УТВЕРЖДАЮ
Генеральный директор
СЗАО «Интерднестрком»
Ганжа С.Н.
«___»_____ 2021г.

ИНСТРУКЦИЯ
по организации парольной защиты информации в СЗАО «Интерднестрком»

1. Общие положения

1.1. Настоящая Инструкция устанавливает требования о необходимости разграничения доступа должностных лиц к информационным ресурсам, хранящимся в персональных компьютерах, вычислительных сетях и базах данных информационных систем Компании.

1.2. Настоящая Инструкция определяет правила выработки, назначения, изменения и ввода имен пользователей и паролей разграничения доступа к указанным информационным ресурсам, порядок работы с парольной документацией.

1.3. Настоящая Инструкция является составной частью комплексной системы защиты от несанкционированного доступа к информационным ресурсам и обязательна к исполнению всеми сотрудниками Компании.

1.4. Имя пользователя представляет собой последовательность символов установленного формата, позволяющую однозначно идентифицировать пользователя при входе в систему и проведении им каких-либо действий над информационными ресурсами.

1.5. Пароль, как средство идентификации пользователей в компьютерной сети, используется для защиты от несанкционированного доступа к средствам вычислительной техники, сетям, базам данных информационных систем и представляет собой буквенную, цифровую или буквенно-цифровую группу символов определенной длины.

1.6. В системе пользователю присваиваются персональные имя и пароль для доступа к определенным информационным ресурсам. При этом устанавливаются следующие категории пользователей:

- имя и пароль для аутентификации-идентификации пользователей на доступ к работе за ПК - локальный пользователь;
- имя и пароль для аутентификации-идентификации пользователей на доступ к работе в домене – доменный пользователь;
- имя и пароль для аутентификации-идентификации пользователей для обращения к базам данных (по каждой базе данных отдельно) пользователь БД.

2. Требования к формированию паролей.

2.1. Персональные пароли должны генерироваться специальными программными средствами системных администраторов либо задаваться системным администратором самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее девяти символов;
- в числе символов пароля должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы, такие, как ~ ! @ # $ % ^ & * ( ) - + _ = \ | / ;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.п.), клавиатурные последовательности символов и знаков, аббревиатуры, а также общепринятые сокращения (ЭВМ, ЛВС, User и т.п.).

2.2.При выборе пароля надо учитывать ограничения конкретных систем и программ, которые не могут соответствовать таким требованиям.

Запрещается использовать в качестве пароля «пустой» пароль, имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а также 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.

2.3. Ввод пароля должен осуществляться с учётом регистра (верхний - нижний), в котором пароль был задан и с учётом текущей раскладки клавиатуры (RU-EN).

2.4. Личный пароль сотрудники не имеют права сообщать кому бы то ни было.

3. Порядок смены паролей сотрудников Компании:

3.1. Полная плановая смена паролей сотрудников Компании должна проводиться регулярно, не реже одного раза в 6 месяцев.

3.2. Внеплановая смена личного пароля сотрудника Компании в случае прекращения его полномочий (увольнение, перевод на другую работу и т.п.) должна производиться специалистом по информационному обеспечению немедленно после окончания последнего сеанса работы данного сотрудника с системой.

3.3. В случае компрометации личного пароля сотрудника Компании надлежит немедленно ограничить доступ к информации с данной учетной записи, до момента вступления в силу новой учетной записи пользователя и пароля.

3.4. Внеплановая полная смена паролей всех сотрудников Компании должна производиться в случае прекращения полномочий (увольнение, перевод на другую работу и другие обстоятельства) системного администратора и специалиста, по информационной безопасности, которым по роду работы были предоставлены полномочия по управлению парольной защитой информации, либо в случае компрометации их паролей.

3.5. При смене пароля новое значение должно отличаться от предыдущего не менее чем в шести позициях.

3.6. Системный администратор оказывает необходимую помощь сотрудникам Компании в процессе смены пароля.

4. Хранение пароля:

4.1. Всем сотрудникам Компании запрещается:

- записывать пароли на бумаге, в файле, электронной записной книжке, также на других окружающих предметах (на клавиатуре, мониторе, и т.п.);
- сообщать другим сотрудникам Компании личный пароль и регистрировать их в системе под своим паролем.

4.2. Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или отражённом свете) или техническими средствами (видеокамеры, фотоаппараты, телефоны и др.).

4.3. При увольнении сотрудника Компании, руководитель структурного подразделения Компании обязан в срок не более 1 (одного) рабочего дня сообщить об этом специалисту ответственному по защите информации или системному администратору. Системный администратор немедленно блокирует учетную запись, соответствующую этому сотруднику Компании, из средств электронно-вычислительной техники.

5. Действия в случае утери и компрометации пароля:

5.1. Под компрометацией пароля понимается: утрата, хищение, несанкционированное копирование паролей, разглашение паролей лицам, которые не должны иметь доступ к информационным ресурсам системы или другая ситуация, которая может сложиться с паролем, когда информация о паролях становится известной.

5.2. При компрометации паролей сотрудник Компании обязан немедленно сообщить о случившемся своему непосредственному руководителю и специалисту, ответственному по защите информации, для смены пароля в соответствии с вышеуказанными требованиями.

6. Ответственность при организации парольной защиты:

6.1. Ответственность за организацию парольной защиты возлагается на специалиста, ответственного по защите информации, системного администратора и руководителя подразделения.

6.2. Периодический контроль за соблюдением требований данной Инструкции возлагается на специалиста, ответственного по защите информации.

6.3. Сотрудники Компании должны быть ознакомлены с данной инструкцией и предупреждены об ответственности за использование паролей не соответствующих требованиям, а также за разглашение парольной информации.

6.4. Ответственность в случае несвоевременного уведомления ответственного лица о случаях утери, кражи, взлома или компрометации паролей возлагается на владельца взломанной учетной записи