ООО “АТОМОРС”

Политика информационной безопасности

ООО “АТОМОРС”

г. _____

20__ 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 определения и установления основных требований обеспечения ИБ в деятельности ООО «АТОМОРС» (далее – «Организации»).

3.2. Система обеспечения информационной безопасности представляет собой совокупность задач и мероприятий, направленных на защиту интересов Организации в сфере информационных технологий и информационной среды, через применение нормативных, законодательных и технических средств для защиты информации

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:

– гарантировать конфиденциальность, целостность и доступность информации, с тем чтобы предотвратить утечки данных, искажение информации и недоступность критически важных ресурсов.

– обеспечить соблюдение всех применимых законодательных и регуляторных требований в области информационной безопасности, включая законы о защите данных и стандарты безопасности.

– идентифицировать и снизить риски, связанные с потенциальными угрозами и уязвимостями информационной инфраструктуры, с целью предотвращения инцидентов безопасности.

– разрабатывать и реализовывать долгосрочную стратегию информационной безопасности с целью обеспечить стабильную защиту в будущем.

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 для всех сотрудников Организации

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 РФ О персональных данных от 27.07.2006 № 152-ФЗ

– Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ

- Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ

- ГОСТ Р ИСО 9001-2015

5. ОБЩИЕ ПОЛОЖЕНИЯ

5.1 Настоящая политика разработана для реализации требований п.7.1.3. ГОСТ Р ИСО 9001-2015, а также требований, изложенных в законодательстве РФ и нормах права в части обеспечения ИБ, в том числе ПДн, требований нормативных актов федерального органа исполнительной власти, уполномоченного в области безопасности, федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации.

5.2 Настоящая политика является общедоступным документом и представляет собой официально принятую руководством Общества систему взглядов на проблему обеспечения ИБ и устанавливает принципы построения системы управления ИБ на основе систематизированного изложения целей, задач и мероприятий в области ИБ Общества.

5.3 Руководство и персонал Общества принимают на себя обязательства обеспечить реализацию политики обеспечения безопасности информационных ресурсов АО «Промышленные инновации».

5.4 Финансирование работ по защите информации и выполнению требований по ИБ осуществляется в рамках бюджета службы директора по ИТ

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.

6.3. Правила использования и работы с токенами определены в «Положении об использовании и работы с токенами»(Приложение 2)

6.4.Правила использования паролей определены в «Положении об использовании паролей» (Приложение 2)

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

6.6.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 обеспечение сохранности, доступности и целостности информации, а также защита информационных ресурсов и систем Организации от угроз и рисков, с тем чтобы предотвратить инциденты безопасности и обеспечить непрерывность бизнес-процессов.

7.2. Основными задачами управления ИБ являются:

– Определение потенциальных угроз и уязвимостей в информационных системах и данных Организации, а также оценка вероятности и возможных последствий инцидентов безопасности.

– Разработка долгосрочных и краткосрочных стратегий, целей и приоритетов для обеспечения информационной безопасности, а также определение необходимых ресурсов.

– Проведение обучения и повышение осведомленности сотрудников в области ИБ, чтобы снизить риск человеческого фактора в угрозах безопасности.

– Обеспечение соответствия законодательным и регуляторным требованиям в области информационной безопасности.

– Оценка эффективности мер по управлению ИБ и регулярная проверка соответствия установленным целям и стандартам

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 директора дивизиона информационной безопасности, руководителей структурных подразделений дивизиона информационной безопасности.

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. Руководство всеми видами деятельности по управлению ИБ в структурных подразделениях подлежат руководителям этих подразделения.

8.1.3. Функции администраторов ИБ подлежат на штатных сотрудников отдела ИБ

8.1.4. Ответственность работников за надлежащее выполнение требований и правил ИБ определена в внутреннем регламенте Организации. Работники и сотрудники несут ответственность за обеспечение требований ИБ в своих подразделений

8.2. Осведомленность и информирование

Сотрудники организации должны подписать освидетельствование о осведомлении политике безопасности, соблюдать требования. В рамках повышения осведомленности и развитии служебных навыков необходимы мероприятия по повышению осведомленности в вопросах ИБ.

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 №).

9. КОНТРОЛЬ

9.1 Контроль за актуальностью Политики осуществляет ответственное лицо, назначенное руководителем Дивизиона ИБ Организации

9.2 Контроль соблюдения требований Политики возглагается на ответственное лицо, назначенное руководителем Дивизиона ИБ Организации

9.3 Объектами контроля ИБ являются информационные ресурсы Организации.

10. СОВЕРШЕНСТВОВАНИЕ

10.1 В рамках совершенствования Организации необходимо проведение оценки текущего состояние СУИБ и рисков ИБ, установление целей и приоритетов для совершенствования СУИБ

10.2 В рамках совершенствования Организации необходимо проводить анализ угроз и уязвимостей, идентификация необходимых мероприятий.

10.3 Необходимо установление постоянного мониторинга состояния ИБ в организации, планирование и разработка плана реагирования на инциденты ИБ

10.4 Необходима регулярная оценка эффективности мероприятий по предотвращению инцидентов и реагирование на них

10.5 Необходима разработка стратегии ИБ, включая долгосрочные цели и приоритеты, определение бюджета и ресурсов, необходимых для реализации стратегии.

10.6 Необходим ыбор и внедрение технических средств и решений, соответствующих целям совершенствования СУИБ.