ООО «АСТРА»

Адрес: 607060, Нижегородская обл., г. Выкса, пл. Октябрьской революции, д. 48, офис 217
ИНН 5247054590 КПП 524701001 ОГРН 1175275064062
Банк: Волго-Вятский Банк ПАО « Сбербанк» г. Нижний Новгород р/с 40702810642000030189 к/с 30101810900000000603
БИК 042202603

Инструкция по организации парольной защиты в информационных системах персональных данных

Утверждено

Директор ООО »АСТРА»

Приказ от "01" сентября 2024 г. N 1 ПД

Инструкция
по организации парольной защиты в информационных системах персональных данных в ООО «АСТРА».

1. Общие положения

1.1. Настоящая Инструкция определяет порядок организации парольной защиты в информационных системах персональных данных в ООО «АСТРА» (далее - организация).

1.2. Настоящая Инструкция обязательна для соблюдения всеми сотрудниками организации, имеющими доступ к персональным данным.

1.3. Настоящая Инструкция разработана в соответствии со ст. 19 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", Постановлением Правительства Российской Федерации от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.4. Контроль за соблюдением настоящей Инструкции сотрудниками организации, имеющими доступ к персональным данным, осуществляет ответственный за безопасность информационных систем в организации.

2. Основы организации парольной защиты
в информационных системах организации

2.1. Для защиты информационных систем всем сотрудникам, имеющим доступ к персональным данным, для входа в информационную систему устанавливаются пароли.

2.2. Пароль генерируется ответственным за безопасность информационных систем и выдается каждому сотруднику в запечатанном конверте (вариант: в электронной форме) (либо сотрудник может сам придумать себе пароль). Придуманный пароль должен отвечать следующим требованиям безопасности:

длина пароля должна быть не менее 8 (ВОСЬМИ) символов;

в числе символов пароля должны присутствовать символы трех категорий из числа следующих четырех:

- прописные буквы английского алфавита от A до Z;

- строчные буквы английского алфавита от a до z;

- десятичные цифры (от 0 до 9);

- неалфавитные символы (например: !, $, #, %);

пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.д.), а также общепринятые сокращения (LAN, USER и т.п.);

при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях).

2.3. Ввод пароля должен осуществляться сотрудником - владельцем пароля - по памяти и без произнесения символов пароля вслух. Во время ввода пароля необходимо исключить возможность его просмотра посторонними лицами или техническими средствами.

2.4. Пароль не должен отображаться на экране персонального компьютера.

2.5. Для ввода пароля сотруднику дается 3 попытки. В случае провала всех попыток сотрудник должен обратиться к ответственному за безопасность информационных систем за решением данной проблемы. Сотрудник должен написать объяснительную по данному инциденту. Ответственный за безопасность информационных систем восстанавливает доступ к информационной системе для данного сотрудника и обязан уведомить руководителя организации с приложением объяснительной сотрудника.

2.6. Сотрудник организации, имеющий доступ к информационной системе персональных данных, не имеет права сообщать каким-либо образом свой пароль кому-либо, осуществлять регистрацию других сотрудников в информационной системе персональных данных под своим паролем, а также осуществлять работу в информационной системе персональных данных с использованием чужих паролей.

2.7. Смена пароля должна производиться каждые 12 МЕСЯЦЕВ.

Смена пароля также должна производиться в случаях:

- попыток взлома пароля;

- внепланово в целях дополнительной безопасности в случаях компрометации или утери пароля сотрудником, прекращения полномочий (увольнения, перехода на другую должность и т.п.) ответственного за безопасность информационных систем.

2.8. В случае возникновения необходимости смены пароля сотрудник должен получить разрешение руководителя организации.

2.9. Организация массовой смены паролей сотрудниками при необходимости производится ответственным за безопасность информационных систем на основании соответствующего приказа руководителя организации.

2.10. Для смены пароля сотрудник организации должен ввести старый пароль и дважды ввести новый пароль. Новый пароль генерируется аналогично алгоритму создания пароля, указанному в п. 2.2 настоящей Инструкции.

2.11. Удаление пароля происходит в случаях:

- увольнения сотрудника;

- смерти сотрудника;

- ухода сотрудника в длительный отпуск.

2.12. Удаление пароля осуществляется ответственным за безопасность информационных систем на основании приказа руководителя организации.

2.13. Хранение паролей осуществляется на бумажном носителе, запечатанном в конверт, в сейфе у ответственного за безопасность информационных систем и у непосредственного руководителя сотрудника организации. В случае необходимости срочно войти в информационную систему персональных данных в отсутствие ответственного сотрудника организации конверт может быть вскрыт. О вскрытии конверта должен быть составлен акт. После использования пароль сотрудника должен быть удален и сгенерирован новый.

2.14. Сотрудникам организации, имеющим доступ к информационной системе персональных данных, запрещается записывать и хранить пароли на бумажных носителях, в файлах, электронных записных книжках и других носителях информации.

3. Ответственность при организации парольной защиты в информационных системах организации

3.1. Сотрудники организации, имеющие доступ к информационной системе персональных данных, должны быть ознакомлены под подпись с требованиями настоящей Инструкции и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение информации о пароле.