ПРАВИТЕЛЬСТВО САНКТ-ПЕТЕРБУРГА

КОМИТЕТ ПО ГОСУДАРСТВЕННОМУ КОНТРОЛЮ, ИСПОЛЬЗОВАНИЮ И ОХРАНЕ ПАМЯТНИКОВ ИСТОРИИ И КУЛЬТУРЫ

П Р И К А З

окуд

03.05.2012 № 8-191

Об утверждении инструкций по парольной и антивирусной защите информации и маркировке носителей информации

В целях исполнения требований Федерального закона от 27 июля 2006 г. N 152-ФЗ «О персональных данных», Постановления Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и в соответствии со «Специальными требованиями и рекомендации по технической защите конфиденциальной информации» (СТР-К)

П Р И К А З Ы В А Ю:

1. Утвердить инструкцию по организации парольной защиты в КГИОП (Приложение 1).

2. Утвердить инструкцию по организации антивирусной защиты в КГИОП (Приложение 2).

3. Утвердить порядок маркировки носителей информации, содержащих персональные данные в КГИОП (Приложение 3).

4. Контроль за исполнением приказа остаётся за председателем КГИОП.

Председатель КГИОП А. И. Макаров

Приложение № 1
к приказу КГИОП
от _03.05.2012 № _8-191_

Инструкция
по организации парольной защиты в КГИОП

1. Общие положения

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в ИСПДн КГИОП, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

2. Порядок парольной защиты

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в ИСПДн возлагается на сотрудника обслуживающей организации, оказывающего услуги по системному администрированию и техническому обслуживанию локальных вычислительных сетей. Контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на начальника сектора информационных технологий и материального обеспечения.

2. Личные пароли должны генерироваться и распределяться централизованно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ 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.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

3. Формирование личных паролей пользователей осуществляется централизованно. Ответственность за правильность их формирования и распределения возлагается на сотрудника обслуживающей организации, оказывающего услуги по системному администрированию и техническому обслуживанию локальных вычислительных сетей. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность

ознакомления (самих уполномоченных сотрудников, а также руководителей подразделений) с паролями других сотрудников подразделений.

4. Списки паролей в опечатанном виде хранятся в сейфе начальника отдела по вопросам государственной службы, кадров и организационной работы (каб. 505).

5. Полная плановая смена паролей пользователей должна проводиться регулярно**.**

6. Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться по представлению администратора безопасности уполномоченными сотрудниками немедленно после окончания последнего сеанса работы данного пользователя с системой.

7. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры в соответствии с п.6 настоящей Инструкции.

8. Хранение сотрудником (исполнителем) значений своих паролей на материальном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя подразделения в опечатанном конверте или пенале (возможно вместе с персональным носителем информации и идентификатором Touch Memory).

9. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены и использования в подразделениях возлагается на администратора безопасности, периодический контроль – начальника сектора информационных технологий и материального обеспечения.

3. Ответственность

Пользователь и администратор безопасности несут ответственность за качество и своевременность выполнения задач и функций, возложенных на них в соответствии с настоящей Инструкцией.

Приложение № 2
к приказу КГИОП
от _03.05.2012 № _8-191_

Инструкция
по организации антивирусной защиты в КГИОП

1. Общие положения

Компьютерный вирус является разрушающей программной закладкой и характеризуется значительным деструктивным потенциалом для программ, данных и любой информации, хранящейся на компьютерах и магнитных носителях. Особую опасность представляет то обстоятельство, что компьютерные вирусы могут скрытно и постепенно уничтожать, либо мгновенно разрушать хранящуюся в компьютере и магнитных носителях информацию, при этом также могут пострадать аппаратные средства.

Основными путями вирусного вторжения являются неквалифицированное обращение пользователей с компьютерной техникой при использовании ими зараженных дискет и программ, либо целенаправленное спланированное воздействие извне с использованием компьютерных вирусов. При любых обстоятельствах это затрагивает вопросы защиты информации и интересы собственной безопасности Правительства СПб.

2. Порядок, обеспечивающий безопасную работу на компьютере и с магнитными носителями.

1. Приобретение средств вычислительной техники (СВТ) и программных продуктов подразделениями осуществляется исключительно через Комитет по информации и связи, а их установка и техническая поддержка производятся сотрудниками обслуживающей организации. Там же осуществляется проверка, настройка и тестовые испытания СВТ и программных продуктов.

Вновь поступающее программное обеспечение должно быть подвергнуто входному контролю – проверке на отсутствие вирусов и проверке соответствия длины и контрольных сумм, если таковые указаны в сопроводительных документах, полученным длинам и контрольным суммам.

2. Каждый компьютер решением начальника структурного подразделения персонально закрепляется за ответственным за его эксплуатацию подготовленным работником.

3. Допуск сотрудников к самостоятельной работе на компьютерах и с внешними носителями осуществляется только после овладения ими навыками в работе с компьютером, антивирусными пакетами программ.

4. На компьютерах может использоваться программное и аппаратное обеспечение, необходимое только для выполнения служебной деятельности и согласованное с комитетом по информационным технологиям. Запрещается использовать на компьютерах программные и аппаратные средства, не согласованные с документами ФСТЭК, а для систем, обрабатывающих информацию ограниченного доступа, с документами ФСТЭК и ФСБ.

5. На любом, работающем компьютере, в обязательном порядке должен быть установлен и активирован пакет антивирусных программ. Ответственность за это несет конкретный, отвечающий за его работоспособность сотрудник, а также администратор безопасности

организации. Установка средств антивирусного контроля (в том числе настройка параметров средств антивирусного контроля) на автоматизированных рабочих местах (АРМ), серверах локальной вычислительной сети (ЛВС) осуществляется сотрудниками обслуживающей организации в соответствии с руководствами по применению конкретных антивирусных средств. Антивирусные средства устанавливаются при вводе в эксплуатацию автоматизированной системы или при их плановой замене.

6. Периодически, не реже 1 раза в неделю, работник, ответственный за компьютер, проверяет его дисковое пространство с использованием антивирусного пакета программ на возможное наличие компьютерного вируса.

7. Пользователь (в случае необходимости совместно с администратором безопасности) обязан проводить антивирусный контроль любой электронной информации (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивируемые/разархивируемые файлы и т.д.), получаемой и передаваемой по телекоммуникационным каналам, а также информации на съемных носителях (магнитных дисках, оптических носителях, Flash - память и т.п.).

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

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности подразделения, начальника сектора информационных технологий и материального обеспечения, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь специалистов по информационным технологиям);

Все факты обнаружения зараженных вирусом файлов администратор безопасности АС заносит в «Журнал учета работы АС», где отображается тип зараженного файла, характер содержащейся в файле информации, название вируса, тип вируса и выполненные антивирусные мероприятия.

3. Ответственность

Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на администратора безопасности информации в организации.

Пользователь и администратор безопасности несут ответственность за качество и своевременность выполнения задач и функций, возложенных на них в соответствии с настоящей Инструкцией.

Приложение № 3
к приказу КГИОП
от _03.05.2012 № _8-191_

Порядок
маркировки носителей информации, содержащих персональные данные в КГИОП

Магнитные носители (магнитные ленты, съемные магнитные диски, дискеты и флешнакопители), предназначенные для нанесения на них закрытой информации, берутся на учет до записи на них персональных данных

Для записи информации содержащей персональные данные должны использоваться специально выделенные персональные компьютеры, дискеты и флешнакопители.

При постановке на учет съемного диска их маркировка производится на металлической пластине, прикрывающей нерабочую поверхность нижнего диска, посредством нанесения записей механическим путем или красящим веществом, имеющим хорошую механическую стойкость. На дискеты и флешнакопители с двух сторон наносится красящее стойкое вещество.

На каждый магнитный носитель персональных данных заводится лицевой счет, по которому осуществляется допуск к персональному компьютеру и выдача съемных дисков, дискет или флешнакопителей.

К работе с персональными данными должны допускаться только те лица, которые указаны в разрешении на автоматизированную обработку информации, составляющей коммерческую тайну, и только в те интервалы рабочего времени, которые отведены для решения указанной задачи в графике рабочего времени.

Инвентарный номер персональному компьютеру, съемному диску, флешнакопителю или дискете присваивается один раз при их первичном учете и может быть изменен только при проведении переинвентаризации и заведении нового учета, о чем делается отметка в соответствующих учетных формах.

Персональные компьютеры, используемые для сохранения коммерческой информации на длительное время, подлежат инвентарному учету по книге, где отражается наименование содержащейся информации. В этих случаях указанные компьютеры на период, пока они не используются в работе, опечатываются работником подразделения по ведению делопроизводства документов, ответственным за учет магнитных накопителей информации. Включение этих компьютеров в работу в соответствии с заказом (заданием, запросом) производится исполнителем (оператором) в присутствии работника этого подразделения.

Жесткие магнитные диски при обработке на них персональных данных используются, как правило, в качестве рабочих магнитных носителей информации, которая должна обязательно стираться по окончании выполнения каждого конкретного расчета.

Отметка о стирании информации с жесткого диска, а также из основной памяти после проведения работ производится в журнале оператора в графе "примечание" и заверяется подписями оператора и уполномоченного подразделения по ведению делопроизводства документов.

При наличии системы автоматического стирания запоминающих устройств отметка о стирании информации с жесткого диска в журнале оператора не производятся.