

УТВЕРЖДЕНА
Приказом АО «Содружество»
от «04» 04 2023 №108

**ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
АО «СОДРУЖЕСТВО»**

СОДЕРЖАНИЕ

- 1. Общие положения**
- 2. Перечень применяемых терминов и определений**
- 3. Описание объекта защиты**
- 4. Цели политики**
- 5. Содержание политики**
- 6. Ответственность в сфере информационной безопасности**
- 7. 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. Перечень применяемых терминов и определений

- ЭВМ - электронная вычислительная машина, системный блок (компьютер).
- КПК - карманный персональный компьютер.
- Антивирус - средство защиты оборудования с программным обеспечением от вредоносного кода (вирусов).
- Программные средства - объекты, состоящие из программ, а также, если предусмотрено, сопутствующих им документации и данных, относящихся к функционированию системы обработки информации.
- Аппаратные средства - электронные и механические части вычислительного устройства, входящие в состав системы, например, мышка, клавиатура, монитор, принтер.
- Информационная система - система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы, которые обеспечивают и распространяют информацию.
- Программный продукт - набор машинных программ, процедур и связанных с ним документации и данных.
- Сетевые ресурсы - «общая папка», «технологические инструкции», «папка кассира» и т.п. расположенные в разделе сетевые расположения.
- Портативное запоминающее устройство - подключаемое к компьютеру или мультимедийным цифровым устройствам обычно через интерфейс USB (флеш-накопитель, компакт-диск, внешний жесткий диск).
- Электронная цифровая подпись (ЭЦП) - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа.

3. 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.

4. 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» являются:

- 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.

5. Содержание политики

5.1 Правила и процедуры идентификации и аутентификации пользователей

5.1.1 С целью соблюдения принципа персональной ответственности за свои действия каждому работнику АО «Содружество», допущенному к работе с ресурсами, присваивается уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в информационных системах компании.

5.1.2 Использование одного и того же имени пользователя несколькими пользователями (или группового имени для нескольких пользователей) запрещено.

5.1.3 Идентификация и аутентификация на сетевом оборудовании (коммутаторы, маршрутизаторы, точки доступа и т. д.) разрешена только администраторам безопасности, системным администраторам и работникам сторонней организации, производящим работы в сети АО «Содружество» на договорной основе под контролем Администратора.

5.1.4 Идентификаторы (логин) и пароли доступа к информационным системам должны удовлетворять следующим требованиям:

- быть уникальными для каждой системы и случайными;
- не являться именами собственными, словарными словами, набором повторяющихся или последовательно идущих символов;
- должны состоять из символов как минимум 3-х видов из следующих 4-х подмножеств:

A-Z - буквы латинского алфавита в верхнем регистре;

a-z - буквы латинского алфавита в нижнем регистре;

0-9 - цифры;

~+\$#@% и т.п. - спецсимволы;

- иметь длину не менее восьми символов;
- не использовать для процессов автоматический вход в систему.

5.1.5 Пароли должны держаться в тайне

5.1.6 Пользователю ЭВМ запрещается:

- передавать пароли в сообщениях электронной почты без шифрования, мессенджерах и других открытых каналах связи;
- сообщать пароли другим лицам, друзьям, родственникам и т.п.;
- публиковать пароли в анкетах, соц. сетях и других формах;

- указывать в подсказке к паролю способ составления пароля либо парольную фразу, из которой сформирован пароль (например, «моя фамилия»);
 - хранить пароли в открытом (незашифрованном) виде в файлах на любом компьютере, в том числе на ноутбуках, на КПК, в смартфонах и т.п.;
 - хранить пароли на любых носителях в общедоступном месте;
 - использовать опцию «запомнить пароль» в программных продуктах, таких, как Chrome, Outlook, Яндекс браузер, Internet Explorer и т.п.

5.1.7 Раскрытие пароля разрешается только работникам сектора по информационным технологиям и только для технического обслуживания персонального компьютера или устранения неисправностей. После завершения работ пароль считается скомпрометированным.

5.1.8 Не допускается использование одинаковых паролей для служебных учетных записей и учетных записей, используемых в личных целях за пределами АО «Содружество» (например, учетная запись домашнего и рабочего компьютера и т.п.)

5.1.9 Каждый работник, работающий на ЭВМ, должен проводить плановую смену паролей от учетной записи компьютера, почтового аккаунта, корпоративного портала Битрикс 24, служебных программ и т.п. не реже чем раз в 90 дней.

5.1.10 Внеплановая смена паролей работниками производится в следующих случаях:

- если появились основания полагать, что тайна пароля раскрыта;
- в случае компрометации пароля;
- по возвращении к месту работы после длительного отсутствия (отпуск, больничный, командировка, учебная сессия и т.п.);
- после технического обслуживания оборудования или программного обеспечения, или устранения неисправностей работниками сектора по информационным технологиям, если для технического обслуживания передавался пароль от учетной записи пользователя, почты программы и т.п.

5.1.11 При смене предыдущего пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях.

5.1.12 При смене предыдущего пароля новое значение не должно совпадать с любым из трех предыдущих использованных паролей.

5.1.13 При покидании рабочего места запрещается оставлять разблокированным ЭВМ. Во избежание несанкционированного доступа необходимо его блокировать. Заблокировать можно двумя способами - с помощью сочетания клавиш Win+L или Ctrl+Alt+Delete. После данной команды ЭВМ вызывает окно безопасности Windows, в котором

необходимо выбрать пункт «Заблокировать».

5.2 Правила и процедуры работы в сети Интернет и локальной сети

5.2.1 При работе в сети Интернет не следует заходить на незнакомые, потенциально опасные сайты.

5.2.2 Запрещается открывать рекламные баннеры, скачивать файлы из неизвестных источников, вводить номер сотового телефона для скачивания файлов.

5.2.3 Запрещается хранить корпоративную информацию на личных облачных ресурсах такие как, Google Диск, Яндекс Диск, Облако Mail.ru и т.п

5.2.4 Для исключения переполнения сервера необходимо очищать неиспользуемую и потерявшую актуальность информацию.

5.2.5 Запрещается хранить личные данные в общих папках организации (фото и видеинформацию, программы, неслужебные документы).

5.2.6 Перед загрузкой новых файлов на внутренние сетевые ресурсы, их необходимо проверить на вирусы.

5.2.7 Запрещается использовать интернет в личных целях.

5.3 Правила и процедуры управления установкой компонентов программного обеспечения

5.3.1 В ЭВМ разрешено использование только того программного обеспечения, его компонентов, утилит и драйверов, которые необходимы для обеспечения функционирования информационной системы, а также необходимы для выполнения служебных (должностных) обязанностей пользователями.

5.3.2 Установка программного обеспечения, его компонент, утилит и драйверов осуществляется только системными администраторами или администратором безопасности.

5.3.3 Запрещается самовольно вносить изменения в конфигурацию программного обеспечения.

5.4 Правила использования специализированных внешних носителей информации.

5.4.1 На внешних носителях, которые используются и подключаются к ЭВМ (флеш-накопитель, компакт-диск, внешний жесткий диск), разрешено хранить только информацию служебного

характера. Запрещено хранить на внешних носителях личные данные (фото- и видеинформацию, программы, неслужебные документы).

5.4.2 Личные и неучтенные носители информации подключать к ЭВМ и использовать категорически запрещено.

5.4.3 Следует разделять носители на два вида:

- для конфиденциальной, коммерческой информации и персональных данных;
- для всей остальной служебной не конфиденциальной информации.

5.4.4 На внешние носители, предназначенные для конфиденциальной, коммерческой информации и персональных данных, записывать не конфиденциальную информацию запрещено.

5.4.5 На внешние носители, не предназначенные для конфиденциальной, коммерческой информации и персональных данных, записывать конфиденциальную, коммерческую информацию и персональные данные запрещено.

5.4.6 Каждый внешний электронный носитель информации должен иметь персональный номер (идентификатор, инвентарный номер), который наносится на его корпус.

5.4.7 Каждый внешний носитель должен быть учтен в специальном журнале (реестре), утвержденном главным инженером («Журнал учета машинных носителей»). При этом:

- носители для конфиденциальной, коммерческой информации и персональных данных следует учитывать в отдельном журнале для носителей с конфиденциальной информацией в соответствии с положениями и иными локальными нормативными актами АО «Содружество»;
- носители для служебной не конфиденциальной информации следует учитывать в журнале учета служебных носителей для не конфиденциальной информации, в который должны вноситься персональный номер носителя (идентификатор), фамилия, имя, отчество владельца и примерное (возможное) содержание записанных данных;

5.4.8 Журнал учета машинных носителей должен находиться у начальника сектора по ИТ.

5.4.9 Работники АО «Содружество», работающие на ЭВМ, несут персональную ответственность за содержание информации на внешних электронных носителях, подключаемых к ЭВМ.

5.5 Правила использования электронной почты и защиты от спама

5.5.1 При работе с электронной почтой запрещается открывать письма от неизвестных отправителей, скачивать и запускать вложения так же переходить по ссылкам. Вложенные в письмо файлы необходимо

обязательно проверять антивирусом перед открытием;

5.5.2 Для служебной переписки разрешено использование только корпоративного почтового адреса (@sodrppk.ru).

5.5.3 Запрещается отправка данных содержащие информацию составляющую коммерческую тайну или персональные данные на почтовые адреса, не входящие в корпоративную почту компании.

5.6 Правила использования электронной цифровой подписи

5.6.1 Необходимо обеспечить защиту ЭВМ паролем. При покидании рабочего места компьютер необходимо блокировать.

5.6.2 Хранить флэш-накопитель с квалифицированной электронной подписью нужно в сейфе или другом защищенном месте.

5.6.3 При утере (пропаже) электронного ключа необходимо оперативно обратиться в удостоверяющий центр и аннулировать электронную подпись, сообщить о данном факте руководству АО «Содружество».

5.6.4 Пользователям необходимо периодически (раз в 14 дней) проверять электронные подписи на сайте «Госуслуги». В портале «Госуслуги» есть возможность узнать, не оформлена ли «без Вашего вмешательства на Вас» новая электронная подпись.

5.6.5 При задании обновленного пароля придерживаться следующих рекомендаций:

- длина должна составлять 8-10 символов;
- пароль должен включать в себя одновременно цифры, латинские буквы, специальные символы;
- запрещено использовать наборы символов, представляющих комбинации типа «qwerty» и другие, где элементы находятся на соседних кнопках;
- запрещено использование в качестве PIN-кода личных данных;
- запрещается на разных устройствах ЭЦП использовать одинаковые пароли.

5.7 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.

5.8 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.

5.9 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».

5.10 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.

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

6. 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, включенными в трудовые договоры с работниками АО «Содружество», а также положениями внутренних нормативных документов.

7. Контроль за соблюдением положений Политики

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

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