

Инструкция пользователю служебной ПЭВМ органов и организаций прокуратуры Российской Федерации

Генеральная прокуратура Российской Федерации · № 565

• Утратил силу 16.10.2026

(утв. Приказом Генпрокуратуры России от 08.09.2016 № 565)

Утверждена
Приказом
Генерального прокурора
Российской Федерации

от 8 сентября 2016 г. № 565

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЮ СЛУЖЕБНОЙ ПЭВМ ОРГАНОВ И ОРГАНИЗАЦИЙ ПРОКУРАТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

1. Общие положения и область применения

1.1. Инструкция пользователю служебной ПЭВМ органов и организаций прокуратуры Российской Федерации (далее – Инструкция) разработана на основании требований инструкций по эксплуатации технических и программных средств производителя, Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организация работы».

1.2. Настоящая Инструкция распространяется на все виды работ на персональных электронно-вычислительных машинах (далее – ПЭВМ, компьютер), регламентирует правила использования защищаемой информации баз данных, порядок допуска пользователей ПЭВМ к работе в составе локальной вычислительной сети (далее – ЛВС).

1.3. Положения Инструкции устанавливаются на единой основе в Генеральной прокуратуре Российской Федерации, прокуратурах субъектов Российской Федерации, прокуратурах городов и районов, других приравненных к ним

территориальных и специализированных прокуратурах, в Академии Генеральной прокуратуры Российской Федерации (далее – органы и организации прокуратуры Российской Федерации) правила пользования служебной ПЭВМ.

1.4. Ответственность за выполнение требований Инструкции возлагается на руководителей структурных подразделений, а в прокуратурах городского и районного звена – на руководителей органов прокуратуры.

1.5. Пользователи ПЭВМ знакомятся с Инструкцией под роспись при приеме на работу.

2. Основные положения гигиенических требований к организации работы с ПЭВМ

2.1. Санитарно-эпидемиологические правила и нормативы (далее – санитарные правила) действуют на всей территории Российской Федерации и устанавливают санитарно-эпидемиологические требования к персональным электронно-вычислительным машинам, копировальным аппаратам и условиям труда.

2.2. Требования санитарных правил направлены на предотвращение неблагоприятного воздействия на здоровье человека вредных факторов производственной среды и трудового процесса при работе с ПЭВМ и на копировально-множительных аппаратах.

2.3 Требования санитарных правил распространяются на условия и организацию работы с:

ПЭВМ и копировально-множительным оборудованием;

персональными и портативными вычислительными электронными цифровыми машинами;

периферийными устройствами вычислительных комплексов (принтеры, сканеры, клавиатуры, внешние модемы, электрические компьютерные сетевые устройства, устройства хранения информации, блоки бесперебойного питания и пр.);

устройствами отображения информации (видеодисплейные терминалы всех типов) и копировально-множительным оборудованием.

2.4. Контроль выполнения санитарных правил возложен на органы и учреждения, осуществляющие федеральный государственный санитарно-эпидемиологический надзор в соответствии с Федеральным законом от 30.03.1999 № 52-ФЗ «О санитарно-эпидемиологическом благополучии населения».

3. Технические средства и стандартизация программного обеспечения

3.1 В целях настоящей Инструкции используются следующие основные понятия:

машинный носитель информации — сменный носитель данных, предназначенный для записи и считывания данных;

съёмный носитель информации — устройство, предназначенное для записи и хранения данных;

технические средства — все оборудование, включая носители данных, предназначенное для автоматизированной обработки информации, а также аппаратные средства и программные средства;

программные средства (нематериальные объекты) — системное программное обеспечение, прикладные программы, а также средства экранного и печатного представления (пользовательский интерфейс);

регламентные работы с техническими средствами — комплекс организационно-технических мероприятий, в том числе по обеспечению аппаратных средств компонентами и оборудованием, предназначенным для обеспечения эффективности работы, необходимого уровня безопасности информации.

3.2 Ответственными за выполнение регламентных работ и первоначальной настройки технических средств являются:

в Генеральной прокуратуре Российской Федерации — управление информационно-технологического обеспечения и связи Главного управления обеспечения деятельности органов и организаций прокуратуры;

в управлениях Генеральной прокуратуры Российской Федерации в федеральных округах, нижестоящих прокуратурах, в Академии Генеральной прокуратуры Российской Федерации — уполномоченные работники структурных подразделений.

3.3. На всех рабочих станциях и мобильных компьютерах используются лицензионные копии операционной системы семейства Windows, не старше Windows XP. Установка других операционных систем допускается в следующих случаях:

аппаратная конфигурация рабочей станции не отвечает минимальным требованиям операционной системы Windows;

программное обеспечение, необходимое пользователю для выполнения должностных обязанностей, не совместимо с операционной системой Windows.

Решение об установке другой операционной системы принимает управление информационно-технологического обеспечения и связи Главного управления обеспечения деятельности органов и организаций прокуратуры и согласовывает с руководителем структурного подразделения органа или организации прокуратуры.

3.4. Установка, переустановка, изменение аппаратной конфигурации ПЭВМ, ЛВС, ключевых параметров операционных систем (в том числе затрагивающих вопросы информационной безопасности) пользователем недопустима.

3.5. Настройка принтеров, копировальных аппаратов с функцией принтера для коллективного пользования в компьютерной сети производится работником структурного подразделения, обслуживающим информационную систему по заявке руководителя подразделения.

3.6. Обладателем всей информации, хранимой и обрабатываемой на служебных ПЭВМ, является соответствующий орган или организация прокуратуры Российской Федерации.

4. Правила регистрации пользователей ПЭВМ в ЛВС и наделение их полномочиями доступа к ресурсам информационной системы органов прокуратуры

4.1. С целью соблюдения персональной ответственности за свои действия каждому пользователю ПЭВМ, допущенному к работе в ЛВС, присвоено персональное уникальное имя (учетная запись пользователя), под которым он регистрируется и работает в сети. Использование несколькими работниками при работе в ЛВС одного и того же имени пользователя («группового имени») запрещается.

4.2. Процедура регистрации пользователя для работника органа прокуратуры и предоставления ему (или изменения) прав доступа к ресурсам информационной системы инициируется заявкой руководителя подразделения, в котором работает данный работник.

4.3 В заявке указываются:

содержание запрашиваемых изменений (регистрация нового пользователя, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам информационной системы ранее зарегистрированного пользователя, использование сетевого принтера для печати документов);

должность (с полным наименованием подразделения), фамилия, имя и отчество работника;

полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач на конкретных рабочих станциях компьютерной сети);

срок начала и окончания действия доступа.

4.4. Начальник структурного подразделения, отвечающий за техническую поддержку информационных систем, рассматривает представленную заявку на внесение необходимых изменений в списки пользователей соответствующих подсистем.

4.5. Работнику, зарегистрированному в качестве нового пользователя системы, сообщается соответствующее ему имя пользователя, выдается начальное значение пароля, которое он обязан сменить при первом же входе в систему.

4.6. Подключение пользователей к сети Интернет производится по заявке руководителя структурного подразделения.

4.7. При передаче технических средств между пользователями производится полная очистка данных силами ответственного подразделения (работника). Те же действия производятся при списании технических средств.

4.8. Передача служебной информации ограниченного распространения в рамках служебной деятельности по беспроводным каналам связи запрещена.

5. Правила организации парольной защиты информационной системы органов прокуратуры

5.1 Личные пароли выбираются пользователями компьютерной сети самостоятельно с учетом следующих требований:

длина пароля должна быть не менее 8 символов;

среди символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы;

пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих станций и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;

личный пароль пользователь не имеет права сообщать никому;

смена паролей пользователей должна проводиться регулярно, не реже одного раза в месяц.

5.2. В случае прекращения полномочий пользователя (увольнение, переход на другую должность и т.п.) сразу после окончания последнего сеанса работы с системой должны производиться внеплановая смена личных паролей и удаление учетной записи пользователя ПЭВМ, ЛВС на основании письменного указания начальника структурного подразделения.

5.3. В случае компрометации (утери, передачи другому лицу) личного пароля пользователя информационной системы должна быть немедленно произведена внеплановая смена личного пароля. Ответственность за своевременную смену пароля лежит на начальнике структурного подразделения.

5.4. Хранение пользователями ПЭВМ значений своих действующих паролей на бумажном носителе допускается только в опечатанном владельцем пароля сейфе.

6. Правила организации антивирусной защиты

6.1. К использованию в информационной системе органов прокуратуры допускаются только лицензионные антивирусные средства, централизованно

закупленные и рекомендованные к применению управлением информационно-технологического обеспечения и связи Главного управления обеспечения деятельности органов и организаций прокуратуры.

6.2. Установка средств антивирусной защиты на ПЭВМ, серверах ЛВС осуществляется ответственным подразделением (работником) в соответствии с руководством по настройке применяемого средства. Запрещается самостоятельная установка пользователем средств антивирусной защиты на ПЭВМ.

6.3. В начале работы при включении ПЭВМ (для серверов ЛВС – при перезапуске), а также при первом доступе к файлам в автоматическом режиме проводится их антивирусный контроль.

6.4. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, CD-ROM, USB-накопителях и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенном автономном компьютере.

6.5. 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 ПЭВМ самостоятельно или вместе с ответственным за выполнение регламентных работ и первоначальной настройки технических средств (пункт 3.2 настоящей Инструкции) должен провести внеочередной антивирусный контроль своей рабочей станции для определения факта наличия или отсутствия компьютерного вируса.

6.6. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь ПЭВМ обязан:

приостановить работу;

немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя подразделения, владельца зараженных файлов, смежные подразделения, использующие эти файлы в работе, а также проинформировать управление информационно-технологического обеспечения и связи Главного управления обеспечения деятельности органов и организаций прокуратуры.

6.7. Периодический контроль состояния антивирусной защиты в компьютерной сети, соблюдения установленного порядка антивирусного контроля и выполнения требований настоящей Инструкции пользователями ПЭВМ подразделений Генеральной прокуратуры Российской Федерации осуществляется специалистами управления информационно-технологического обеспечения и связи Главного управления обеспечения деятельности органов и организаций прокуратуры, в других органах и организациях прокуратуры – уполномоченными специалистами соответствующего подразделения.

7. Обязанности пользователя ПЭВМ

7.1 Пользователь ПЭВМ обязан:

при работе со служебной информацией ограниченного распространения исключать присутствие в помещении, где расположены средства вычислительной техники, не допущенных к обрабатываемой информации лиц, а также располагать во время работы экран видеомонитора так, чтобы отображаемая на нем информация была недоступна для просмотра посторонним лицам;

соблюдать правила работы со средствами защиты информации, а также установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с информацией ограниченного использования при ее обработке;

оповещать непосредственного руководителя обо всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в ПЭВМ;

не допускать «загрязнения» ПЭВМ посторонними программными средствами;

знать способы выявления нештатного поведения используемых операционных систем и пользовательских приложений, меры предотвращения ухудшения ситуации;

знать и соблюдать правила поведения в экстренных ситуациях, порядок действий при ликвидации последствий аварий;

помнить личные пароли и персональные идентификаторы;

знать штатные режимы работы программного обеспечения, пути проникновения и распространения компьютерных вирусов;

при применении внешних носителей информации перед началом работы проводить их проверку на наличие компьютерных вирусов.

7.2 Пользователю ПЭВМ запрещается:

создавать и хранить на ПЭВМ не предназначенные для обработки сведения, составляющие государственную тайну, документы с грифом «секретно», «совершенно секретно» и «особой важности»;

записывать и хранить служебную информацию ограниченного распространения на не учтенных в установленном порядке машинных носителях информации;

удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности;

самостоятельно подключать к ПЭВМ какие-либо устройства, кроме съемных носителей информации, а также вносить изменения в состав, конфигурацию и размещение ПЭВМ;

самостоятельно устанавливать или запускать на ПЭВМ любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей;

осуществлять обработку служебной информации ограниченного распространения в условиях, позволяющих просматривать ее лицам, не имеющим к ней допуска, а также нарушающих требования по эксплуатации ПЭВМ;

сообщать кому-либо устно или письменно личные атрибуты доступа к ресурсам ПЭВМ;

отключать (блокировать) средства защиты информации; производить какие-либо изменения в подключении и размещении технических средств;

производить иные действия, ограничения на исполнение которых предусмотрены утвержденными регламентами и инструкциями;

бесконтрольно оставлять ПЭВМ с информацией ограниченного использования, установленными маркированными носителями, электронными ключами и выведенными на печать документами, содержащими информацию ограниченного использования.

8. Ответственность пользователей информационной системы

Пользователи ПЭВМ и ЛВС за нарушение положений настоящей Инструкции несут ответственность в соответствии с действующим законодательством.
