# **Инструкция пользователю автоматизированного рабочего места**

## **Общие обязанности сотрудников Компании по обеспечению информационной безопасности при работе с АС**

Каждый сотрудник подразделений «Компании», участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным автоматизированного рабочего места (АРМ), 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 АРМ;
3. хранить в тайне свой пароль (пароли). В соответствии с «Политикой управления паролями в «Компании», утвержденной приказом №\_\_ от \_\_\_\_\_\_\_\_\_, с установленной периодичностью менять свой пароль (пароли);
4. передавать для хранения свои зарегистрированные носители информации только руководителю своего подразделения или ответственному за информационную безопасность в подразделении (в пенале, опечатанном своей личной печатью);
5. если сотруднику (исполнителю) предоставлено право подписи документов, передаваемых по технологическим каналам связи и/или сети Интернет, при помощи электронной цифровой подписи, то он дополнительно обязан соблюдать все требования «Порядка работы с ключевыми носителями»;
6. выполнять требования «Инструкции по организации антивирусной защиты в АРМ», утвержденную приказом №\_\_ от \_\_\_\_\_\_\_\_\_\_\_, в части касающейся действий пользователей АРМ;
7. немедленно вызывать ответственного за информационную безопасность в «Компании» и ставить в известность руководителя подразделения в случае при подозрении компрометации личных ключей и паролей, а также при обнаружении:

* несанкционированных (произведенных с нарушением установленного порядка)
* изменений в конфигурации программных или аппаратных средств АРМ;
* отклонений в нормальной работе системных и прикладных программных средств,
* затрудняющих эксплуатацию РС, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств, а также перебоев в системе электроснабжения;
* некорректного функционирования установленных на АРМ технических средств защиты;
* присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленной за ним РС в подразделении.

## **Сотрудникам «Компании» категорически ЗАПРЕЩАЕТСЯ:**

* 1. использовать компоненты программного и аппаратного обеспечения АРМ «Компании» 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;
  5. оставлять включенной без присмотра свою рабочую станцию, не активизировав временную блокировку операционной системы;
  6. передавать кому-либо свои зарегистрированные носители информации (кроме ответственного за информационную безопасность или руководителя своего подразделения), делать неучтенные копии на любой другой носитель;
  7. использовать свои ключи электронной подписи 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 свои зарегистрированные носители информации, содержащие защищаемую информацию (конфиденциальную информацию);
  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 информационную безопасность и руководителя своего подразделения.

# **ПАМЯТКА**

## **Выдержки из статей Уголовного кодекса РФ**

Статья 183. Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну.

Собирание сведений, составляющих коммерческую, путем похищения документов, подкупа или угроз, а равно иным незаконным способом в целях разглашения либо незаконного использования этих сведений - наказываются штрафов в размере от ста до двухсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода, осужденного за период от одного до двух месяцев либо лишением свободы на срок до двух лет.

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказываются штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, - наказываются штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительным работам на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сетей, а равно использование либо распространение таких программ или машинных носителей с такими программами - наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказывается лишением свободы на срок от трех до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, - наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, - наказывается лишением свободы на срок до четырех лет.

Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) - влечет предупреждение или наложение административного штрафа на граждан в размере от трех до пяти минимальных размеров оплаты труда; на должностных лиц - от пяти до десяти минимальных размеров оплаты труда; на юридических лиц - от пятидесяти до ста минимальных размеров оплаты труда.

• Статья 13.12. Нарушение правил защиты информации

1. Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), - влечет наложение административного штрафа на граждан в размере от трех до пяти минимальных размеров оплаты труда; на должностных лиц – от пяти до десяти минимальных размеров оплаты труда; на юридических лиц – от пятидесяти до ста минимальных размеров оплаты труда.

2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), - влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц - от десяти до двадцати минимальных размеров оплаты труда; на юридических лиц - от ста до двухсот минимальных размеров оплаты

• Статья 13.14. Разглашение информации с ограниченным доступом

Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, - влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда; на должностных лиц – от сорока до пятидесяти минимальных размеров оплаты труда