# ИНСТРУКЦИЯ
# ПОЛЬЗОВАТЕЛЯ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА (АРМ)

## 1. Общие обязанности сотрудников по обеспечению информационной безопасности при работе на АРМ

Каждый сотрудник, 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:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АРМ;
- знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ;
- хранить в тайне свой пароль (пароли). В соответствии с “Инструкцией по организации парольной защиты” с установленной периодичностью менять свой пароль (пароли);
- выполнять требования “Инструкции по организации антивирусной защиты” в части касающейся действий пользователей;
- немедленно ставить в известность администратора защиты информации при подозрении компрометации паролей;
- вызывать специалиста организации** при обнаружении:
    - фактов совершения в его отсутствие попыток несанкционированного доступа (НСД) к АРМ;
    - 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 АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисковода, и т.п.), а также перебоев в системе электроснабжения;
    - некорректного функционирования установленных на АРМ технических средств защиты;
    - непредусмотренных отводов кабелей и подключенных устройств;
- присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленного за ним АРМ в подразделении.

**Пользователям категорически ЗАПРЕЩАЕТСЯ:**

- использовать компоненты программного и аппаратного обеспечения АРМ в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств АРМ или устанавливать дополнительно любые программные и аппаратные средства;
- осуществлять обработку информации в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить информацию (содержащую сведения конфиденциального характера) на неучтенных носителях информации (гибких магнитных дисках и т.п.);
- оставлять включенной без присмотра ПЭВМ, не активизировав средства защиты от несанкционированного доступа к данным (временную блокировку экрана);
- оставлять без личного присмотра на рабочем месте (или где бы то ни было) машинные носители, распечатки и другие носители, содержащие защищаемую информацию (сведения конфиденциального характера);
- 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 администратора безопасности информации.

## ИНСТРУКЦИЯ ПО ПРОВЕДЕНИЮ АНТИВИРУСНОГО КОНТРОЛЯ В *ОРГАНИЗАЦИИ**

1. Настоящая Инструкция предназначена для пользователей, хранящих и обрабатывающих информацию на автоматизированных рабочих местах (АРМ) локально-вычислительной сети *организации*.

2. Антивирусный контроль проводится в целях обеспечения антивирусной защиты на АРМ ЛВС.

3. Установку и настройку антивирусных пакетов, а также периодическую проверку всех программ, установленных на АРМ пользователей осуществляет специалист организации (указать должность).

4. На АРМ запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

5. К применению на АРМ допускаются только лицензионные антивирусные средства.

6. Пользователь АРМ при работе с гибкими магнитными носителями информации обязан перед началом работы осуществить проверку гибких магнитных дисков (ГМД) на предмет отсутствия компьютерных вирусов.

7. Во время работы запрещается отключать средства антивирусной защиты.

8. Пользователь ЛВС должен ежедневно проверять жесткие магнитные диски (ЖМД) АРМ на наличие вредоносных программ.

9. При обнаружении компьютерного вируса пользователь обязан немедленно осуществить лечение зараженных файлов путем выбора соответствующего пункта меню антивирусной программы и поставить в известность специалиста организации.

10. Техник проводит, в случае необходимости, повторное лечение зараженных файлов путем выбора соответствующего пункта меню антивирусной программы и после этого вновь проводит антивирусный контроль.

11. В случае обнаружения на ГМД нового вируса, не поддающегося лечению, пользователь обязан прекратить использование ГМД.

12. В случае обнаружения на ЖМД не поддающегося лечению вируса, техник обязан поставить в известность администратора безопасности информации, прекратить работу на АРМ и в возможно короткие сроки обновить пакет антивирусных программ.

13. Периодическое обновление антивирусных пакетов на сервере осуществляют администраторы безопасности информации организации.

## ИНСТРУКЦИЯ
## ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ

1. Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей на автоматизированных рабочих местах (АРМ) сотрудников организации.

2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей на компьютерах пользователей возлагается на специалиста организации.

3. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей на серверах возлагается на администраторов безопасности информации.

4. Личный пароль должен генерироваться и распределяться централизованно либо выбираться пользователем автоматизированной системы самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 6 символов;

- пароль не должен включать в себя легко вычисляемые сочетания символов, а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

5. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
6. Личный пароль пользователь не имеет права сообщать никому.
7. Владелец пароля должен быть ознакомлен под роспись с перечисленными выше требованиями и предупрежден об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.
8. В случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п. технологической необходимости использования имен и паролей сотрудника (исполнителя) в его отсутствие, сотрудник обязан сразу же сменить свой пароль на новый.
9. Плановая смена паролей пользователя должна проводиться регулярно, не реже одного раза в 6 месяцев.
10. Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на другую работу внутри предприятия и т.п.) должна производиться немедленно после окончания последнего сеанса работы данного пользователя с системой администратором безопасности информации.
11. В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии с п.7 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.
12. Пароли пользователей (вместе с именами соответствующих учетных записей) должны храниться в запечатанном конверте в сейфе администратора безопасности информации.
13. Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе.
14. Пользователю следует помнить, что при смене пароля на компьютере пользователя доступ к сетевым ресурсам под новым паролем без соответствующей смены пароля на сервере невозможен.

* *Организация* – Ваше образовательное учреждение

** *Специалист организации* – технический специалист – ответственный за техническое обеспечение защиты информации