПО ИНФОРМАЦИННОЙ БЕЗОПАСНОСТИ**

1. Положения по информационной безопасности Организации (далее –«Положения») разрабатываются на основании Политики информационной безопасности Организации в целях создания, развития и совершенствования общей системы защиты информации Организации.
2. Положения по ИБ являются приложениями к настоящей Политике.
3. Принятие новых Положений, а также пересмотр или отмена действующих Положений оформляется документально и утверждается приказом директора Организации.
4. Актуализация Положений осуществляется при изменении законодательной или нормативной базы в области ИБ, а также при изменении внутренней ситуации в Организации.
5. Правила пользования ресурсами сети Интернет в Организации указаны в «Положении об использовании сети интернет» (Приложение №…).
6. Правила по организации антивирусной защиты информации «Положении о защите по средству использования средств антивирусной защиты» (Приложение №…).
7. Меры по физической защите оборудования и данных предпринимаются в соответствии с «Положением о физической защите информационных ресурсов» (Приложение №…).
8. Меры по обеспечению безопасности предпринимаются в соответствии с положением «Положение по организации парольной защиты» (Приложение №2).

# **7. ЗАДАЧИ СИСТЕМЫ УПРАВЛЕНИЯ ИБ**

1. Основной целью управления ИБ является защита интересов Организации по средству обеспечения целостности, конфиденциальности и доступности информации располагающей Организацией.
2. Основными задачами управления ИБ являются:
   1. Сбор данных и последующий анализ текущего состояния информационной безопасности в Организации;
   2. Выбор средств и мер для обеспечения ИБ;
   3. Внедрение средств ИБ;
   4. Контроль выполнения правил ИБ;
   5. Документальное подтверждение мер предупреждения ИБ.
   6. В основе управления ИБ Организации лежит подход, отраженный в модели деятельности в виде циклического процесса «планирование – реализация – контроль – совершенствование» (по ГОСТ Р ИСО/МЭК 27001-2021).
   7. Организация осуществляет деятельность по управлению рисками, повышению осведомленности сотрудников и реагированию на инциденты в области ИБ. Регулярно, не реже одного раза в два года, производится анализ состояния рисков, связанных с ИБ. Защитные меры должны основываться на всесторонней оценке этих рисков и должны быть им соразмерны.
   8. Всю ответственность за защиту своей информации и информационных ресурсов Организация возлагает на руководителей отделов и на весь штат сотрудников отделов обеспечивающих защиту информации в Организации.

# **8. РЕАЛИЗАЦИЯ**

Реализация системы управления ИБ осуществляется на основе четкого распределения ролей и ответственности в области информационной безопасности.

## **8.1 Структура и ответственность**

* + 1. Ответственное лицо, назначенное приказом директора Организации, руководит работами по внедрению и совершенствованию СУИБ, в том числе организует выполнение Положений по ИБ.
    2. Руководитель отдела ИБ несет ответственность за контроль выполнения начальниками отделов мер обеспечения ИБ в Организации.
    3. Сотрудники отдела ИБ несут ответственность за контроль выполнения мер обеспечения ИБ, в том числе расследуя и устраняя по средствам других отделов потенциальных инцидентов ИБ.
    4. Руководители отделов Организации ведут и контролируют соблюдение мер и правил проведения ИБ в организации своими подчиненными.
    5. Сотрудники отделов ведут личный контроль и ответственность за выполнение и соблюдение мер и правил ИБ в Организации.

## **8.2 Осведомленность и информирование**

1. Осведомленность и информирование сотрудников Организации осуществляется по средствам электронного документооборота.
2. Осведомленность и информирование сотрудников Организации осуществляется по средствам бумажного документооборота
3. Осведомленность и информирование сотрудников Организации осуществляется по средствам бумажного документооборота
4. При устройстве на работу и допуском к взаимодействию с защищенной информацией руководство подразделений должно провести новому сотруднику ознакомление с положениями о ИБ.

## **8.3 Реагирование на инциденты безопасности**

* + 1. Для определения возможных сценариев восстановления информационной системы Организации в чрезвычайных ситуациях, конкретизации технических средств и действий работников и структурных подразделений по локализации инцидентов ИБ должны быть разработаны планы восстановительных работ для важных информационных ресурсов.
    2. Реагирование на инциденты ИБ осуществляется в соответствии с «Положением о реагировании на инциденты информационной безопасности» (Приложение № ).

# **9. КОНТРОЛЬ**

* 1. Контроль соблюдения требований настоящей Политики возлагается на ответственное лицо, назначенное приказом директора Организации.
  2. При отсутствии главного ответственного лица, контроль соблюдения требований передается нижестоящему лицу, вплоть, но начальства другого подразделения Организации.
  3. Контроль за актуальностью Политики осуществляет ответственное лицо, назначенное приказом директора Организации.
  4. Контроль ИБ проводится в форме мониторинга ИБ, который выполняется в соответствии с «Положением о мониторинге событий информационной безопасности» (Приложение №…).

# **10. СОВЕРШЕНСТВОВАНИЕ**

* произвести мониторинг эффективности процессов СУИБ
* в ситуациях, требующих оперативного реагирования, работа ведется согласно «Положению о реагировании на инциденты ИБ».
* управление записями СУИБ;
* анализ рисков информационной безопасности;
* внутренние документы подразделений Организации не должны противоречить Концепции ИБ, Политике ИБ и иным документам по информационной безопасности, утвержденным приказом по Организации.
* Разработка и внедрение нормативных и организационно-распорядительных документов по информационной безопасности проводится поэтапно.

Приложение № 1

к Политике информационной безопасности

АО «Россети»

# **ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

**Аудит информационной безопасности** — систематический, независимый и документируемый процесс получения свидетельств деятельности по обеспечению информационной безопасности и установлению степени выполнения критериев информационной безопасности, а также допускающий возможность формирования профессионального аудиторского суждения о состоянии информационной безопасности организации (ГОСТ Р 53114-2008).

**Безопасность информационной технологии** — Состояние защищенности информационной технологии, при котором обеспечиваются безопасность информации, для обработки которой она применяется, и информационная безопасность информационной системы, в которой она реализована (ГОСТ Р 53114-2008).

**Блокирование доступа (к информации)** — Прекращение или затруднение доступа к информации лиц, имеющих на это право (законных пользователей) (ГОСТ Р 53114 2008).

**Защита информации** — Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. (ГОСТ Р 50922-2006)

**Информационная безопасность организации** — Состояние защищенности интересов организации в условиях угроз в информационной сфере (ГОСТ Р 53114-2008)

**Доступность информации** — Состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно (ГОСТ Р 50922-2006).

**Информационная инфраструктура** — совокупность объектов информатизации, обеспечивающая доступ потребителей к информационным ресурсам (по ГОСТ Р 53114-2008).

**Информационная система** — Система, предназначенная для хранения, обработки, поиска, распространения, передачи и предоставления информации (ГОСТ 7.0-99)

**Информационные технологии** — процессы и методы создания, поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

**Инцидент информационной безопасности** — любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность (ГОСТ Р 53114-2008).

**Конфиденциальность информации** — Свойство информации, которое обеспечивает ее защиту от несанкционированного доступа и использования (ГОСТ Р 50922-2006).

**Меры обеспечения ИБ** — совокупность действий, направленных на разработку и/или практическое применение способов и средств обеспечения информационной безопасности (ГОСТ Р ИСО/МЭК 27002-2021).

**Мониторинг ИБ** — Процесс постоянного наблюдения и анализа результатов регистрации событий безопасности и иных данных с целью выявления (ГОСТ Р 59547-2021)

**Несанкционированный доступ** — Доступ к информации или к ресурсам автоматизированной информационной системы, осуществляемый с нарушением установленных прав и (или) правил доступа (ГОСТ Р 53114-2008).

**Носитель информации** — физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин (ГОСТ Р 50922-2006).

**Обеспечение ИБ** — деятельность, направленная на устранение (нейтрализацию, парирование) внутренних и внешних угроз информационной безопасности Организации или на минимизацию ущерба от возможной реализации таких угроз (ГОСТ Р 53114-2008).

**Обработка информации** — Систематическое выполнение операций над данными, представляющими предназначенную для обработки информацию (ГОСТ 15971-90)

**Объект защиты информации** — информация либо носитель информации, или информационный процесс, которую (который) необходимо защищать в соответствии с целью защиты информации (ГОСТ Р 53114-2008).

**Политика безопасности (информации в организации)** — Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности (ГОСТ Р 50922-2006).

**Оценка риска** — процесс, объединяющий идентификацию риска, анализ риска и их количественную оценку (ГОСТ Р 53114-2008).

**Система управления информационной безопасностью (СУИБ)** — часть общей системы управления Организацией, основанная на использовании методов оценки рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности (по ГОСТ Р 53114-2008).

**Пользователь информационной системы** — лицо, участвующее в функционировании информационной системы либо использующее результаты ее функционирования (ГОСТ 7.0-99).

**Распространение информации** — Процесс предоставления информации, имеющейся в информационно-поисковых системах, потребителям информации (ГОСТ 7.73-96).

**Риск** — сочетание вероятности события и его последствий (ГОСТ Р ИСО/МЭК 27002-2012).

**Техническая защита информации** — Защита информации, заключающаяся в обеспечении не криптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств (ГОСТ Р 50922-2006).

**Физическая защита информации** — Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты (ГОСТ Р 50922-2006).

**Целостность информации** — Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право (ГОСТ Р 50922-2006).

Приложение № 2 к Политике   
информационной безопасности   
АО «Россети»

# **Положение об Организации парольной защиты**

# **Назначение и область действия**

* 1. Настоящее Положение о доступе к информационным ресурсам (далее – «Положение») определяет основные правила и требования по обеспечению информационной безопасности информационных ресурсов АО «Россети» (далее – «Организация») процессов смены, прекращения действия и генерации паролей.
  2. При наличии технической возможности контроль за соответствием паролей требованиям настоящим положением осуществляется автоматически техническими средствами автоматизированных систем, а при отсутствии такой возможности контроль осуществляется сотрудниками отдела информационной безопасности и администраторами информационных систем Организации.
  3. Соответствует требованиям Политики информационной безопасности Организации.
  4. Распространяется на всех работников Организации и третьих лиц, использующих информационные ресурсы и системы Организации. Является обязательным для исполнения.

# **Основные требования**

* 1. Для создания учетной записи нового пользователя начальник структурного подразделения или лицо, его замещающее, создаёт запрос на отел информационной безопасности и администраторов информационных систем.
  2. С целью ограничения доступа к информационным ресурсам устанавливаются следующие категории паролей:
* пароли администраторов информационных систем, средств (модулей) доверенной загрузки (программно-аппаратный комплекс «Соболь» и др.), ППО, баз данных, на сетевую/доменную или локальную (используемую в автономных СВТ, неподключенных к сети ЗКВС или ИК) учетную запись;

– пользовательские пароли на сетевую/доменную или локальную учетную запись, на вход в ППО (если предусмотрено технической документацией), пароль (пин-код) на ключевой носитель (ключ электронной подписи);

* пароль на вход и осуществление настроек в BIOS/UEFI.

1. К паролям предъявляются следующие требования
2. Пароль на вход и осуществление настроек в BIOS/UEFI генерируется и устанавливается подразделением АО «Россети», осуществляющим администрирование учетной записи (домена), не сообщается пользователям и должен иметь длину не менее 8 символов.
3. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-x позициях, новый пароль не должен повторять ни одного из шести предыдущих, при этом при наличии технической возможности, контроль этого требования должен проводиться автоматически.
4. После восьми попыток подряд неверного ввода пароля система должна автоматически блокировать сетевую/доменную или локальную учетную запись пользователя.
5. Установка пароля в программно-аппаратный комплекс «Соболь» возможна в режиме администратора или пользователя в соответствии с имеющейся документацией на программно-аппаратный комплекс. В обоих случаях пароль должен соответствовать требованиям, предъявляемым к пользовательским паролям.
6. Запрещается настраивать программно-аппаратный комплекс «Соболь» на мягкий режим работы контроля целостности.
7. В случае обладания значительным количеством парольной информации допускается хранение паролей на учтённом съёмном носителе, хранящемся в сейфе, ключ от которого находится в пенале, опечатанном личной металлической печатью. В таких случаях рекомендуется шифровать парольную информацию специализированным программным обеспечением, имеющим сертификацию Федеральной службы по техническому и экспортному контролю России.
8. Пароли представляют собой конфиденциальную информацию пользователя. Во время ввода пароля пользователь обязан исключить возможность его просматривания другими лицами или техническими средствами (видеокамерами и др.).
9. Временный пароль пользователь обязан сменить на основной при первом входе в систему.
10. Восстановленный (временный) пароль на сетевую/доменную или локальную учетную запись пользователя генерируется и устанавливается структурным подразделением ФКУ «ЦОКР», осуществляющим администрирование учётной записи (домена). Работник такого структурного подразделения создает временный пароль следующим способом:

* в ViPNet Password Generator выполняется генерация пароля с помощью парольной фразы, после чего работник структурного подразделения, осуществляющего администрирование учетной записи (домена), по внутренней телефонной связи озвучивает парольную фразу работнику

1. Временный и основной пароли должны иметь:

* минимальную длину пароля — 8 символов;
* срок действия пароля — не более 90 дней учётной записи оборудования, и не более 30 дней для доменной учётной записи;
* сложность пароля — буквенно-цифровой (в числе символов пароля должны присутствовать латинские буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, \*, % и т.п.).

1. Пароли на ключевой носитель для администратора устанавливает отдел защиты информации, пароль для пользователя устанавливает сам пользователь в соответствии с требованиями настоящей инструкции при первичном получении ключевого носителя.
2. Категорически запрещается использовать в паролях типовые, легко вычисляемые комбинации букв, слов, чисел (имена, фамилии, общепринятые сокращения и т.д.).
3. При выборе основного пароля запрещается использовать:

* личные данные, например: имена и даты рождения, клички домашних животных, номера автомобилей, телефонов и другие пароли которые можно угадать, основываясь на информации о пользователе;

–комбинации символов, набираемых в закономерном порядке на клавиатуре (12345678 и т.п.).

1. В случае утери, компрометации, несанкционированном изменении пароля пользователь обязан незамедлительно сообщать об этом работникам структурного подразделения ФКУ «ЦОКР», отвечающего за обеспечение информационной безопасности и выполнить внеплановую смену пароля.
2. Запрещается использование одних и тех же учётных данных (логин, пароль) в разных доменах.

# **3 Роли и ответственность**

* 1. Ответственность за соблюдение данного Положения возлагается на всех работников Организации и третьих лиц, использующих информационные ресурсы и системы Организации.
  2. Ответственность за реализацию данного Положения возлагается на: руководителей подразделений Организации; работников, ответственных за администрирование сегментов информационной телекоммуникационной системы Организации; работников, выполняющих следующие функции: администраторов информационных систем, администраторов локальной вычислительной сети, администраторов по обеспечению безопасности информации.