ООО «Регард»

Политика информационной безопасности

ООО «Регард»

г. Москва
2023 г.

СОДЕРЖАНИЕ

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

3.1. Настоящая Политика информационной безопасности (далее – «Политика») предназначена для обеспечения информационной безопасности в ООО «Регард» (далее «Организация»), а также для установления норм и требований к системе управления информационной безопасностью.

3.2. Система обеспечения ИБ представляет собой совокупность организационных и технических мер по обеспечению защиты информации в Организации.

3.3. Система управления ИБ является составной частью общей системы управления Организации, обеспечивает поддержку и управление процессами обеспечения ИБ на всех этапах деятельности корпоративной информационной системы.

3.4. Организация разрабатывает и внедряет систему управления ИБ, отвечающую требованиям и рекомендациям нормативных документов Российской Федерации.

3.5. Основные цели внедрения системы управления ИБ Организации:

– повышение осведомленности сотрудников Организации в отношении обращения с информацией внутри Организации, а также повышение квалификации в области информационной безопасности;

– выявление, оценка и прогнозирование угроз ИБ;

– совершенствование нормативно-правовой базы обеспечения ИБ.

3.6. Положения настоящей Политики распространяются на все виды информации в Организации, хранящейся либо передающейся любыми способами, в том числе информацию, зафиксированную на материальных носителях.

3.7. Положения настоящей Политики также распространяются на средства приема, обработки, передачи, хранения и защиты информации Организации.

3.8. Политика применяется ко всем сотрудникам, связанными с Организацией трудовым договорим.

3.9. 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»;

– 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».

5. ОБЩИЕ ПОЛОЖЕНИЯ

Информация является важным ресурсом. Обеспечение безопасности имеет стратегическое значение для достижения целей и задач Организации. Для достижения основных целей информационной безопасности необходимо своевременно и полностью предоставлять сотрудникам информацию, необходимую для выполнения их служебных обязанностей.

Разработка и реализация Политики информационной безопасности необходимы для обеспечения согласованной и эффективной системы управления информационной безопасностью в Организации. Положения настоящей Политики ИБ являются обязательными для всех работников Организации.

6. ПОЛОЖЕНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1.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.

6.2.Положения по ИБ являются приложениями к настоящей Политике.

Меры по физической защите оборудования и данных предпринимаются в соответствии с «Положением о физической защите информационных ресурсов» (Приложение №3).

6.3.Принятие новых Положений, а также пересмотр или отмена действующих Положений оформляется документально и утверждается приказом директора Организации.

6.4.Актуализация Положений осуществляется при изменении законодательной или нормативной базы в области ИБ, а также при изменении внутренней ситуации в Организации.

7. ЗАДАЧИ СИСТЕМЫ УПРАВЛЕНИЯ ИБ

7.1. Основной целью управления ИБ является защита интересов Организации и его работников в области информационной безопасности.

7.2. Основными задачами управления ИБ являются:

– выбор и внедрение мер обеспечения ИБ, адекватных целям и задачам деятельности Организации;

– анализ состояния ИБ Организации;

– контроль выполнения правил ИБ.

7.3. 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).

7.4. 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.

7.5. Всю ответственность за защиту своей информации и информационных ресурсов Организация возлагает на руководителей структурных подразделений.

8. РЕАЛИЗАЦИЯ

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

8.1. Структура и ответственность

8.1.1. Ответственное лицо, назначенное приказом директора Организации, руководит работами по внедрению и совершенствованию СУИБ, в том числе организует выполнение Положений по ИБ.

8.1.2. Руководители отделов являются ответственными за руководство всеми видами деятельности по управлению ИБ в структурных подразделениях.

8.1.3. Руководители подразделений отделов являются ответственными за функции администраторов по ИБ.

8.1.4. На каждого сотрудника возложена ответственность по выполнению требований и правил ИБ.

8.2. Осведомленность и информирование

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

8.3. Реагирование на инциденты безопасности

8.3.1. 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.

8.3.2. Реагирование на инциденты ИБ осуществляется в соответствии с «Положением о реагировании на инциденты информационной безопасности» (Приложение № 8).

9. КОНТРОЛЬ

Объектом контроля является информация, оборудование и средства защиты Организации. Контроль над соблюдением Политики, а также за ее актуальностью возлагается на ответственное лицо, назначенное приказом директора Организации.

10. СОВЕРШЕНСТВОВАНИЕ

Для совершенствования системы управления ИБ в Организации 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 по Организации и рассылаются руководителям подразделений.

Приложение № 1
к Политике информационной безопасности
ООО «Регард»

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.

Защищаемая информация (защищаемые данные) – защита конфиденциальности, целостности и доступности информации.

Информационная безопасность – сохранение конфиденциальности, целостности и доступности информации (ИСО/МЭК 27000).

Меры обеспечения ИБ – совокупность действий, направленных на разработку и/или практическое изменение способов и средств обеспечения информационной безопасности (по ГОСТ Р 53114-2008).

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 ее 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 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 доступа – единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Приложение № 2
к Политике информационной безопасности
ООО «Регард»

ПОЛОЖЕНИЕ
ОБ ИСПОЛЬЗОВАНИИ ПАРОЛЕЙ

1. Назначение и область действия

1.1. Настоящее Положение о доступе к информационным ресурсам (далее – «Положение») определяет основные правила и требования по обеспечению информационной безопасности информационных ресурсов ООО «Регард» (далее – «Организация») от угроз, связанных с некорректным использованием средств аутентификации.

1.2. Соответствует требованиям Политики информационной безопасности Организации.

1.3. Распространяется на всех работников Организации и третьих лиц, использующих информационные ресурсы и системы Организации. Является обязательным для исполнения.

2. Основные требования

2.1. Пользовательские пароли (для доступа к электронной почте, сети, компьютеру и т.д.) должны содержать не менее шести буквенно-цифровых символов (буквы латинского алфавита, цифры).

2.2. 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 ! @ # $ % ^ & * _ =).

2.3. Для простоты запоминания могут быть использованы парольные фразы, разделенные спецсимволами и цифрами.

2.4. 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.).

2.5. Пользователи лично ответственны за выбор пароля, отвечающего заданным критериям сложности, и за его хранение, исключающее ознакомление с ним третьих лиц.

2.6. Запрещается передача паролей третьим лицам.

2.7. Запрещается запись и хранение паролей в местах, где они могут быть легко доступны и прочитаны.

2.8. Все пользовательские пароли должны заменяться не реже одного раза в год. Рекомендованный интервал – шесть месяцев.

2.9. Все административные пароли должны заменяться не реже одного раза в полгода. Рекомендованный интервал – три месяца.

2.10. 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.).

2.11. Доступ к общедоступным страницам веб-сайтов Института не требует парольной защиты.

2.12. 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.

2.13. Учетные записи пользователей, чьи пароли не соответствуют требованиям настоящего Положения, могут быть заблокированы ответственными лицами (см. раздел 3.2).

3. Роли и ответственность

3.1. Ответственность за соблюдение данного Положения возлагается на всех работников Организации и третьих лиц, использующих информационные ресурсы и системы Организации.

3.2. 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.