

УТВЕРЖДЕНО  
Приказом генерального директора  
ООО ТСО «Зиновы»  
№ \_11\_ от 15.12.2017 г.



## ИНСТРУКЦИЯ

15.12.2017 г. № \_\_4\_\_

г. Кирово-Чепецк

### Пользователя информационной системы персональных данных

## I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция регламентирует обязанности сотрудников, участвующих в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющих доступ к аппаратным средствам, программному обеспечению и данным информационной системы персональных данных (далее ИСПДн) ООО ТСО «Зиновы».

## II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. **Автоматизированная система** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

2.2. **Автоматизированное рабочее место (АРМ)** – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

2.3. **Документированная информация** - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель (ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»).

2.4. **Доступ к информации** – возможность получения информации и её использования (ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»).

2.5. **Защита информации** — деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.

2.6. **Информация** - сведения (сообщения, данные) независимо от формы их представления (ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»).

2.7. **Информационная система персональных данных (ИСПДн)** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.8. **Компрометация пароля** – раскрытие, обнаружение или утеря пароля.

2.9. **Несанкционированный доступ (НСД)** – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.

2.10. **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 (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.11. **Пароль** - секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам.

2.12. **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.13. **Распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.14. **Средство защиты информации (СЗИ)** – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

### **III. ОБЩИЕ ОБЯЗАННОСТИ СОТРУДНИКОВ**

Каждый сотрудник ООО ТСО «Зиновы», являющийся пользователем ИСПДн, обязан:

3.1. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн.

3.2. Знать и строго выполнять правила работы со средствами защиты информации, установленными на его автоматизированном рабочем месте (далее АРМ).

3.3. Соблюдать правила работы с паролем своей учётной записи.

3.4. Немедленно вызывать администратора безопасности ИСПДн и поставить в известность руководителя структурного подразделения при обнаружении:

3.4.1. нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа к защищаемой АРМ;

3.4.2. несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ;

3.4.3. отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;

3.4.4. некорректного функционирования установленных на АРМ технических средств защиты;

3.4.5. непредусмотренных отводов кабелей и подключенных к АРМ дополнительных устройств.

3.5. Всем сотрудникам ООО ТСО «Зиновы», являющимся пользователями ИСПДн, категорически ЗАПРЕЩАЕТСЯ:

3.5.1. использовать компоненты программного и аппаратного обеспечения ИСПДн ООО ТСО «Зиновы» в неслужебных целях;

3.5.2. самовольно вносить какие-либо изменения в конфигурацию АРМ или устанавливать в АРМ любые программные и аппаратные средства, кроме выданных или разрешённых к использованию ответственным за обеспечение безопасности персональных данных;

3.5.3. оставлять без присмотра своё АРМ не активизировав блокировки доступа или оставлять своё АРМ включенным по окончании работы;

3.5.4. умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению безопасности персональных данных.

#### **IV. ОБЕСПЕЧЕНИЕ СОХРАННОСТИ ИНФОРМАЦИИ**

4.1. Для обеспечения сохранности электронных информационных ресурсов ООО ТСО «Зиновы» необходимо соблюдать следующие требования:

4.1.1. Для копирования информации не должны использоваться непроверенные на наличие компьютерных вирусов и других вредоносных программ носители информации.

4.2. Субъектам доступа запрещается:

4.2.1. Установка и использование при работе с электронно-вычислительными машинами вредоносных программ, ведущих к блокированию работы сети.

4.2.2. Самовольное изменение сетевых адресов.

4.2.3. Самовольное вскрытие блоков электронно-вычислительных машин, модернизация или модификация электронно-вычислительных машин и программного обеспечения.

4.2.4. Несанкционированная передача компьютеров с прописанными сетевыми настройками. Передача компьютеров из одного подразделения в другое производится только администратором безопасности ИСПДн с предварительно удаленными сетевыми настройками.

4.3. Сведения, содержащиеся в электронных документах и базах данных ООО ТСО «Зиновы», должны использоваться только в служебных целях в рамках полномочий сотрудника, работающего с соответствующими материалами.

## **V. ПАРОЛЬНАЯ ЗАЩИТА**

5.1. Личные пароли выбираются пользователями информационной системы самостоятельно с учетом следующих требований:

5.1.1. длина пароля должна быть не менее 6 символов;

5.1.2. в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, \$, &, \*, % и т.п.);

5.1.3. пароль не должен включать в себя имя пользователя, легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, абвгд и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, которые можно угадать, основываясь на информации о пользователе;

5.1.4. при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6-ти позициях.

5.2. Сотрудникам допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами (например Кожзгсф7!).

5.3. Для обеспечения возможности использования имён и паролей некоторых сотрудников в их отсутствие (например, в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п.), сотрудники обязаны сразу же после установки своих паролей передавать их на хранение вместе с именами своих учетных записей администратору безопасности ИСПДн в запечатанном конверте или опечатанном пенале.

5.4. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

5.5. Смена паролей должна проводиться регулярно, не реже одного раза в 6 месяцев, самостоятельно каждым пользователем.

5.6. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке, мобильном телефоне и любых других предметах и носителях информации.

5.7. Запрещается сообщать свой пароль полностью или частично другим пользователям, запрещается спрашивать или подсматривать пароль других пользователей.

5.8. Запрещается регистрировать других пользователей в ИСПДн со своим личным паролем, запрещается входить в ИСПДн под учётной записью и паролем другого пользователя.

5.9. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователя должна быть немедленно проведена внеплановая процедура смены пароля.

## **VI. АНТИВИРУСНАЯ ЗАЩИТА**

6.1. При возникновении подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажения данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) самостоятельно или вместе с администратором безопасности ИСПДн провести внеочередной антивирусный контроль своего АРМ. При самостоятельном проведении антивирусного контроля - уведомить о результатах администратора безопасности ИСПДн для определения им факта наличия или отсутствия вредоносного программного обеспечения.

6.2. В случае появления информационного окна средства антивирусной защиты, сигнализирующем об обнаружении вредоносного программного обеспечения:

6.2.1. приостановить обработку данных;

6.2.2. немедленно поставить в известность о факте обнаружения вредоносного программного обеспечения администратора безопасности ИСПДн, владельца заражённых файлов, а также смежные структурные подразделения, использующие эти файлы в работе;

6.2.3. совместно с владельцем файлов, заражённых вредоносным программным обеспечением, провести анализ необходимости дальнейшего их использования;

6.2.4. произвести лечение или уничтожение заражённых файлов (при необходимости для выполнения требований данного пункта привлечь администратора безопасности ИСПДн).

## **VII. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПРАВИЛ РАБОТЫ**

7.1. Каждый пользователь ИСПДн несёт персональную ответственность за соблюдение требований настоящей Инструкции и за все действия, совершенные от имени его учётной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

7.2. За разглашение персональных данных и нарушение порядка работы со средствами ИСПДн, содержащими персональные данные, сотрудники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

7.3. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим сотрудникам, не имеющим к ним доступ), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) ООО ТСО «Зиновы», влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Сотрудник ООО ТСО «Зиновы», имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба ООО ТСО «Зиновы» (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

7.3.1. В отдельных случаях, при разглашении персональных данных, сотрудник, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях РФ.

7.4. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.

Приложение: Лист ознакомления с «Инструкцией пользователя информационной системы персональных данных» № \_\_\_\_ от \_\_\_\_\_ на 1 л. в 1 экз.

Руководитель группы по  
обслуживанию средств связи



О.Н.Маринченко

