УТВЕРЖДЕНО приказом
ОГПОБУ «Политехнический техникум»
№134 от 11.05.2016 г.

ИНСТРУКЦИЯ
по организации парольной защиты в ОГПОБУ «Политехнический техникум»

1. Правила формирования личного пароля.

1.1. В качестве пароля должна выбираться последовательность символов, обеспечивающая малую вероятность её угадывания. Пароль должен легко запоминаться. В пароль должны быть включены символы верхнего и нижнего регистров и цифры. Длина пароля должна быть не менее шести символов.

1.2. При выборе пароля надо учитывать ограничения конкретных систем и программ, которые не могут соответствовать таким требованиям (например, не все программы позволяют вводить пробелы в пароле или длина пароля может быть ограничена до какого-либо числа символов).

1.3. Запрещается использовать в качестве пароля «пустой» пароль, имя входа в систему, простые пароли типа «123», «111», «abc» 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.

1.4. Запрещается выбирать пароли, которые уже использовались ранее.

2. Ввод пароля.

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

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

3. Порядок смены личных паролей.

3.1. Полная плановая смена паролей должна проводится регулярно, не реже одного раза в год.

3.2. Внеплановая смена (удаление) личного пароля любого пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, либо переход на другую работу внутри банка) должна производится немедленно после окончания последнего сеанса работы данного пользователя системы.

3.3. Внеплановая полная смена паролей должна производится в случае прекращения полномочий (увольнение, переход на другую должность и другие обстоятельства) администраторов информационной безопасности и других сотрудников, которым по роду работы были предоставлены либо полномочия по управлению автоматизированной системой в целом, либо полномочия по управлению подсистемой защиты информации данной системы, а значит, кроме личного пароля им могут быть известны пароли других пользователей системы.

3.4. Смена личного пароля производится пользователем самостоятельно.

3.5. Администратор информационной безопасности оказывает необходимую помощь пользователям в процессе смены пароля.

3.6. Изменять заданный администратором информационной безопасности временный пароль изменяется пользователем при первом же входе в систему.

4. Хранение пароля.

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

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

5. Действия в случае утери и компрометации пароля.

5.1. В случае утери пароля сотрудник временно получает у администратора информационной безопасности временный пароль.

5.2. В случае компрометации пароля (подсматривание кем-либо, разглашение пароля и др.) пароль необходимо сменить в соответствии с вышеуказанными требованиями.

6. Ответственность при организации парольной защиты.

6.1. Ответственность за организацию парольной защиты в подразделении возлагается на администратора безопасности.

6.2. Периодический контроль за соблюдением требований данной инструкции возлагается на администратора безопасности информации.

6.3. Владельцы паролей должны под расписку быть ознакомлены с данной инструкцией.

Подготовил:

Администратор безопасности информации _____