Утверждаю
Заместитель
Главы Администрации
Смоленской области
Председатель комиссии
по защите информации
в компьютерных и
телекоммуникационных системах
Администрации
Смоленской области
28.01.2002

ИНСТРУКЦИЯ
И ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РУКОВОДИТЕЛЯМИ СОТРУДНИКАМИ СТРУКТУРНЫХ ПОДРАЗДЕЛЕНИЙ АДМИНИСТРАЦИИ СМОЛЕНСКОЙ ОБЛАСТИ ПРИ ИСПОЛЬЗОВАНИИ В РАБОТЕ ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРОВ, ИМЕЮЩИХ ДОСТУП К ИНФОРМАЦИОННЫМ РЕСУРСАМ ИНТРАНЕТ-СЕТИ АДМИНИСТРАЦИИ СМОЛЕНСКОЙ ОБЛАСТИ И ИНТЕРНЕТ

1. Общие положения

1.1. Настоящая Инструкция разработана в соответствии с Положением о системе защиты информации в компьютерных и телекоммуникационных системах Администрации Смоленской области, утвержденным постановлением Главы администрации Смоленской области от 30.03.98 N 135, и определяет основные обязанности и ответственность руководителей и сотрудников структурных подразделений Администрации Смоленской области - пользователей персональных компьютеров (ПК), имеющих доступ к информационным ресурсам Интранет-сети Администрации Смоленской области и Интернет.

1.2. Основная цель обеспечения информационной безопасности - предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации в компьютерных и телекоммуникационных системах администрации Смоленской области.

1.3. Методическое руководство работой пользователей ПК, организацию антивирусного контроля, установку средств антивирусного контроля на ПК подразделения и настройку их параметров осуществляет ответственный (уполномоченный) за обеспечение информационной безопасности в структурном подразделении Администрации Смоленской области.

1.4. Ответственный за обеспечение информационной безопасности назначается приказом руководителя подразделения из числа наиболее квалифицированных его сотрудников в области компьютерных технологий и подчиняется непосредственно руководителю подразделения, в штате которого он состоит.

1.5. Контроль за выполнением требований настоящей Инструкции в структурных подразделениях Администрации Смоленской области осуществляется Комитетом по информационным ресурсам и телекоммуникациям Смоленской области.

2. Обязанности

2.1. Руководитель структурного подразделения Администрации Смоленской области для обеспечения информационной безопасности при использовании в работе структурного подразделения ПК, имеющих доступ к информационным ресурсам Интранет-сети Администрации Смоленской области и Интернет, обязан:

2.1.1. Организовывать и контролировать вопросы информационной безопасности в структурном подразделении в соответствии с Законом Российской Федерации от 20.02.95 N 24-ФЗ "Об информации, информатизации и защите информации", Положением о системе защиты информации в компьютерных и телекоммуникационных системах администрации Смоленской области, утвержденным постановлением Главы администрации Смоленской области от 30.03.98 N 135, и настоящей Инструкцией.

2.1.2. Для исключения возможности бесконтрольной работы пользователей ПК в Интернет и предотвращения утечки конфиденциальной информации обязан:

а) Издать соответствующий распорядительный документ, предусмотрев в нем:

- круг лиц, допущенных к работе в сети Интернет;
- назначение ответственного лица за обеспечение информационной безопасности при использовании ПК;
- подготовку компьютера, предназначенного для работы в сети Интернет, к работе в автономном режиме с отключением его от локальных и глобальных сетей и проверкой на предмет отсутствия

конфиденциальной информации. При подключении к коммутируемому каналу связи пользователь получает в Комитете по информационным ресурсам и телекоммуникациям Смоленской области сетевое имя и пароль, которые являются конфиденциальными, разглашение которых кому бы то ни было, включая других работников Администрации Смоленской области, не допускается;

- регистрацию в специальном журнале полученной и переданной информации с указанием времени начала и окончания работы в сети Интернет;

- антивирусный контроль всей информации, полученной и передаваемой по сети Интернет;

- ознакомление под роспись лиц, допущенных к работе в сети Интернет, с перечисленными выше требованиями и предупреждение об ответственности за использование доступа в сеть Интернет в неслужебных целях, а также о неразглашении парольной информации.

б) Направить в Комитет по информационным ресурсам и телекоммуникациям Смоленской области копию указанного распорядительного документа.

2.2. Ответственный (уполномоченный) за обеспечение информационной безопасности в подразделении обязан:

2.2.1. Знать и выполнять требования настоящей Инструкции и других документов по обеспечению информационной безопасности, а также обеспечивать постоянный контроль за их выполнением сотрудниками подразделения при использовании в работе подразделения ПК.

2.2.2. Немедленно сообщать руководителю подразделения и в Комитет по информационным ресурсам и телекоммуникациям Смоленской области об имевших место в подразделении попытках несанкционированного доступа к информации, а также принимать необходимые меры по их недопущению.

2.2.3. Знать перечень компьютеров в подразделении и перечень задач, решаемых с их использованием.

2.2.4. Обеспечить заполнение и ведение формуляров на ПК в подразделении по форме, указанной в приложении N 1 (не приводится).

2.2.5. Присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию компьютеров в подразделении.

2.2.6. Обеспечить соблюдение требований по обеспечению информационной безопасности при проведении технического обслуживания и ремонтных работ ПК.

2.2.7. Проводить инструктаж сотрудников подразделения по правилам работы с используемыми аппаратно-программными средствами.

2.2.8. Предоставлять сотрудникам Комитета по информационным ресурсам и телекоммуникациям Смоленской области необходимую информацию в части возложенных на него полномочий и обязанностей в пределах своей компетенции.

2.2.9. Осуществлять повседневный контроль за действиями пользователей подразделения при работе с паролями, соблюдением порядка их смены, хранения и использования.

2.3. Сотрудники структурных подразделений Администрации Смоленской области - пользователи ПК, имеющие доступ к информационным ресурсам Интранет-сети Администрации Смоленской области и Интернет, обязаны:

2.3.1. Знать и соблюдать требования настоящей Инструкции и других документов по информационной безопасности при работе с ПК, имеющими доступ к информационным ресурсам Интранет-сети Администрации Смоленской области и Интернет.

2.3.2. Знать и уметь правильно использовать то аппаратно-программное обеспечение, которое установлено на его ПК, а также строго выполнять правила работы со средствами защиты информации, установленными на них.

2.3.3. Хранить в тайне свой пароль (пароли).

2.3.4. Выполнять следующие требования по антивирусному контролю:

а) Антивирусный контроль всех дисков и файлов ПК должен проводиться ежедневно в начале работы при их загрузке в автоматическом режиме;

б) К использованию в структурных подразделениях Администрации Смоленской области допускаются только лицензионные антивирусные средства, согласованные с Комитетом по информационным ресурсам и телекоммуникациям Смоленской области;

в) Обновление антивирусных баз должно проводиться в соответствии с периодичностью, указанной в руководствах по применению конкретных антивирусных средств;

г) В процессе работы 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, лентах, CD-ROM и т.п.). Разархивирование и контроль входящей информации должен проводиться непосредственно после ее приема. Контроль исходящей информации должен проводиться непосредственно перед архивированием и отправкой (записью на съемный носитель);

д) Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц;

е) Устанавливаемое (изменяемое) на ПК программное обеспечение должно быть предварительно

проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения на ПК лицом, установившим (изменившим) программное обеспечение, в присутствии пользователя ПК или ответственного за информационную безопасность в подразделении должна быть выполнена антивирусная проверка;

ж) 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.) сотрудник подразделения самостоятельно или вместе с ответственным за обеспечение информационной безопасности в подразделении должен провести внеочередной антивирусный контроль своего(ей) ПК;

з) В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение информационной безопасности своего подразделения, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ возможности дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов;
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл на гибком магнитном диске в Комитет по информационным ресурсам и телекоммуникациям Смоленской области для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку;
- по факту обнаружения зараженных вирусом файлов составить служебную записку в Комитет по информационным ресурсам и телекоммуникациям Смоленской области, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

2.3.5. Присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленного за ним ПК в подразделении.

2.3.6. Немедленно вызывать ответственного за информационную безопасность в подразделении при подозрении компрометации личных паролей или их утери, а также при обнаружении:

а) Нарушений целостности пломб, наклеек на аппаратных средствах ПК или иных фактов совершения в его отсутствие попыток несанкционированного доступа к ПК;

б) Несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ПК;

в) Отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ПК, выхода из строя или неустойчивого функционирования узлов ПК или периферийных устройств (дисководов, принтера и т.п.);

г) Непредусмотренных формуляром ПК отводов кабелей и подключенных устройств.

2.3.7. Хранить значение своих паролей на бумажном или другом носителе информации только в сейфе у ответственного за информационную безопасность или руководителя подразделения в опечатанном конверте.

2.3.8. Сотрудникам структурных подразделений Администрации Смоленской области категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения ПК в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ПК или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные формулярами ПК;
- осуществлять обработку конфиденциальной информации в присутствии посторонних (не допущенных к данной информации) лиц;
- осуществлять обработку конфиденциальной информации при подключенном ПК к сети Интернет;
- записывать и хранить конфиденциальную информацию на неучтенных носителях информации (гибких магнитных дисках и т.п.);
- оставлять включенными без присмотра свои ПК, не активировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры), если таковые имеются;
- оставлять без личного присмотра на рабочем месте или где бы то ни было машинные носители и распечатки, содержащие конфиденциальную информацию;
- предпринимать попытки несанкционированного доступа к недоступным информационным ресурсам, осуществлять намеренное изменение, уничтожение, чтение или передачу информации неавторизованным способом;
- 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 немедленно ставить в известность ответственного за информационную безопасность в подразделении.

3. Права

3.1. Сотрудники структурных подразделений Администрации Смоленской области - пользователи ПК имеют право:

3.1.1. Давать ответственному за обеспечение информационной безопасности в подразделении предложения по совершенствованию мер информационной безопасности в подразделении.

3.1.2. Обращаться к ответственному за обеспечение информационной безопасности в подразделении для оказания необходимой технической и методологической помощи в своей работе.

3.2. Ответственный за обеспечение информационной безопасности в подразделении имеет право:

3.2.1. Требовать от сотрудников подразделения - пользователей ПК соблюдения установленных технологий обработки информации и выполнения инструкций и других документов по обеспечению безопасности и защите информации.

3.2.2. Обращаться к руководителю своего подразделения с требованием прекращения работы сотрудников подразделения - пользователей ПК при несоблюдении ими установленных технологий обработки информации или невыполнении требований по обеспечению информационной безопасности.

3.2.3. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи информации и технических средств.

3.2.4. Давать руководителю своего подразделения предложения по совершенствованию мер информационной безопасности в подразделении.

3.2.5. Обращаться в Комитет по информационным ресурсам и телекоммуникациям администрации Смоленской области для оказания необходимой технической и методологической помощи в своей работе.

4. Ответственность

4.1. Руководитель структурного подразделения Администрации Смоленской области несет персональную ответственность за обеспечение информационной безопасности в подразделении при использовании ПК, имеющих доступ к Интранет-сети Администрации Смоленской области и Интернет.

4.2. Ответственный за обеспечение информационной безопасности несет персональную ответственность за организацию и качество проводимых им работ по обеспечению защиты информации в подразделении при использовании ПК, имеющих доступ к Интранет-сети Администрации Смоленской области и Интернет, за соблюдение требований настоящей Инструкции.

4.3. Сотрудники структурных подразделений Администрации Смоленской области, пользователи ПК, имеющие доступ к информационным ресурсам Интранет-сети Администрации Смоленской области и Интернет, несут персональную ответственность за обеспечение информационной безопасности при их использовании, за соблюдение требований настоящей Инструкции.

Приложение N 1. Формуляр на персональный компьютер (рабочую станцию) (не приводится).

Приложение N 2. Выдержки из статей Уголовного кодекса РФ (в "Обязанности сотрудников структурных подразделений Администрации Смоленской области по обеспечению информационной безопасности при работе в компьютерных и телекоммуникационных системах Администрации Смоленской области") (не приводится).

Председатель Комитета
по информационным ресурсам
и телекоммуникациям
Смоленской области
В.И.МНЕВ