Утверждена
приказом Службы по
финансово-бюджетному
надзору Республики Тыва
от «20» июля 2020 г. № 57/од

Инструкция
пользователя информационной системы персональных в Службе по финансово-бюджетному надзору Республики Тыва

1. Общие положения

1.1. Пользователь информационной системы персональных данных (далее – ИСПДн) осуществляет обработку персональных данных в ИСПДн.

1.2. Пользователем является каждый сотрудник Службы по финансово-бюджетному надзору Республики Тыва (далее – Служба), участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей инструкцией, Положением об обработке и защите персональных данных субъектов персональных данных в Службе, руководящими и нормативными документами ФСТЭК России, ФСБ России и регламентирующими документами Службы.

1.5. Методическое руководство работой пользователя осуществляется сотрудником ответственным за техническую защиту информации в Службе (далее - ответственный за обеспечение защиты персональных данных).

2. Должностные обязанности

Пользователь обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены должностными обязанностями или регламентом.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики (раздел 4).

2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена - Интернет и других.

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7. При работе с конфиденциальной информацией обрабатывать информацию в папках соответствующего уровня конфиденциальности.

2.8. Обо всех выявленных нарушениях, связанных с информационной безопасностью Службы, а также для получений консультаций по вопросам информационной безопасности, необходимо обратиться к ответственному за обеспечение защиты персональных данных.

2.9. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИСПДн;

2.10. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах возложенных на него функций.

3. Пользователям запрещается

3.1. Разглашать защищаемую информацию третьим лицам.

3.2. Копировать защищаемую информацию на любые носители и папки непредназначенные для обработки конфиденциальной информации.

3.3. Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

3.4. Несанкционированно открывать общий доступ к папкам на своей рабочей станции.

3.5. Запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства.

3.6. Отключать (блокировать) средства защиты информации и изменять их настройки.

3.7. Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн.

3.8. Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.

3.9. Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.

3.10. использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных целях.

3.11. При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>

4. Организация парольной защиты

4.1. Личные пароли доступа к элементам ИСПДн создаются самостоятельно.

4.2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

4.3. Правила формирования пароля:

— Пароль не может содержать имя учетной записи пользователя или какую-либо его часть.

— Пароль должен состоять не менее чем из 6 символов.

— В пароле должны присутствовать символы трех категорий из числа следующих четырех:

а) прописные буквы английского алфавита от A до Z;

б) строчные буквы английского алфавита от a до z;

в) десятичные цифры (от 0 до 9);

г) символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).

— Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа "123", "111", "qwerty" и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе.

— Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

— Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

— Запрещается выбирать пароли, которые уже использовались ранее. 4.4. Правила ввода пароля:

— Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.

— Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

4.5. Правила хранение пароля:

— Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

— Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

— Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

4.6. Лица, использующие паролирование, обязаны:

— четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию.

— своевременно сообщать Администратору информационной безопасности об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

4.7. За нарушение положений данной инструкции к работнику может быть применена ответственность, предусмотренная действующим законодательством РФ.