ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЮ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

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 автоматизированной системы (АС), несет персональную ответственность за свои действия и обязан:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АС;
- знать и строго выполнять правила работы со средствами защиты информации, установленными на его рабочей станции (РС);
- хранить в тайне свой пароль (пароли). В соответствии с «Инструкцией по организации парольной защиты автоматизированной системы» с установленной периодичностью менять свой пароль (пароли);
- 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);
- 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»;
- 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;
- выполнять требования «Инструкции по организации антивирусной защиты в АС _____» в части касающейся действий пользователей РС АС;
- немедленно вызывать ответственного за безопасность информации в подразделении 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:
    - нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах РС или иных фактов совершения в его отсутствие попыток несанкционированного доступа (НСД) к защищенной РС;
    - несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств РС;

- 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;
- некорректного функционирования установленных на РС технических средств защиты;
- непредусмотренных формуляром РС отводов кабелей и подключенных устройств;

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

Сотрудникам Компании категорически ЗАПРЕЩАЕТСЯ:

- использовать компоненты программного и аппаратного обеспечения АС Компании в неслужебных целях;
- 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;
- осуществлять обработку конфиденциальной информации в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных носителях информации (гибких магнитных дисках и т.п.);
- оставлять включенной без присмотра свою рабочую станцию (ПЭВМ), не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);
- передавать кому-либо свою персональную ключевую дискету (кроме ответственного за информационную безопасность 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;
- использовать свою ключевую дискету для формирования цифровой подписи любых электронных документов, кроме регламентированных технологическим процессом на его рабочем месте;
- 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);
- 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.

Выдержки из статей Уголовного кодекса РФ (в памятку пользователей АС Компании)

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

  1. Собирание сведений, составляющих коммерческую или банковскую тайну, 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.
  2. Незаконные разглашение или использование сведений, составляющих коммерческую или банковскую тайну, без согласия их владельцев, совершенные из корыстной или иной личной заинтересованности и причинившие крупный ущерб, - наказывается штрафом в размере от двухсот до пятисот минимальных окладов оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев либо лишением свободы на срок до трех лет со штрафом в размере до пятидесяти минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период до одного месяца либо без такового.

- 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 283. Разглашение государственной тайны

  1. Разглашение сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по службе или работе, если эти сведения стали достоянием других лиц, при отсутствии признаков государственной измены - наказывается арестом на срок от четырех до шести месяцев либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

- Статья 284. Утрата документов, содержащих государственную тайну

  Нарушение лицом, имеющим допуск к государственной тайне, установленных правил обращения с содержащими государственную тайну документами, а равно с предметами, сведения о которых составляют государственную тайну, если это повлекло по неосторожности их утрату и наступление тяжких последствий, - наказывается ограничением свободы на срок до трех лет, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

- Статья 293. Халатность

  Халатность, то есть неисполнение или ненадлежащее исполнение должностным лицом своих обязанностей вследствие недобросовестного или небрежного отношения к службе, если это повлекло существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства, - наказывается штрафом 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 обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок от шести месяцев до одного года, либо арестом на срок до трех месяцев.

- 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 труда с конфискацией несертифицированных средств защиты информации или без таковой.
  3. Нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, - влечет наложение административного штрафа на должностных лиц в размере от двадцати до тридцати минимальных размеров оплаты труда; на юридических лиц - от ста пятидесяти до двухсот минимальных размеров оплаты труда.
  4. Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, - влечет наложение административного штрафа на должностных лиц в размере от тридцати до сорока минимальных размеров оплаты труда; на юридических лиц - от двухсот до трехсот минимальных размеров оплаты труда с конфискацией несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, или без таковой.

- Статья 13.13. Незаконная деятельность в области защиты информации

  1. Занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна), - влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда с конфискацией средств защиты информации или без таковой; на должностных лиц - от двадцати до тридцати минимальных размеров оплаты труда с конфискацией средств защиты информации или без таковой; на юридических лиц - от ста до двухсот минимальных размеров оплаты труда с конфискацией средств защиты информации или без таковой.
  2. Занятие видами деятельности, связанной с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну без лицензии, - влечет наложение административного штрафа на должностных лиц в размере от сорока до пятидесяти минимальных размеров оплаты труда; на юридических лиц - от трехсот до четырехсот минимальных размеров оплаты труда с конфискацией созданных без лицензии средств защиты информации, составляющей государственную тайну, или без таковой.

- 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.