ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НА ПРЕДПРИЯТИИ ООО МФО ПРОСТОДЕНЬГИ

ЧТО ТАКОЕ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры

КАКОЙ МОЖЕТ БЫТЬ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Состояние (качество)

- Информация
- Данные
- ресурсы автоматизированной системы,
- автоматизированная система,
- информационная система предприятия

и т. п.); **Деятельность,** направленная на обеспечение защищённого состояния объекта (в этом значении чаще используется термин «защита информации»).

ОТВЕТСТВЕННОСТЬ СОТРУДНИКОВ РАБОТАЮЩИХ В АРМ

- сохранение пароля в тайне, обеспечение конфиденциальности ввода пароля с клавиатуры;
- смена пароля при первом входе в систему, смене паролей по истечении срока его действия, смена пароля при его компрометации;
- обеспечение требуемой сложности используемых паролей в соответствии с положениями настоящей Политики;
- использование в каждой ИС, к которой пользователь имеет доступ, своего уникального пароля;
- в случае компрометации (случайной или намеренной) или утери пароля пользователь должен оперативно подать заявку на изменение пароля;
- пользователь обязан незамедлительно информировать ИТ-отдел при подозрении о несанкционированном доступе третьих лиц к его учетной записи;
- пользователь несет персональную ответственность за конфиденциальность пароля и действия, выполняемые от имени учетной записи, принадлежащей ему.

ЗАПРЕЩАЕТСЯ

- устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности. Все компьютеры, подключенные к корпоративной сети, должны быть оснащены системой антивирусной защиты, утвержденной руководителем службы информационных технологий.
- блокировать антивирусное программное обеспечение;
- устанавливать другое антивирусное программное обеспечение;
- изменять настройки и конфигурацию антивирусного программного обеспечения.

ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЮ ЗАПРЕЩАЕТСЯ:

- записывать и хранить персональные данные на неучтенных установленным порядком машинных носителях информации;
- записывать, накапливать и хранить архивы, содержащие персональные данные контрагентов, на ПЭВМ;
- самостоятельно подключать к ПЭВМ какие-либо устройства и вносить изменения в состав, конфигурацию, размещение ПЭВМ;
- самостоятельно устанавливать и/или запускать (выполнять) на ПЭВМ любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей;
- осуществлять обработку персональных данных в условиях, позволяющих осуществлять их просмотр лицами, не имеющими к ним допуска, а также при несоблюдении требований по эксплуатации ПЭВМ;
- сообщать кому-либо устно или письменно личные атрибуты доступа к ресурсам ПЭВМ;
- отключать (блокировать) средства защиты информации;
- производить какие-либо изменения в подключении и размещении технических средств.
- оставлять бесконтрольно ПЭВМ с загруженными персональными данными, с установленными маркированными носителями, электронными ключами, а также распечатываемыми бумажными документами с персональными данными.

ПРАВА СОТРУДНИКОВ, РАБОТАЮЩИХ В АРМ

- Обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленных ему полномочий.

- Обращаться к обслуживающему ПЭВМ персоналу с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, установленным в ПЭВМ, а также со средствами защиты информации.