|  |
| --- |
| РОСЭНЕРГОАТОМ |
| **Политика информационной безопасности**  РОСЭНЕРГОАТОМ |
|  |
| 2024 г. |

# СОДЕРЖАНИЕ

1. [ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ](#_gjdgxs)
2. [ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ](#_30j0zll)
3. [ОБЛАСТЬ ПРИМЕНЕНИЯ](#_1fob9te)
4. [НОРМАТИВНЫЕ ССЫЛКИ](#_3znysh7)
5. [ОБЩИЕ ПОЛОЖЕНИЯ](#_2et92p0)
6. [ПОЛОЖЕНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ](#_tyjcwt)
7. [ЗАДАЧИ СИСТЕМЫ УПРАВЛЕНИЯ ИБ](#_3dy6vkm)
8. [РЕАЛИЗАЦИЯ](#_1t3h5sf)
9. [КОНТРОЛЬ](#_4d34og8)
10. [СОВЕРШЕНСТВОВАНИЕ](#_2s8eyo1)

Приложение № 1 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Приложение № 2 ПОЛОЖЕНИЕ О ДОСТУПЕ К ИНФОРМАЦИОННЫМ РЕСУРСАМ

# ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящем документе использованы следующие сокращения:

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

# 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».

# ОБЛАСТЬ ПРИМЕНЕНИЯ

* 1. Настоящая Политика информационной безопасности (далее – «Политика») предназначена для специалистов по обеспечению безопасности информации, руководителей, организующих и проводящих работы по обработке подлежащей защите информации
  2. Система обеспечения ИБ представляет собой совокупность нормативно-правовых, организационных, технических мер по обеспечению защищенности
  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:

-оценка текущего уровня защищённости ИС

-выявление и локализация уязвимостей в системе защиты ИС

-анализ рисков, связанных с возможностью осуществления угроз безопасности

-оценка соответствия ИС требованиям настоящей Политики

-выработка рекомендаций по совершенствованию СУИБ за счёт внедрения новых мер защиты информации

– повышение осведомленности сотрудников

* 1. Положения настоящей Политики распространяются на все виды информации в Организации, хранящейся либо передающейся любыми способами, в том числе информацию, зафиксированную на материальных носителях.
  2. Положения настоящей Политики также распространяются на средства приема, обработки, передачи, хранения и защиты информации Организации.
  3. Политика применяется
  4. Область применения настоящей Политики распространяется на все подразделения Организации, в которых обрабатывается информация, не составляющая государственную тайну.

# 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»;

– Федеральный закон от 29.07.2004 г. №98-ФЗ «О коммерческой тайне»;

– ГОСТ Р ИСО/МЭК 27001–2021 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности».

# ОБЩИЕ ПОЛОЖЕНИЯ

Целью настоящей Политики является обеспечение безопасности объектов защиты Организации от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

# ПОЛОЖЕНИЯ ПО ИНФОРМАЦИОННОЙ 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.

Меры по обеспечению безопасности предпринимаются в соответствии с положением «Положение по организации парольной защиты» (Приложение №2)

* + 1. Принятие новых Положений, а также пересмотр или отмена действующих Положений оформляется документально и утверждается приказом директора Организации.
    2. Актуализация Положений осуществляется при изменении законодательной или нормативной базы в области ИБ, а также при изменении внутренней ситуации в Организации.

# ЗАДАЧИ СИСТЕМЫ УПРАВЛЕНИЯ ИБ

* 1. Основной целью управления ИБ является обеспечение необходимого уровня доступности, целостности и конфиденциальности компонентов
  2. Основными задачами управления ИБ являются:

— осознание степени необходимости защиты информации и постановку задач;

— сбор и анализ данных о состоянии информационной безопасности в организации;

— оценку информационных рисков;

— планирование мер по обработке рисков;

— реализацию и внедрение соответствующих механизмов контроля, распределение ролей и ответственности

—обучение и мотивацию персонала, оперативную работу по осуществлению защитных мероприятий;

— мониторинг функционирования механизмов контроля, оценку их эффективности и соответствующие корректирующие воздействия

* 1. 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.
  2. Всю ответственность за защиту своей информации и информационных ресурсов Организация возлагает на отдел информационной безопасности

# РЕАЛИЗАЦИЯ

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

# 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. Руководители отделов являются ответственными за руководство всеми видами деятельности по управлению ИБ в структурных подразделениях.
    3. Руководители подразделений отделов являются ответственными за функции администраторов по ИБ.

# Осведомленность и информирование

Доведение правил ИБ до работников проводится при приеме на работу, в ходе производственных совещаний, собраний, профессиональной подготовки персонала.

# 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 № 8).

# КОНТРОЛЬ

9.1. Контроль соблюдения требований настоящей Политики возлагается

на ответственное лицо, назначенное приказом директора организации. При необходимости контролирующие функции выполняют также третьи лица и организации, действующие на законных основаниях.

9.2. Контроль за актуальностью Политики осуществляет ответственное

лицо, назначенное приказом директора организации.

9.3. Контроль в области информационной безопасности является частью

работ по обеспечению ИБ Организации. Целью контроля ИБ является выявление угроз, предотвращение их реализации, минимизация возможного ущерба.

# СОВЕРШЕНСТВОВАНИЕ

-анализ рисков информационной безопасности;

-внутренние аудиты в области информационной безопасности;

-управление корректирующими/предупреждающими действиями;

-мониторинг эффективности процессов СУИБ;

-анализ функционирования СУИБ со стороны руководства;

-управление инцидентами информационной безопасности;

-управление непрерывностью бизнеса;

-организация обучения и осведомленности в области ИБ персонала;

-управление документацией СУИБ;

-управление записями СУИБ.

-обследование, обнаружение и анализ степени соответствия требованиям стандарта ISO/IEC 27001:2005.

-создание СУИБ (разработка процессов) в соответствии с требованиями стандарта ISO/IEC 27001:2005.

-внедрение процессов СУИБ и подготовка СУИБ к сертификации.

-сертификация СУИБ10 (при необходимости подтверждения качества системы).

Приложение № 1 к Политике информационной безопасности РОСЭНЕРГОАТОМ

# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**Автоматизированная система** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

**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).

**Аутентификация пользователя** – подтверждение того, что пользователь соответствует заявленному.

**Безопасность информации (данных)** – Состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность (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 информации (данных)** – временное прекращение сбора, систематизации, накопления, использования, распространения информации, в том числе ее передачи.

**Владелец информационного ресурса** – работник или структурное подразделение Института, распоряжающийся информационным ресурсом, в том числе определяющий порядок доступа и его использования.

**Вредоносная программа** – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационных систем.

**Доступ к информации (данным)** – возможность получения и использования информации (данных).

**Защищаемая информация (защищаемые данные)** – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

**Идентификация** – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов (ГОСТ Р 53114-2008).

**Идентификация риска** – процесс обнаружения, распознавания и описания рисков (ГОСТ Р 53114-2008).

**Информационная безопасность** –защищенность информационных систем (информации и обрабатывающей еѐ инфраструктуры) от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или инфраструктуре (согласно Концепции ИБ Института).

Приложение № 2 к Политике информационной безопасности “ РОСЭНЕРГОАТОМ ”

# ПОЛОЖЕНИЕ ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ

1. **Общие положения**

1.1. Положение регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей.

1.2. Положение является дополнением к действующим нормативным документам по вопросам защиты информации и не исключает обязательного выполнения их требований.

1.3. При наличии технической возможности контроль за соответствием паролей требованиям настоящей положения осуществляется автоматически техническими средствами автоматизированных систем, а при отсутствии такой возможности контроль осуществляется отдел защиты информации.

1.4. Положение обязательны для выполнения всем пользователями и распространяются на все структурные подразделения.

1.5. Пользователи должны быть ознакомлены с положение

1.6. Пользователи несут ответственность за исполнение требований.

1.7. Контроль за выполнением требований возлагается на отдел защиты информации.

1.8. Контроль за выполнением требований положения возлагается на лиц, ответственных в соответствии с приказами.

1. **Установка и изменение паролей**

2.1. Для создания учетной записи нового пользователя начальник структурного подразделения или лицо, его замещающее, создаёт запрос.

2.2. С целью ограничения доступа к информационным ресурсам устанавливаются следующие категории паролей:

– пароль на вход и осуществление настроек в BIOS/UEFI;

– пароли администраторов информационных систем, средств доверенной загрузки, баз данных, на сетевую/доменную или локальную учетную запись;

– пользовательские пароли на сетевую/доменную или локальную учетную запись, пароль на ключ электронной подписи.

2.3. К паролям предъявляются следующие требования.

2.3.1. Пароль на вход и осуществление настроек в BIOS/UEFI генерируется и устанавливается подразделением, осуществляющим администрирование учетной записи, не сообщается пользователям и должен иметь длину не менее 8 символов (цифры и/или специальные символы).

2.3.2. Первичный пароль на сетевую/доменную или локальную учетную запись пользователь составляет самостоятельно, используя данные, полученные от начальника структурного подразделения.

Временный пароль пользователь обязан сменить на основной пароль при первом входе в систему.

Восстановленный (временный) пароль на сетевую/доменную или локальную учетную запись пользователя генерируется и устанавливается структурным подразделением, осуществляющим администрирование учётной записи.

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.).

2.3.3. Пин-код (пароль) на ключевой носитель (ключ электронной подписи) должен быть длиной не менее 8 символов.

2.3.4. 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.

2.4. Категорически запрещается использовать в паролях типовые, легко вычисляемые комбинации букв, слов, чисел (имена, фамилии, общепринятые сокращения и т.д.).

2.5. 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.).

2.6. Ввод пароля должен осуществляться с учетом регистров и языка ввода на котором он задан.

2.7. После восьми попыток подряд неверного ввода пароля система должна автоматически блокировать сетевую/доменную или локальную учетную запись пользователя. Повторный ввод пароля возможен после разблокировки не ранее чем через 60 минут.

2.8. Для генерации пароля возможно использование специальной утилиты генерации паролей.

2.9. 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.

2.10. Внеплановая смена пароля может производиться по инициативе пользователя.

2.11. В случае утери, компрометации, несанкционированном изменении пароля пользователь обязан незамедлительно сообщать об этом работникам структурного подразделения, отвечающего за обеспечение информационной безопасности и выполнить внеплановую смену пароля.

2.12. Пароли представляют собой конфиденциальную информацию пользователя. Во время ввода пароля пользователь обязан исключить возможность его просматривания другими лицами или техническими средствами (видеокамерами и др.).

2.13. Запрещается сообщать кому-либо и разглашать пароли, работать с использованием чужих учетных записей и паролей, подбирать пароли других пользователей и собирать о них информацию.

2.14. Запрещается хранить пароли на жестких дисках СВТ (HDD, SSD) и съемных носителях, в том числе с использованием специализированного программного обеспечения, а также на рабочем месте в открытом виде.

2.15. 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.

2.16. Запрещается использовать обезличенную электронную почту без согласования с отдела защиты информации.

# 2.17. Запрещается использование одних и тех же учётных данных (логин, пароль) в разных доменах.