Утверждено приказом

ООО «ЛОУДЕР ЭСПИИКС»

№ ____ от «___» _____ 2023 г.

ИНСТРУКЦИЯ РАБОТНИКА ПО ПРАВИЛАМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2023 год
Москва

СОДЕРЖАНИЕ

1. СОКРАЩЕНИЯ, ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.1. Термины и определения

В настоящем документе использованы следующие термины и определения:

1.1.1. **Безопасность персональных данных** – состояние защищенности персональных данных от неправомерных действий, характеризуемое способностью пользователей, технических средств и информационных систем обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке, независимо от формы их представления.

1.1.2. **Вредоносное программное обеспечение** – программное обеспечение, предназначенное для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

1.1.3. **Доступность персональных данных** – возможность беспрепятственного получения санкционированного доступа к персональным данным лицами, имеющими право на такой доступ.

1.1.4. **Информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.1.5. **Конфиденциальность персональных данных** – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не раскрывать третьим лицам и не допускать их распространения при отсутствии согласия субъекта персональных данных или иного законного основания.

1.1.6. **Обработка персональных данных** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

1.1.7. **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

1.1.8. **Пользователь персональных данных** – лицо, участвующее в процессе обработки персональных данных или использующее результаты такой обработки.

1.1.9. **Процесс обработки персональных данных** – бизнес-процесс Компании, в рамках которого осуществляется обработка персональных данных.

1.1.10. **Средство вычислительной техники** – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

1.1.11. **Средство защиты информации** – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

1.1.12. **Уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

1.1.13. **Целостность персональных данных** – способность средства вычислительной техники или информационной системы обеспечивать неизменность персональных данных в условиях случайного и (или) преднамеренного их искажения (разрушения).

1.2. **Используемые сокращения**

В настоящем документе использованы сокращения, приведенные в Таблице 1.

Таблица 1. Сокращения

Сокращение	Описание
АРМ	Автоматизированное рабочее место
ИБ	Информационная безопасность
ИСПДн	Информационная система персональных данных
ПДн	Персональные данные
ПО	Программное обеспечение
СЗИ	Средство защиты информации
СЗПДн	Система защиты персональных данных

2. НАЗНАЧЕНИЕ И ОБЛАСТЬ ДЕЙСТВИЯ ДОКУМЕНТА

2.1. Настоящая Инструкция работника по правилам обработки персональных данных (далее – "Инструкция") определяет основные обязанности, права и ответственность работника, допущенного к автоматизированной и неавтоматизированной обработке ПДн в ООО «ЛОУДЕР ЭСПИИКС» (далее – "Компания").

2.2. Требования настоящей Инструкции обязательны для исполнения всеми работниками Компании, участвующими в процессах обработки ПДн, либо использующими результаты их функционирования – Пользователями ПДн.

2.3. Настоящая Инструкция должна быть доведена до всех Пользователей ПДн под подпись.

3. ПОРЯДОК ПОЛУЧЕНИЯ ДОСТУПА К ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Доступ к обработке ПДн предоставляется работникам при условиях:

- ознакомления с внутренними документами Компании, определяющими правила обработки и обеспечения безопасности ПДн;
- прохождения инструктажа по правилам обработки и обеспечения безопасности ПДн.

3.2. До получения доступа к обработке ПДн Пользователю ПДн необходимо изучить следующие документы:

- Политика обработки и обеспечения безопасности ПДн в ООО «ЛОУДЕР ЭСПИИКС»;
- Положение по обработке персональных данных;
- настоящая Инструкция.

3.3. Инструктаж Пользователей ПДн проводится Ответственным за организацию обработки ПДн.

3.4. По результатам изучения документов и прохождения инструктажа Пользователь ПДн обязан знать:

- штатные режимы работы и правила работы с техническими компонентами ИСПДн;
- правила парольной защиты;
- правила антивирусной защиты;

– способы выявления и последовательность действий в случае выявления нештатного функционирования технических компонентов ИСПДн;

– правила поведения в экстренных ситуациях, последовательность действий при ликвидации последствий от инцидентов ИБ.

3.5. Пользователь ПДн имеет право обратиться за консультацией:

– по общим вопросам обеспечения безопасности ПДн в Компании – к Ответственному за организацию обработки ПДн;

– по вопросам автоматизированной и неавтоматизированной обработки ПДн в рамках процесса обработки ПДн, в котором он принимает участие, к непосредственному руководителю или руководителю структурного подразделения, в компетенции которого находится данный процесс;

– по вопросам использования СЗИ и технических компонентов ИСПДн – к Ответственному за обеспечение безопасности ПДн;

– Пользователь ИСПДн имеет право вносить на рассмотрение предложения по совершенствованию процессов обработки персональных данных, в которых он принимает участие в соответствии со своими должностными обязанностями.

4. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Общие меры

При обработке ПДн Пользователи ПДн обязаны соблюдать следующие меры предосторожности:

– не предоставлять ПДн лицам, не имеющим права доступа к данной информации;

– не выносить носители ПДн за пределы территории Компании без согласования с непосредственным руководителем;

– не осуществлять запись и не хранить ПДн на неучтенных носителях информации (гибких магнитных дисках, USB-flash накопителях и т.п.);

– не использовать ПДн в открытых публикациях (например, при написании статей, докладов и др.);

– не накапливать излишние ПДн (уничтожать документы и файлы по мере завершения работы с ними);

– осуществлять уничтожение документов средствами гарантированного уничтожения (шредер);

– не копировать и не печатать содержащие ПДн файлы без надобности (в том числе и на внешние съемные носители);

– не отправлять содержащие ПДн файлы на личную электронную почту, общедоступные файловые хранилища;

– не разглашать логины и (или) пароли доступа к ресурсам Компании;

– не оставлять на рабочих местах носители ПДн без присмотра;

– не оставлять незапертыми после окончания работы шкафы, сейфы, помещения и хранилища с носителями ПДн;

– не осуществлять обработку ПДн в условиях, позволяющих осуществлять просмотр ПДн лицами, не имеющими к ним доступа, а также в условиях несоблюдения требований по эксплуатации рабочей станции;

– блокировать рабочую станцию при покидании рабочего места;

– не устанавливать самостоятельно программное обеспечение на рабочие станции;

– не подключать самостоятельно к рабочим станциям какие-либо устройства и не вносить изменения в состав, параметры конфигурации технических компонентов рабочих станций;

– не использовать программные и (или) аппаратные компоненты ИСПДн в неслужебных целях (в т. ч. для хранения ПДн, не связанных с выполнением трудовых обязанностей);

– не использовать личные устройства для обработки ПДн (смартфоны, планшетные компьютеры и т. п.);

– соблюдать правила работы со СЗИ и установленный режим разграничения доступа к техническим компонентам ИСПДн и файлам, содержащим ПДн, при их обработке;

– присутствовать при работах по изменению аппаратно-программной конфигурации закрепленной за ним рабочей станции, а по завершении таких работ проверять ее работоспособность;

– хранить в тайне информацию о СЗПДн (о средствах, механизмах, процедурах и т. д.);

– предоставлять всю необходимую информацию и документы при расследовании инцидентов ИБ, связанных с обработкой и обеспечением безопасности ПДн, проведении внутренних контрольных мероприятий по защите ПДн, а также во время проверок со стороны регулирующих органов.

4.2. Порядок работы на рабочем месте

4.2.1. Перед началом работы на рабочем месте пользователь обязан**:**

– проверить правильность подключения периферийного оборудования к рабочему месту;

– в случае обнаружения нарушений в подключении периферийного оборудования и неисправности СЗИ немедленно сообщить об этом Администратору безопасности или ответственному за обеспечение безопасности персональных данных и сделать соответствующую запись в журнале, где указать обнаруженные нарушения.

4.2.2. В процессе выполнения работ на рабочем месте пользователь обязан:

– строго соблюдать технологию обработки информации, использовать только то программное обеспечение и информационные ресурсы, которые необходимы для выполнения текущих работ;

– в случае возникновения нештатных ситуаций немедленно прекращать работу и сообщать об этом Администратору безопасности или ответственному за обеспечение безопасности персональных данных.

4.3. Обеспечение парольной защиты

4.3.1. При первичном доступе к ПДн Пользователю ПДн необходимо сформировать стойкий пароль для своей учетной записи. Пароль должен быть сформирован в соответствии со следующими рекомендациями:

– длина пароля составляет не менее восьми символов;

– длина пароля для привилегированных пользователей составляет не менее 10 символов;

– в составе символов пароля обязательно присутствуют буквы в верхнем и нижнем регистрах, цифры и специальные символы (“~!@#$%^&*()-+_=\|/?,);

– при смене пароля новое значение отличается от предыдущего не менее чем в четырех позициях;

– пароль может повторяться не менее чем после использования пяти различных паролей;

– пароль не включает в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т. д.), последовательности символов и знаков (111, qwerty, abcd и т. д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т. п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на знании информации о Пользователе ПДн.

4.3.2. В рамках обеспечения парольной защиты Пользователь ПДн обязан:

– хранить в тайне свои данные для аутентификации в системе (имя пользователя и пароль доступа);

– обновлять пароли не реже чем один раз в полгода;

– использовать разные пароли для разных систем (где это возможно).

4.4. Обеспечение антивирусной защиты

4.4.1. В рамках обеспечения антивирусной защиты Пользователь ПДн обязан:

– контролировать факт запуска антивирусного ПО после загрузки операционной системы;

– контролировать обновление антивирусных баз на своем АРМ путем сравнения даты последнего обновления с датой на момент контроля (даты не должны отличаться более чем на один календарный день);

– осуществлять антивирусный контроль любой информации, получаемой по телекоммуникационным каналам;

– осуществлять антивирусный контроль съемных носителей информации (дискет, оптических дисков, USB-flash-накопителей) при их подключении к рабочей станции.

4.4.2. При возникновении подозрения на наличие вредоносного ПО (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т. п.) Пользователь ПДн обязан сообщить об этом Ответственному за обеспечение безопасности ПДн, а также провести внеочередной антивирусный контроль своей рабочей станции (если это позволяют сделать его права доступа в системе).

4.5. Оповещение при нарушениях безопасности персональных данных

4.5.1. С целью своевременного обнаружения событий безопасности, которые могут привести к нарушению конфиденциальности ПДн или нарушению процессов их обработки, Пользователь ПДн должен своевременно оповещать Ответственного за обеспечение безопасности ПДн в следующих случаях:

– заметное снижение производительности при работе с сетью Интернет, недоступность ресурсов;

– значительное увеличение времени отклика рабочей станции, изменение дат обновления файлов, значительное возрастание размеров файлов, системные сбои (включая случаи, когда операционная система перестает загружаться);

– получение по электронной почте подозрительных сообщений;

– получение сообщений от антивирусного ПО об обнаружении вредоносного ПО;

– присутствие незнакомых подозрительных лиц на территории Компании;

– утеря личного пропуска на территорию Компании;

– недоступность одного или нескольких информационных ресурсов;

– повреждение, удаление или утрата доступа к файлам;

– обнаружение вскрытых шкафов, ящиков и прочих мест хранения носителей ПДн.

4.5.2. Пользователь ПДн должен своевременно оповещать своего непосредственного руководителя в следующих случаях:

– подозрение на неправомерность обработки ПДн;

– обращение субъекта по вопросам, связанным с обработкой или обеспечением безопасности ПДн;

– получение запроса ПДн, если есть основания полагать, что запрашивающая сторона не имеет соответствующего допуска;

– недоступность одного или нескольких информационных ресурсов;

– обнаружение вскрытых шкафов, ящиков и прочих мест хранения носителей ПДн;

– отправка ПДн на ошибочный адрес;

– утеря документа, содержащего ПДн;

– подозрение на компрометацию личных ключей и паролей;

– нахождение документа, содержащего ПДн;

– обнаружение любых подозрительных событий, которые могут привести к разглашению ПДн или нарушению процессов обработки ПДн Компании;

– нарушение требований настоящей Инструкции.

5. ОТВЕТСТВЕННОСТЬ

5.1. За несоблюдение требований нормативных документов РФ в области обработки и защиты ПДн предусмотрена дисциплинарная, административная, гражданская и уголовная ответственность.

5.2. Пользователь ПДн несет ответственность в пределах, определенных действующими нормативными документами РФ:

- за ненадлежащее выполнение требований настоящей Инструкции и документов перечисленных в п. 3.2;
- за сохранность ПДн (обеспечение их конфиденциальности, целостности и доступности);
- за сохранность и работоспособность используемых им средств обработки и защиты ПДн.

Руководство Компании вправе применять к Пользователям ПДн предусмотренные Трудовым Кодексом РФ дисциплинарные взыскания.