РОССИЙСКАЯ ФЕДЕРАЦИЯ
БЕЛГОРОДСКАЯ ОБЛАСТЬ

АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО РАЙОНА
«ИВНЯНСКИЙ РАЙОН»
Р А С П О Р Я Ж Е Н И Е
Поселок Ивня

09 июня 2014 г. № 250-р

Об обязанностях ответственных за обработку персональных данных сотрудников администрации Ивнянского района по обеспечению информационной безопасности при работе с автоматизированной системой

В соответствии с Федеральным законом Российской Федерации от 27 июля 2006 года №152-ФЗ «О персональных данных»:

Утвердить общие обязанности ответственных за обработку персональных данных сотрудников администрации Ивнянского района по обеспечению информационной безопасности при работе с автоматизированной системой (далее-АС).

Глава администрации района **В.А. Старченко**

УТВЕРЖДЕНЫ
распоряжением администрации
Ивнянского района

09 июня 2014г. № 250-р

Общие обязанности ответственных за обработку персональных данных сотрудников администрации Ивнянского района по обеспечению информационной безопасности при работе с автоматизированной системой (далее – АС)

Каждый ответственный за обработку персональных данных сотрудник администрации Ивнянского района, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным автоматизированной системы, несет персональную ответственность за свои действия и обязан:

1. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АС.
2. Знать и строго выполнять правила работы со средствами защиты информации, установленными на его рабочей станции (далее-РС).
3. Хранить в тайне свой пароль (пароли). В соответствии с «Инструкцией по организации парольной защиты в информационной системе персональных данных администрации Ивнянского района» с установленной периодичностью менять свой пароль (пароли).
4. Передавать для хранения установленным порядком свое индивидуальное устройство идентификации Touch Memory, личную ключевую дискету и другие реквизиты разграничения доступа только руководителю своего подразделения или ответственному за информационную безопасность в подразделении (в пенале, опечатанном своей личной печатью).
5. Если сотруднику (исполнителю) предоставлено право защиты (подтверждения подлинности и авторства) документов, передаваемых по технологическим цепочкам в АС, при помощи электронной цифровой подписи, то он дополнительно обязан соблюдать все требования «Порядка работы с ключевыми дискетами».
6. Надежно хранить и никому не передавать личную печать и использовать ее только для опечатывания пенала с личной ключевой дискетой (и другими реквизитами доступа) при передаче его на хранение ответственному за информационную безопасность своего технологического участка или руководителю подразделения.

7. Выполнять требования «Инструкции по антивирусной защите информационной ситемы персональных данных в администрации Ивнянского района» в части, касающейся действий пользователей РС АС.
8. Немедленно вызывать ответственного по защите персональных данных в локальной вычислительной сети и безопасности информационных ресурсов от внутренних и внешних угроз в администрации района и ставить в известность руководителя подразделения в случае утери персональной ключевой дискеты, индивидуального устройства идентификации Touch Memory или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

а) нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах РС или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее-НСД) к защищенной РС;

б) несанкционированных подключений неучтенных магнитных носителей информации (далее-МНИ), (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств РС;

в) отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию РС, выхода из строя или неустойчивого функционирования узлов РС или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;

г) некорректного функционирования установленных на РС технических средств защиты;

д) непредусмотренных формуляром РС отводов кабелей и подключенных устройств;

е) присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленной за ним РС в подразделении.

Ответственным за обработку персональных данных сотрудников администрации Ивнянского района категорически ЗАПРЕЩАЕТСЯ:

1. Использовать компоненты программного и аппаратного обеспечения АС администрации Ивнянского района в неслужебных целях.
2. Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные формулярами рабочих станций.
3. Осуществлять обработку конфиденциальной информации в присутствии посторонних (не допущенных к данной информации) лиц.

4. Записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных носителях информации (гибких магнитных дисках и т.п.).
5. Оставлять включенной без присмотра свою рабочую станцию (ПЭВМ), не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры).
6. Передавать кому-либо свою персональную ключевую дискету (кроме ответственного по защите персональных данных в локальной вычислительной сети и безопасности информационных ресурсов от внутренних и внешних угроз администрации района или руководителя своего подразделения установленным порядком), делать неучтенные копии ключевой дискеты (на любой другой носитель), снимать с дискеты защиту записи и вносить какие-либо изменения в файлы ключевой дискеты.
7. Использовать свою ключевую дискету для формирования цифровой подписи любых электронных документов, кроме регламентированных технологическим процессом на его рабочем месте.
8. Оставлять без личного присмотра на рабочем месте или где бы то ни было свою персональную ключевую дискету, персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения).
9. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок – ставить в известность ответственного за безопасность информации и руководителя своего подразделения.