

## **ИНСТРУКЦИЯ**

пользователей и технология обработки конфиденциальной информации  
на объектах информатизации – автоматизированных системах  
ТОГАПОУ «Аграрно-промышленный колледж»

### **1. Общие положения**

1.1. Настоящая Инструкция пользователей и технология обработки конфиденциальной информации в автоматизированных системах ТОГАПОУ «Аграрно-промышленный колледж» (далее – Инструкция) разработана в дополнение к Положению об организации и проведении работ по обеспечению безопасности конфиденциальной информации при их автоматизированной обработке в информационных системах и определяет требования, права, обязанности, а так же порядок реализации задач и функций пользователей автоматизированной системы (далее – АС) при исполнении ими своих должностных обязанностей при обработке конфиденциальной информации.

Перед началом обработки информации пользователи автоматизированной системы должны ознакомиться с требованиями настоящей инструкции, а также эксплуатационной документацией на используемые средства защиты информации.

Первичный доступ пользователей к автоматизированной обработке конфиденциальной информации, в том числе персональных данных, в АС, осуществляется после проведения Администратором защиты информации (далее – Администратор) инструктажа по правилам работы в АС и порядку применения средств защиты информации.

1.2. Объект информатизации (далее – ОИ) разрешается использовать для обработки информации конфиденциального характера при соблюдении следующих условий:

- вспомогательные технические средства и системы (далее – ВТСС), провода и кабели располагать от основных технических средств и систем (далее – ОТСС) в соответствии с Предписаниями на эксплуатацию;
- подключение ОТСС осуществлять с использованием штатных кабелей;
- право работы на ОИ предоставляется Администратору и пользователям;
- каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным, несет персональную ответственность за свои действия.

### **2. Обязанности пользователей автоматизированной системы**

2.1. Пользователи АС, обязаны строго соблюдать установленные правила работы на комплексах средств автоматизации и несут персональную ответственность за неукоснительное выполнение требований и мероприятий по защите информации на своих автоматизированных рабочих местах.

2.2. Пользователи обязаны:

- знать и выполнять требования нормативных правовых документов по обеспечению информационной безопасности, а также настоящей Инструкции, организационно-распорядительных и эксплуатационных документов АС;
- знать и соблюдать установленные требования по режиму обработки конфиденциальной информации, учету и хранению машинных носителей информации;
- при работе в АС использовать только учтенные установленным порядком машинные носители информации, штатное общесистемное, прикладное и специальное программное обеспечение;

- экран видеомонитора в помещении располагать во время работы так, чтобы исключалась возможность ознакомления посторонними лицами с отображаемой на нём информацией;
- при выходе из помещения в течение рабочего дня выключать или блокировать рабочую станцию;
- соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с конфиденциальной информацией, в том числе персональными данными при их обработке;
- уметь пользоваться средствами антивирусной защиты и при необходимости проверять ПЭВМ на наличие вредоносных программ – «вирусов»;
- осуществлять проверку файлов на наличие вредоносных программ перед началом обработки информации, хранящейся на съемных машинных носителях информации.
- осуществлять антивирусный контроль ПЭВМ не реже одного раза в неделю;
- перед началом работы получить у Администратора свои учётные данные (логин, пароль, идентификатор), надёжно запоминать и хранить в тайне
- докладывать Администратору о фактах компрометации пароля, несанкционированного доступа со стороны других пользователей, случаях утечки и нарушения целостности информации, обрабатываемой в АС, нарушениях целостности компонентов системы защиты информации;
- информировать Администратора о нарушениях установленной технологии обработки защищаемой информации или нарушениях функционирования средств и систем защиты информации.

### 2.3. Пользователям АС запрещается:

- осуществлять обработку информации конфиденциального характера на автоматизированном рабочем месте (далее – АРМ) без выполнения мероприятий по защите информации;
- обрабатывать информацию с грифом, выше установленного для АС;
- оставлять без контроля АРМ до окончания сеанса работы без его блокировки;
- оставлять во время работы съемные носители с конфиденциальной информацией без присмотра, передавать их посторонним лицам;
- сообщать устно или письменно другим лицам личные имена учётных записей и пароли к ним;
- осуществлять ввод паролей, допуская возможность ознакомления с ними посторонних лиц;
- сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам АС;
- хранить пароли на любых носителях (как бумажных, так и электронных);
- самовольно вносить изменения в состав, конструкцию и размещение аппаратного обеспечения АС, открывать крышки устройств и блоков технических средств объекта информатизации;
- устанавливать и использовать при работе в АС программное обеспечение, не входящее в перечень средств, указанных в документации на АС,
- изменять установленный алгоритм функционирования технических и программных средств;
- осуществлять электропитание и заземление основных технических средств и систем от нештатных сетей электропитания и заземления;
- обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационным ресурсам обработки информации;
- создавать или модифицировать программное обеспечение для АРМ или вносить изменения в существующее программное обеспечение, приводящее к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы АС, а равно использование либо распространение таких программ или машинных носителей с такими программами;

- отключать (блокировать), тиражировать, распространять (передавать) и модифицировать используемые в составе АС средства защиты информации;
- допускать к результатам решения задач (в том числе промежуточным) лиц, не имеющих к ним прямого отношения;
- пытаться работать от имени других пользователей;
- уничтожать, копировать или производить какие-либо другие действия над документами, программами, файлами, базами данных других пользователей без их разрешения;
- использовать для обработки и хранения защищаемой информации неучтенные установленным порядком машинные носители информации (оптические диски, флеш-накопители, съёмные (внешние) жёсткие диски, дискеты и т.п.);
- хранить на учтенных носителях информации программы и данные, не относящиеся к рабочей информации;
- хранить носители с конфиденциальной информацией вблизи сильных источников электромагнитных излучений и прямых солнечных лучей;
- работать на средствах АС при обнаружении компьютерных вирусов или каких-либо неисправностей;
- осуществлять попытки НСД к конфиденциальной информации, в том числе персональным данным АС, в частности производить подбор пароля другого пользователя, превышать свои полномочия при работе на АРМ;
- проводить работы по исследованию обнаруженных компьютерных вирусов;
- привлекать посторонних лиц для производства ремонта ОТСС без согласования со специалистом по защите информации
- производить иные действия, ограничения на исполнение которых предусмотрены требованиями нормативных актов.

#### 2.4. Пользователь имеет право:

- доступа к аппаратным и программным средствам АС, необходимым для исполнения его должностных обязанностей, и в защищаемые помещения, в которых они расположены;
- доступа к информационным ресурсам в соответствии с таблицей разграничения доступа (матрицей доступа) АС. Для каждой категории пользователей любой ресурс имеет свои значения атрибутов управления доступом, используемые при определении прав доступа пользователя к ресурсу;
- обращаться к Администратору по вопросам защиты информации;
- обращаться к Администратору с просьбой об оказании технической и методической помощи по обеспечению безопасности обрабатываемой в АС информации.

#### 2.5. Пользователь несет ответственность:

- за невыполнение и/или несвоевременное, некачественное, халатное выполнение своих должностных обязанностей;
- за несоблюдение действующих инструкций, приказов и распоряжений;
- за разглашение защищаемой информации, ставшей ему известной в ходе исполнения своих должностных обязанностей;
- за нарушение правил внутреннего трудового распорядка, трудовой дисциплины, правил техники безопасности и противопожарной безопасности;
- за правонарушения, совершенные в процессе осуществления своей деятельности в пределах, определенным действующим административным, уголовным и гражданским законодательством Российской Федерации.
- за причинение материального ущерба в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

### **3. Организация парольной защиты при работе на объекте информатизации**

3.1. Личные пароли доступа к объекту информатизации, системе защиты от несанкционированного доступа (НСД), выдаются пользователям Администратором, и при этом необходимо руководствоваться следующими требованиями:

- длина пароля должна быть не менее 6-ти буквенно-цифровых символов;

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера телефонов, автомобилей, адреса места жительства, наименования автоматизированной системы, общепринятые сокращения, и другие данные, которые могут быть подобраны злоумышленником путем анализа информации об ответственном исполнителе);

- не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

- не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре;

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

- в числе символов пароля, обязательно должны присутствовать буквы в верхнем и нижнем регистрах, а также цифры;

- не использовать ранее использованные пароли.

3.2. Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию;

- своевременно сообщать Администратору обо всех нештатных ситуациях, нарушениях работы подсистем защиты от НСД, возникающих при работе с паролями.

3.3. При организации парольной защиты запрещается:

- записывать свои пароли в очевидных местах, внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.д.;

- хранить пароли в записанном виде на отдельных листах бумаги;

- сообщать посторонним лицам свои пароли, а также сведения о применяемой системе защиты от НСД.

#### **4. Порядок применения парольной защиты**

4.1. Полная плановая смена паролей в АС проводится один раз в 3 месяца.

4.2. Удаление (в т.ч. внеплановая смена) личного пароля любого пользователя АС должна производиться в следующих случаях:

- в случае подозрения на дискредитацию пароля;

- по окончании срока действия;

- в случае прекращения полномочий (увольнение, переход в другое структурное подразделение) пользователя после окончания последнего сеанса работы данного пользователя с системой;

- по указанию Администратора.

4.3. Смена пароля осуществляется Администратором.

4.4. Для предотвращения доступа к конфиденциальной информации, находящейся в ПЭВМ, минуя ввод пароля, пользователь во время перерыва в работе обязан осуществить блокирование системы или выключить ПЭВМ.

4.5. Порядок применения (смены) паролей при работе на ПЭВМ, оборудованных системой защиты от НСД, приведен в эксплуатационной документации на СЗИ.

#### **5. Порядок применение средств антивирусной защиты**

5.1. Пользователь должен контролировать запуск и работу средства антивирусной защиты (антивирусного монитора), осуществляющего постоянные проверки файлов при операциях чтения/записи.

5.2. Обязательному входному антивирусному контролю подлежит любая информация (в том числе носители информации), поступающая на ПЭВМ, входящие в состав АС, а именно: программные средства общего и специального назначения, любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по каналам передачи данных, информация на съемных машинных носителях (магнитных дисках, оптических дисках, флеш-накопителях и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед ее отправкой (записью на съемный носитель).

5.3. Периодическая проверка жестких дисков на отсутствие программных вирусов должна проводиться не реже одного раза в неделю. Обязательная проверка используемых в работе съёмных носителей информации должна осуществляться перед началом работы с ними.

5.4. При повреждении программных средств и информационных массивов программными вирусами должны выполняться мероприятия по восстановлению целостности поврежденных данных.

5.5. Обновление баз данных вирусных описаний и средств антивирусной защиты, используемых для защиты АРМ, должно осуществляться Администратором без участия пользователей.

5.6. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно или совместно с Администратором должен провести внеочередной антивирусный контроль своей ПЭВМ.

5.7. В случае обнаружения зараженных компьютерными вирусами файлов пользователи обязаны:

- приостановить работу;
- принять меры по локализации программного вируса (отключить ПЭВМ от локальной вычислительной сети);
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов Администратора, руководителя подразделения, владельца зараженных файлов;
- совместно с Администратором и владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- по возможности провести лечение зараженного файла. В случае невозможности вылечить зараженный файл, необходимо поместить его в карантин, выполнить процедуру по восстановлению незараженной копии исходного файла из имеющегося архива.

5.8. Непосредственную ответственность за соблюдение в повседневной деятельности установленных настоящим порядком правил антивирусной защиты информации и требований настоящей Инструкции несут работники, за которыми закреплены соответствующие рабочие станции.

## **6. Технология обработки конфиденциальной информации**

6.1. При первичном допуске к работе на ПЭВМ пользователь должен знакомится с требованиями руководящих, нормативно-методических и организационно-распорядительных документов по вопросам автоматизированной обработки информации, изучает инструкцию пользователя системы защиты от НСД, получает персональный идентификатор или личный текущий пароль у Администратора.

6.2. Пользователь включает ПЭВМ, визуально убеждается в исправности и нормальном функционировании ПЭВМ.

6.3. В процессе работы пользователь создает файлы и массивы информации на ПЭВМ с применением операционной системы.

6.4. При необходимости вывод конфиденциальной информации из ПЭВМ осуществляется следующим образом:

- копированием на учетные носители;
- на печатающие устройства.

## **7. Заключение**

7.1. Настоящая Инструкция доводится до пользователей автоматизированной системы под подпись.

7.2. Настоящая Инструкция вступает в силу с момента её утверждения руководителем ТОГАПОУ «Аграрно-промышленный колледж».