ООО "ЦИФРОВАЯ НЕЗАВИСИМОСТЬ"

# Политика информационной безопасности

ООО "ЦИФРОВАЯ НЕЗАВИСИМОСТЬ"

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 определения основных требований обеспечения информационной безопасности в деятельности ООО "ЦИФРОВАЯ НЕЗАВИСИМОСТЬ" (далее – «Организация»).

3.2. Система обеспечения ИБ представляет собой совокупность целей и задач, обеспечивающих защиту интересов Организации в информационном пространстве, посредством применения нормативно-правовых, Организационных, технических мер 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:

3.5.1. Защита конфиденциальности информации, обрабатываемой в Организации, а также создаваемых в Организации продуктов программного обеспечения;

3.5.2. Защита целостности и аутентичности информации хранящейся, обрабатываемой, и создаваемой в Организации, как и передаваемой по каналам связи;

3.5.3. Доступность хранящейся и обрабатываемой информации сотрудникам, обладающим достаточным уровнем допуска;

3.5.4. Введение четкой и обоснованной системы контроля и мер по обеспечению защищенности интересов Организации.

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, также любых третьих лиц, получивших доступ к источникам информации 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 от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Методический документ ФСТЭК России от 11.02.2014 г. «Меры защиты информации в государственных информационных системах».

ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

РС БР ИББС-2.2-2009 «Методика оценки рисков нарушения информационной безопасности».

Методический документ «Методика оценки угроз безопасности информации» (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.)

## 5. ОБЩИЕ ПОЛОЖЕНИЯ

Разработка и реализация политики информационной безопасности являются необходимыми для Организации, по нескольким причинам:

- В деятельности такой Организации образуются массивы информации, подлежащей охране. Через Организацию ежедневно проходит большое количество информации, содержащей коммерческую тайну и персональные данные сотрудников. В процессе работы Организации создается новое программное обеспечение и механические устройства, подлежащие патенту. Особенности выпускаемой продукции требуют защиты.
- Политика необходима для того, чтобы донести до руководящего состава Организации цели и задачи информационной безопасности. Организация должна понимать, что отдел информационной безопасности это не

только инструмент для расследования фактов утечек данных, но и помощник в минимизации рисков Организации, в повышении её продуктивности.

- Разработка политики безопасности должна предоставлять сводку действенных инструментов и правил, согласно которым сотрудники компании могут оценить важность вверенной им информации и использовать ее в собственных интересах и интересах Организации. При этом риск навредить основной деятельности Организации должен оставаться минимальным.

## 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 паролей определены в «Положении об использовании паролей» (Приложение № 2).

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

6.5.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 эффективности процессов и деятельности Организации, а также минимизация рисков кибербезопасности.

7.2. Основными задачами управления ИБ являются:

7.2.1. Обеспечение конфиденциальности, целостности и доступности информации.

7.2.2. Выявление и анализ рисков информационной безопасности.

7.2.3. Обучение сотрудников правилам безопасного использования информации и технологий.

7.2.4. Постоянное совершенствование системы управления информационной безопасностью.

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 заведующих научными лабораториями.

## 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 Организации осуществляют руководители этих подразделений. Они же несут ответственность за выполнение обязательств Положений по ИБ.

8.1.3. Функции администраторов по ИБ возлагаются на штатных сотрудников отдела ИБ, которые осуществляет свою деятельность во взаимодействии с другими подразделениями Организации. Координацию их деятельности по защите информации осуществляет ответственное лицо, назначенное приказом директора Организации.

8.1.4. Ответственность работников за надлежащее выполнение требований и правил ИБ определена в положениях, правилах, регламентах и других внутренних документах Организации. Руководители структурных подразделений Организации несут ответственность за обеспечение выполнения требований ИБ в своих подразделениях. Работники Организации несут персональную ответственность за соблюдение требований информационной безопасности.

### 8.2. Осведомленность и информирование

Сотрудники Организации должны быть осведомлены о политике информационной безопасности и ее требованиях. Для этого необходимо периодически проводить мероприятия по повышению осведомленности сотрудников в вопросах информационной безопасности. Ответственность за проведение, качество проведения и периодичность лежит на руководителях подразделений.

Список мероприятий:

- Тренинг по вопросам информационной безопасности;
- Разработка и распространение информационных материалов, посвященных вопросам ИБ;
- Проведение регулярных внутренних проверок на соответствие требованиям 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.

## 9. КОНТРОЛЬ

9.1. Контроль соблюдения требований 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.

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

## 10. СОВЕРШЕНСТВОВАНИЕ

10.1. Для совершенствования системы управления ИБ необходимо выполнять следующие действия:

- Анализ рисков. Необходимо провести анализ рисков, связанных с безопасностью информационных ресурсов Организации.
- Постоянный мониторинг и анализ событий, связанных с безопасностью информации. Необходимо постоянно мониторить и анализировать события, связанные с безопасностью информации, для выявления уязвимостей и предотвращения инцидентов.
- Реагирование на инциденты. Необходимо дорабатывать регламент реагирования на инциденты информационной безопасности, определяющий порядок действий при возникновении инцидентов.
- Разработка политик и процедур СУИБ. На основе результатов анализа рисков и мониторинга необходимо разработать новые и доработать имеющиеся политики и процедуры СУИБ.
- Внедрение новых политик и процедур СУИБ в эксплуатацию. После разработки политик и процедур СУИБ необходимо внедрить их в эксплуатацию.

10.2. Порядок мониторинга информационной безопасности. Мониторинг информационной безопасности проводится с целью выявления несанкционированных действий работников и авторизованных третьих лиц в корпоративной информационной системе Организации, оперативного реагирования на инциденты информационной безопасности, сбора данных и проведения служебных расследований.

Для целей мониторинга информационной безопасности используются специализированные средства и штатные (входящие в состав информационных систем) средства контроля доступа, регистрации событий и синхронизации времени.

Необходимо получать своевременную информацию о технических уязвимостях используемых информационных систем, оценивать опасность таких уязвимостей и принимать соответствующие меры для рассмотрения связанного с ними риска.

Проверка журналов аудита и анализ данных по инцидентам информационной безопасности проводятся на регулярной основе.

10.3. Порядок реагирования на инциденты ИБ. Все пользователи информационных систем и ресурсов Организации должны сообщать о любых замеченных или подозреваемых недостатках безопасности в системах или услугах так оперативно, насколько это возможно. Пользователи должны знать способы информирования об известных или предполагаемых случаях нарушения информационной безопасности с использованием телефонной связи, электронной почты и других методов. Все инциденты ИБ должны быть идентифицированы, зафиксированы, доведены до соответствующих служб и решены (минимизированы негативные последствия).

10.4. Обобщенные результаты анализа ИБ представляются на встрече директора Организации и начальника отдела ИБ с целью их оценки и выработки согласованных рекомендаций, направленных на формирование и реализацию корректирующих и превентивных действий по совершенствованию системы управления ИБ Организации. Рекомендации, принятые на встрече, заносятся в протокол, который утверждается участвующими сторонами.

10.5. Все нормативные и организационно-распорядительные документы по информационной безопасности могут быть приняты, отменены и пересмотрены отдельными приказами по Организации, а также уточнены и дополнены распоряжениями по отдельному структурному подразделению.

10.6. Внутренние документы подразделений Организации не должны противоречить Концепции ИБ, Политике ИБ и иным документам по информационной безопасности, утвержденным приказом по Организации. При наличии расхождений и противоречий между документами по информационной безопасности, утвержденными приказами по Организации, и внутренними документами подразделений Организации – все документы, утвержденные приказами по Организации, имеют преимущественную силу.