

УТВЕРЖДАЮ

Директор

ООО «Альянс»

Н.А. Демиденко



2026 г.

ПРАВИЛА
работы с обезличенными данными
в ООО «Альянс»

СОДЕРЖАНИЕ

<u>1.</u>	<u>ОБЩИЕ ПОЛОЖЕНИЯ</u>	3
<u>2.</u>	<u>ПРАВИЛА РАБОТЫ ПОЛЬЗОВАТЕЛЕЙ</u>	3
<u>3.</u>	<u>ПОРЯДОК ПЕРЕСМОТРА ПРАВИЛ</u>	5
<u>4.</u>	<u>ОТВЕТСТВЕННЫЕ ЗА КОНТРОЛЬ ВЫПОЛНЕНИЯ ИНСТРУКЦИИ</u>	5
	<u>ПРИЛОЖЕНИЕ 1 ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ В ИНСТРУКЦИИ</u>	6

1. ОБЩИЕ ПОЛОЖЕНИЯ

- 1.1. Правила работ с обезличенными данными (далее Правила), устанавливают обязанности, права и порядок работы пользователей в информационных системах и на бумажных носителях общества с ограниченной ответственностью «Следующее поколение» (далее по тексту – организация) с обезличенными данными.
- 1.2. Ознакомление сотрудников структурных подразделений организации с Правилами проводят руководители этих структурных подразделений под роспись.

2. ПРАВИЛА РАБОТЫ ПОЛЬЗОВАТЕЛЕЙ

Сотрудники обязаны:

Выполнять свои функциональные обязанности строго в рамках прав доступа к внутренним и внешним информационным ресурсам.

Немедленно ставить в известность администратора ИСПДн и руководителя подразделения в случае утери личных реквизитов доступа или при подозрении компрометации личных паролей, а также:

При подозрении на совершение попыток несанкционированного доступа к обезличенным данным, как в ИСПДн, так и на бумажных носителях информации.

Использовать носители информации исключительно для выполнения своих служебных обязанностей.

Обеспечивать физическую безопасность носителей информации всеми разумными способами.

Извещать администраторов ИБ и ИСПДн о фактах утраты (кражи) учтенных носителей информации.

При сдаче в ремонт ПЭВМ в стороннюю организацию в обязательном порядке изымать жесткий магнитный диск с хранящимися на нём обезличенными данными.

Вход в помещение, где хранятся обезличенные данные, разрешен работникам, служебные обязанности которых предусматривают работу с данными документами. Доступ других лиц в данные помещения в случае служебной необходимости возможен только с разрешения Директора организации.

Для хранения обезличенных данных на бумажных носителях организация обеспечивается необходимым количеством сейфов, в которых запрещается хранение предметов, не относящихся к данным документам.

Все замки сейфов должны иметь по два экземпляра ключей.

Вторые экземпляры ключей от них, а также от входных дверей помещений, где организовано хранение обезличенных данных, хранятся в сейфе ответственного за обеспечение персональных данных в организации.

Лица, работающие с обезличенными данными на бумажных носителях информации, должны иметь на рабочем столе те документы, которые необходимы в данный момент, а все остальные должны находиться в сейфах или папках, на столе не должно быть посторонних бумаг. Работать с документами при открытых окнах разрешается в том случае, если на окнах имеются сетки, предотвращающие вылет документов из помещения и соблюдаются меры по защите от просмотра документов.

По окончании рабочего дня каждый исполнитель обязан проверить наличие находящихся у него документов и убрать их в сейфы. Сейфы закрыть и сдать под охрану.

Сотрудникам категорически ЗАПРЕЩАЕТСЯ:

- ~ Хранить и обрабатывать личную информацию на ПЭВМ, где обрабатываются обезличенные данные.
- ~ Оставлять без присмотра включенную ПЭВМ, не активизировав средства защиты от НСД.
- ~ Оставлять без присмотра документы с обезличенными данными на рабочем месте, выходя из кабинета.
- ~ Оставлять без личного присмотра на рабочем месте или где бы то ни было свои персональные реквизиты доступа.
- ~ Использование для хранения и обработки обезличенных данных машинных носителей информации, не поставленных на учет в установленном порядке.
- ~ Использовать носители информации в личных целях.
- ~ Передавать носители информации другим лицам (за исключением администраторов ИБ и администраторов ИСПДн).
- ~ Хранить съемные носители с обезличенными данными вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;
- ~ Выносить съемные носители с обезличенными данными из служебных помещений для работы с ними на дому и т. д.

3. ПОРЯДОК ПЕРЕСМОТРА ПРАВИЛ

Правила подлежат полному пересмотру в следующих случаях:

~ при изменении перечня решаемых задач, организационных мер, состава технических и программных средств ИСПДн, приводящих к существенным изменениям технологии обработки информации.

Правила подлежат частичному пересмотру в остальных случаях.

Полный пересмотр данного документа проводится ответственным за обеспечение безопасности персональных данных, совместно с директором организации с целью проверки соответствия определенных данным документом мер защиты реальным условиям применения их в ИСПДн.

Частичный пересмотр данного документа проводится ответственным за обеспечение безопасности персональных данных в организации с обязательным указанием оснований и внесенных изменений в Листе регистрации изменений в Инструкции (Приложение 1).

Вносимые изменения не должны противоречить другим положениям Инструкции.

4. ОТВЕТСТВЕННЫЕ ЗА КОНТРОЛЬ ВЫПОЛНЕНИЯ ИНСТРУКЦИИ

Ответственным за постоянный контроль выполнения требований данной Инструкции является:

Ответственный за обеспечение безопасности персональных данных в организации.

