

УТВЕРЖДЕНА
Приказом АО «Содружество»
от «11» 04 2024 № 145

**ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
АО «СОДРУЖЕСТВО»**

СОДЕРЖАНИЕ

- 1. Общие положения**
- 2. Описание объекта защиты**
- 3. Цели политики**
- 4. Содержание политики**
- 5. Ответственность в сфере информационной безопасности**
- 6. Контроль за соблюдением положений Политики**

1. Общие положения

1.1 Настоящая политика информационной безопасности (далее - Политика) утверждается генеральным директором АО «Содружество» и определяет мероприятия, процедуры и правила по защите информации в информационных системах АО «Содружество».

1.2 Положения настоящей Политики распространяются на информационные системы АО «Содружество».

1.3 Положения настоящей Политики обязательны к исполнению для всех пользователей информационных систем в АО «Содружество» (далее - Пользователи), а также для администраторов безопасности и системных администраторов (далее - Администраторы).

1.4 В соответствии с указом Президента Российской Федерации № 188 от 6 марта 1997 года к сведениям конфиденциального характера (защищаемой информации) в АО «Содружество» относятся:

- сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;
- сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

2. Описание объекта защиты

Основными объектами защиты системы информационной безопасности является:

- информационные ресурсы, содержащие коммерческую тайну, персональные данные физических лиц, сведения ограниченного распространения, а также открыто распространяемая информация, необходимая для работы, независимо от формы и вида представления;
- работники АО «Содружество», являющиеся разработчиками и пользователями информационных систем АО «Содружество»;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

3. Цели политики

Политика представляет собой систематизированное изложение целей и задач защиты, основных принципов построения системы информационной безопасности, требований к организационным и техническим мерам защиты информации в информационных системах АО «Содружество».

Цели деятельности по обеспечению информационной безопасности АО «Содружество» является:

- обеспечение конфиденциальности, целостности, доступности защищаемой информации;
- обеспечение информационной безопасности бизнес-процессов компании;
- предотвращение утечек защищаемой информации;
- мониторинг событий безопасности и реагирование на инциденты безопасности;
- определение стратегии построения, реализации и дальнейшего развития системы информационной безопасности;
- нейтрализация актуальных угроз безопасности информации;
- выполнение требований действующего законодательства по защите информации.

4. Содержание политики

4.1 Неисполнение или некачественное исполнение работниками АО «Содружество» и пользователей информационных систем обязанностей по обеспечению информационной безопасности может повлечь лишение доступа к информационным системам, а также применение к виновным административных мер воздействия, степень которых определяется требованиями действующего законодательства.

4.2 Стратегия АО «Содружество» в части противодействия угрозам информационной безопасности заключается в сбалансированной реализации взаимодополняющих мер по обеспечению безопасности: от организационных мер на уровне руководства АО «Содружество», до специализированных мер информационной безопасности по каждому выявленному риску, основанных на оценке рисков информационной безопасности.

4.3 В рамках реализации деятельности по обеспечению информационной безопасности в АО «Содружество» осуществляются:

- сбор информации о событиях информационной безопасности
- выявление и анализ инцидентов информационной безопасности;
- расследование инцидентов информационной безопасности;
- оперативное реагирование на инцидент информационной безопасности;
- минимизация негативных последствий инцидентов информационной безопасности;
- оперативное доведение до руководства информации по наиболее значимым инцидентам информационной безопасности и оперативное принятие решений по ним, включая регламентирование порядка реагирования на инциденты информационной безопасности;
- выполнение принятых решений по всем инцидентам информационной безопасности в установленные сроки;
- пересмотр применяемых требований, мер и механизмов по обеспечению информационной безопасности по результатам рассмотрения инцидентов информационной безопасности;
- повышение уровня знаний персонала в вопросах обеспечения информационной безопасности;
- обеспечение регламентации и управления доступом к программным и программно-техническим средствам;
- обеспечение бесперебойной работы автоматизированных систем и сетей связи;

- обеспечение возобновления работы автоматизированных систем и сетей связи после прерываний и нештатных ситуаций;
- применение средств защиты от вредоносных программ;
- обеспечение информационной безопасности при использовании доступа в сеть Интернет и услуг электронной почты;
- контроль доступа в здания и помещения АО «Содружество».

4.4 В целях проверки деятельности по обеспечению информационной безопасности осуществляются:

- контроль правильности реализации и эксплуатации защитных мер;
- контроль изменений конфигурации систем и подсистем;
- мониторинг факторов рисков и соответствующий их пересмотр;
- контроль реализации и исполнения требований работниками АО «Содружество» действующих внутренних нормативных документов по обеспечению информационной безопасности;
- контроль деятельности работников и других пользователей информационных систем, направленный на выявление и предотвращение конфликтов интересов.

4.5 В целях совершенствования деятельности по обеспечению информационной безопасности осуществляется периодическое, а при необходимости оперативное, уточнение/пересмотр целей и задач обеспечения информационной безопасности.

5. Ответственность в сфере информационной безопасности

Общее руководство обеспечением информационной безопасности АО «Содружество» осуществляется ответственным лицом, назначенным Генеральным директором.

Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы системы менеджмента информационной безопасности лежит на руководстве ответственного подразделения.

Ответственность работников АО «Содружество» за невыполнение настоящей Политики определяется соответствующими положениями, включаемыми в трудовые договоры с работниками АО «Содружество», а также положениями внутренних нормативных документов.

6. Контроль за соблюдением положений Политики

Общий контроль состояния информационной безопасности АО «Содружество» осуществляется ответственным лицом, назначенным Генеральным директором.

Текущий контроль соблюдения настоящей Политики осуществляет ответственное подразделение. Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов информационной безопасности, по результатам оценки информационной безопасности, а также в рамках иных контрольных мероприятий.