|  |
| --- |
| ГК Астра |
| **Политика информационной безопасности**  ГК Астра |
|  |
| г. Москва  2023 г. |

**Содержание**

[1. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ 3](#_Toc153820112)

[2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 3](#_Toc153820113)

[3. ОБЛАСТЬ ПРИМЕНЕНИЯ 3](#_Toc153820114)

[4. НОРМАТИВНЫЕ ССЫЛКИ 4](#_Toc153820115)

[5. ОБЩИЕ ПОЛОЖЕНИЯ 4](#_Toc153820116)

[6. ПОЛОЖЕНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 5](#_Toc153820117)

[7. ЗАДАЧИ СИСТЕМЫ УПРАВЛЕНИЯ ИБ 5](#_Toc153820118)

[8. РЕАЛИЗАЦИЯ 5](#_Toc153820119)

[8.1. Структура и ответственность 6](#_Toc153820120)

[8.2. Осведомленность и информирование 6](#_Toc153820121)

[8.3. Реагирование на инциденты безопасности 6](#_Toc153820122)

[9. КОНТРОЛЬ 6](#_Toc153820123)

[10. СОВЕРШЕНСТВОВАНИЕ 6](#_Toc153820124)

[Приложение № 1 8](#_Toc153820125)

[Приложение № 2 14](#_Toc153820126)

# 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 предназначена для установления единых норм, правил и требований к системе управления информационной безопасностью ГК Астра.
  2. Система обеспечения ИБ представляет собой совокупность нормативно-правовых, организационных, технических мер по обеспечению защищенности интересов ГК Астра в информационной сфере, а также субъектов информационных отношений.
  3. Система управления ИБ является составной частью общей системы управления ГК Астра, 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:
* Защита конфиденциальности информационных ресурсов ограниченного доступа;
* Обеспечение непрерывного авторизованного доступа к информационным ресурсам ГК Астра для поддержки основной деятельности;
* Защита целостности существенной информации для обеспечения требуемого качества работ и эффективности процесса принятий решений;
* Установление четкой ответственности за управление и использование информационных ресурсов ГК Астра;
* Повышение осведомленности работников ГК Астра и их понимания рисков, связанных с информационными ресурсами ГК Астра, повышение их квалификации в области информационной безопасности.
  1. Положения настоящей Политики распространяются на все виды информации в ГК Астра, 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 ГК Астра.
  3. Политика применяется ко всем работникам ГК Астра, а также к любой третьей стороне, включая лиц, работающих по договорам гражданско- правового характера и прикомандированных работников, имеющих доступ к информационным ресурсам ГК Астра. Агенты и представители, осуществляющие деятельность от имени ГК Астра, а также партнеры и клиенты ГК Астра, консультанты и советники, подрядчики и поставщики – все обязаны соблюдать требования настоящей Политики.
  4. Область применения настоящей Политики распространяется на все подразделения ГК Астра, в которых обрабатывается информация, не составляющая государственную тайну.

# НОРМАТИВНЫЕ ССЫЛКИ

При разработке настоящей Политики учтены требования и рекомендации следующих документов:

* Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) "Об утверждении Перечня сведений конфиденциального характера";
* Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ
* Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ;
* Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ;
* ГОСТ Р 53114-2008 "Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения";
* ГОСТ Р ИСО/МЭК 27001-2021 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования".

# ОБЩИЕ ПОЛОЖЕНИЯ

5.1. Необходимость разработки политики информационной безопасности обусловлена необходимостью обеспечения защиты информационных ресурсов ГК Астра, а также необходимостью анализа потенциальных угроз, рисков, которые они несут организации и определение мер противодействия им;

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

5.3. Разработка политики информационной безопасности инициирует проверку надежности существующей системы защиты ИС, что позволит более тщательно определить перечень средств и методов ИБ, которые требуются для обеспечения информационной безопасности ГК Астра.

# ПОЛОЖЕНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

* + 1. Положения по информационной безопасности ГК Астра (далее –«Положения») разрабатываются на основании Политики информационной безопасности ГК Астра в целях создания, развития и совершенствования общей системы защиты информации ГК Астра.
    2. Положения по ИБ являются приложениями к настоящей Политике.
    3. Правила использования паролей определены в «Положении об использовании паролей» (Приложение №2).
    4. Принятие новых Положений, а также пересмотр или отмена действующих Положений оформляется документально и утверждается приказом директора ГК Астра.
    5. Актуализация Положений осуществляется при изменении законодательной или нормативной базы в области ИБ, а также при изменении внутренней ситуации в ГК Астра.

# ЗАДАЧИ СИСТЕМЫ УПРАВЛЕНИЯ ИБ

* 1. Основной целью управления ИБ является защита интересов ГК Астра и его работников в области информационной безопасности
  2. Основными задачами управления ИБ являются:
* Мониторинг состояния информационной безопасности ГК Астра;
* Выбор и внедрение мер обеспечения информационной безопасности, соответствующих целям и задачам ГК Астра;
* Документальное подтверждение предупреждающих и корректирующих мер обеспечения информационной безопасности.
  1. В основе управления ИБ ГК Астра лежит подход, отраженный в модели деятельности в виде циклического процесса «планирование – реализация – контроль – совершенствование» (по ГОСТ Р ИСО/МЭК 27001-2021).
  2. ГК Астра 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.
  3. Всю ответственность за защиту своей информации и информационных ресурсов ГК Астра возлагает на руководителей структурных подразделений.

# 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 ГК Астра, 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.
    4. На каждого сотрудника возложена ответственность по выполнению требований и правил 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 ГК Астра 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».

# КОНТРОЛЬ

9.1 Контроль соблюдения требований настоящей Политики возлагается на ответственное лицо, назначенное приказом директора ГК Астра. 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 ГК Астра.

9.3 Контроль в области информационной безопасности является частью работ по обеспечению ИБ ГК Астра. Целью контроля ИБ является выявление угроз, предотвращение их реализации, минимизация возможного ущерба.

9.4 Объектами контроля ИБ являются информационные ресурсы ГК Астра (информация, работники и другие субъекты доступа, системы и средства информационных технологий, а также средства защиты информации).

# СОВЕРШЕНСТВОВАНИЕ

Для совершенствования системы управления ИБ в ГК Астра выполняется систематический анализ и оценивание действующей ситуации в области информационной безопасности.

Анализ ИБ осуществляется на основе данных мониторинга в соответствии с «Положением о мониторинге событий ИБ».

Нормативные и организационно-распорядительные документы по информационной безопасности утверждаются приказом ГК Астра и рассылаются руководителям подразделений.

# Приложение № 1

к Политике информационной безопасности

ГК Астра

**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** – 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.

**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** – состояние защищенности интересов организации в условиях угроз в информационной сфере. (ГОСТ Р 53114-2008).

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

**Информационные ресурсы** – документы и массивы документов, содержащиеся в информационных системах (библиотеках, архивах, фондах, банках данных, информационных системах других видов).

**Информационная система** – система, представляющая собой совокупность информации, а также информационных технологий и технических средств, позволяющих осуществлять обработку информации с использованием средств автоматизации или без использования таких средств.

**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 (по ГОСТ Р 53114-2008).

**Источник угрозы безопасности –** субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

**Конфиденциальная информация –** документированная информация, доступ к которой ограничивается в соответствии с законодательством. К конфиденциальным относятся сведения:

а) о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные);

б) составляющие тайну следствия и судопроизводства;

в) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с ГК РФ и федеральными законами (служебная тайна);

г) связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.д.);

д) связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с ГК РФ и федеральными законами (коммерческая тайна);

е) о сущности изобретения, исследования, разработки, модели или промышленного образца до официальной публикации информации о них.

**Управление ИБ –**– скоординированные действия по руководству и управлению ГК Астра в части обеспечения его информационной безопасности в соответствии с изменяющимися условиями внутренней и внешней среды ГК Астра (по ГОСТ Р 53114-2008).

**Управление рисками ИБ** – скоординированные действия по руководству и управлению ГК Астра в отношении рисков ИБ с целью их минимизации (по ГОСТ Р 53114-2008).

**Меры обеспечения ИБ** совокупность действий, направленных на разработку и/или практическое применение способов и средств обеспечения информационной безопасности.

**Мониторинг ИБ** – Непрерывное наблюдение за состоянием и поведением объектов ИБ с целью их контроля, оценки и прогноза в рамках управления ИБ.

**Нарушитель ИБ** – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при её обработке техническими средствами в информационных системах.

**Несанкционированный доступ (несанкционированные действия)** – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами.

**Носитель информации (данных)** – 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.

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

**Обработка информации (данных)** – действия (операции) с информацией, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), блокирование, уничтожение информации.

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

**Объект информатизации** – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены (ГОСТ Р 53114-2008).

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

**Политика** – общее намерение и направление, официально выраженное руководством (ГОСТ Р ИСО/МЭК 27002-2012).

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

**Система обеспечения информационной безопасности** – совокупность нормативно-правовых, организационных и технических мер по обеспечению защищенности интересов Института в информационной сфере, а также субъектов информационных отношений.

**Пользователь информационной системы** – лицо, участвующее в функционировании информационной системы либо использующее результаты ее функционирования.

**Правила разграничения доступа** – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

**Ресурс информационной системы** – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

**Риск** – сочетание вероятности события и его последствий (ГОСТ Р ИСО/МЭК 27002-2012). Применительно к ИБ, риск – сочетание вероятности нанесения ущерба и тяжести этого ущерба.

**Средства вычислительной техники** – совокупность программных и технических элементов систем обработки информации, способных функционировать самостоятельно или в составе других систем.

**Субъект доступа** – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

**Система защиты информации (данных)** – совокупность организационных и технических мероприятий для защиты информации от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий с ней.

**Угрозы безопасности информации (данных)** – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к информации, результатом которого может стать её уничтожение, изменение, блокирование, копирование, распространение, а также иных несанкционированных действий при её обработке в информационных системах.

**Уязвимость** – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

# Приложение № 2

к Политике информационной безопасности

ГК Астра

**ПОЛОЖЕНИЕ**

**ОБ ИСПОЛЬЗОВАНИИ ПАРОЛЕЙ**

1. **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 Сколковский институт науки и технологий (далее – «ГК Астра») от угроз, связанных с некорректным использованием средств аутентификации.
   2. Соответствует требованиям Политики информационной безопасности ГК Астра.
   3. Распространяется на всех работников ГК Астра и третьих лиц, использующих информационные ресурсы и системы ГК Астра Является обязательным для исполнения.
2. **Основные требования**
   1. Пользовательские пароли (для доступа к электронной почте, сети, компьютеру и т.д.) должны содержать не менее шести буквенно-цифровых символов (буквы латинского алфавита, цифры).
   2. Административные пароли (административных учетных записей операционных систем, телекоммуникационного оборудования, баз данных, информационных систем и т.д.) должны содержать не менее восьми буквенноцифровых символов и спецсимволов, если они поддерживаются программным обеспечением (буквы латинского алфавита в верхнем и нижнем регистре, цифры и специальные символы типа ! @ # $ % ^ & \* \_ = ).
   3. Для простоты запоминания могут быть использованы парольные фразы, разделенные спецсимволами и цифрами.
   4. Пароль не должен совпадать с логином пользователя (наименованием учетной записи) и содержать легко угадываемые слова и числа (имена, даты рождения, номера документов и т.п.).
   5. Пользователи лично ответственны за выбор пароля, отвечающего заданным критериям сложности, и за его хранение, исключающее ознакомление с ним третьих лиц.
   6. Запрещается передача паролей третьим лицам.
   7. Запрещается запись и хранение паролей в местах, где они могут быть легко доступны и прочитаны.
   8. Все пользовательские пароли должны заменяться не реже одного раза в год. Рекомендованный интервал – шесть месяцев.
   9. Все административные пароли должны заменяться не реже одного раза в полгода. Рекомендованный интервал – три месяца.
   10. Запрещается отправлять пароли в сообщениях электронной почты, SMS или через другие формы электронного обмена информацией, кроме специально оговоренных случаев (одноразовые пароли с ограниченным сроком действия; пароли, создаваемые самим пользователем при помощи средств электронного обмена информацией и т.п.).
   11. Доступ к общедоступным страницам веб-сайтов Института не требует парольной защиты.
   12. В случае компрометации пароля (утраты, хищения и т.п.), пользователь должен немедленно сменить пароль. Если пользователь не имеет возможности самостоятельно сменить пароль, администратор заменяет его пароль новым паролем, который сообщает пользователю.
   13. Учетные записи пользователей, чьи пароли не соответствуют требованиям настоящего Положения, могут быть заблокированы ответственными лицами (см. раздел 3.2).
3. **Роли и ответственность**
   1. Ответственность за соблюдение данного Положения возлагается на всех работников ГК Астра и третьих лиц, использующих информационные ресурсы и системы ГК Астра.
   2. Ответственность за реализацию данного Положения возлагается на: руководителей подразделений ГК Астра; работников, ответственных за администрирование сегментов информационной телекоммуникационной системы ГК Астра; работников, выполняющих следующие функции: администраторов информационных систем, администраторов локальной вычислительной сети, администраторов по обеспечению безопасности информации.