**ПРИЛОЖЕНИЕ 1**

**Руководство пользователя для оператора СКУД**

Настоящий документ подготовлен в рамках выполнения работ по обеспечению безопасной эксплуатации СКУД аэропорта.

**1. Общие положения**

1.1. Оператор СКУД (далее – Оператор) осуществляет работу с системой контроля и управления доступом в нотариальной конторе ИП Соболева (далее - Система).

1.2. Оператор участвует в рамках своих функциональных обязанностей в процессах обработки информации и имеет доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты Системы.

1.3. Оператор несет персональную ответственность за свои действия.

1.4. Оператор в своей работе руководствуется настоящей инструкцией, Положением о защите объекта и другими регламентирующими документами Компании.

**2. Должностные обязанности**

2.1 Оператор Системы обязан:

2.1.1. Знать и выполнять требования настоящей инструкции и других внутренних распоряжений, регламентирующих порядок действий по работе с Системой.

2.1.2. Выполнять на автоматизированном рабочем месте (далее - АРМ) только те процедуры и действия, которые определены для него должностной инструкцией.

2.1.3. Знать и соблюдать установленные требования по режиму работы с Системой, учету, хранению и пересылке носителей информации, обеспечению безопасности данных, а также руководящих и организационно-распорядительных документов.

2.1.4. Соблюдать требования политики безопасности.

2.1.5. 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).

2.1.6. Обо всех выявленных нарушениях, связанных с безопасностью Компании, а так же для получений консультаций по вопросам безопасности, необходимо обратиться в \_\_\_\_\_\_\_\_\_\_\_\_\_ по электронной почте: \_\_\_\_\_\_\_\_\_\_\_\_\_\_ или по телефону \_\_\_\_\_\_\_.

2.2.Оператору Системы запрещается:

2.2.1. Разглашать какую-либо информацию о Системе третьим лицам.

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

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

2.2.4. Запрещено подключать к рабочей станции личные внешние носители и мобильные устройства.

2.2.5. Отключать (блокировать) средства защиты Системы.

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

2.2.7. Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам Системы.

2.2.8. Привлекать посторонних лиц для производства ремонта или настройки АРМ Системы.

2.2.9. 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>.

2.2.10. Принимать меры по реагированию, в случае возникновения вне-штатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в рамках возложенных, в пределах возложенных на него функций.

**3. Организация парольной защиты на АРМ Системы**

3.1 Личные пароли доступа к АРМ Системы выдаются операторам Администратором информационной безопасности или создаются самостоятельно.

3.2. Полная плановая смена паролей АРМ Системы проводится не реже одного раза в 3 месяца.

3.3. Правила формирования пароля:

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

- Пароль должен состоять не менее чем из 8 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 повторяю-щийся 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.

3.4. Правила ввода пароля:

- Ввод пароля должен осуществляться с учётом регистра, в котором па-роль был задан.

- Во время ввода паролей необходимо исключить возможность его под-сматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.5. 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.

3.6. Лица, использующие паролирование, обязаны:

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

- своевременно сообщать Администратору об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

**С настоящей инструкцией ознакомлен:**

\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_ «\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_ г.

ФИО Подпись