ПРАВИТЕЛЬСТВО САНКТ-ПЕТЕРБУРГА

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

П Р И К А З

окуд

03.05.2012 № 8-196

Об утверждении Инструкции по информационной безопасности в сфере информационно-телекоммуникационного обмена с использованием международных информационных сетей, в том числе «Интернет»

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» в КГИОП

П Р И К А З Ы В А Ю:

1. Утвердить Инструкцию по информационной безопасности в сфере информационно-телекоммуникационного обмена с использованием международных информационных сетей, в том числе «Интернет» (Приложение 1).

2. Контроль за исполнением приказа остаётся за председателем КГИОП.

Председатель КГИОП А. И. Макаров

Приложение № 1
к приказу КГИОП
от 03.05.2012 № 8-196

Инструкция
по информационной безопасности в сфере информационного обмена с использованием международных информационных сетей, в том числе «Интернет»

1. Общие положения

Инструкция разработана на основании Федерального закона «Об информации информатизации и защите информации» от 27 июля 2006 года №149-ФЗ, «Доктрины информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации 9 сентября 2000 года № Пр-1895, «Специальных требований и рекомендаций по защите конфиденциальной информации» (СТР-К) утвержденных приказом Гостехкомиссии России 30 августа 2002 года № 282, указа Президента «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17 марта 2008 года № 351 и других нормативно-правовых документов в области защиты информации.

Настоящая Инструкция определяет основные требования по организации работы в области защиты информации, общий порядок обращения с документами и другими материальными носителями информации при подключении и использовании международных информационных сетей (МИС) общего пользования, в том числе сети Интернет, в КГИОП.

Интернет - всемирная компьютерная сеть, которая использует для взаимодействия стек протоколов TCP/IP (протокол управления передачи сообщений / Интернет протокол). Работа в Интернет осуществляется в режиме реального времени (on-line). Существует ряд протоколов и служб, связанных с TCP/IP и Интернетом. Наиболее распространенными из них являются:

SMTP - протокол приема - передачи электронной почты.

TELNET - протокол для подключения к удаленным системам, присоединенным к МИС общего пользования в режиме удаленного терминала.

FTP - протокол предназначенный для передачи файлов с одного компьютера на другой в вычислительной сети.

DNS - служба сетевых имен используемых для протоколов TELNET, FTP и т.д.

WWW - служба (всемирная паутина), использующая гипертекстовый формат HTML (язык разметки гипертекста), предназначенная для передачи тестовой, графической, аудио и видео информации, а также ссылок на другие документы (гипертекстовые ссылки - выделенные области документа, позволяющие переходить к другому документу, содержащему связанную информацию).

Помимо перечисленных, существует ряд служб и протоколов для удаленной печати, предоставления удаленного доступа к файлам и дискам, работы с распределенными базами данных и т.д.

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

2. Источники угроз информационной безопасности

Подключение средств вычислительной техники к МИС общего пользования представляет реальную угрозу создания разветвленных систем регулярного несанкционированного контроля

информационных процессов и ресурсов, несанкционированного доступа (НСД) в автоматизированные системы (АС).

Информационные вычислительные сети общего пользования являются открытыми системами передачи информации, при работе в которых могут возникнуть следующие основные угрозы безопасности информации:

проникновение в систему незаконных пользователей, которое происходит вследствие ошибок в конфигурации программных средств (ошибок администрирования), дефектов в средствах обеспечения защиты информации от НСД операционных систем;

перенос в АС разрушающего программного обеспечения (внедрение программных закладок, вирусов);

выбор и использование законным пользователем системы неудачных паролей;

несанкционированная передача служебной информации ограниченного распространения пользователями в МИС общего пользования и т.д.

При непосредственном подключении локальной вычислительной сети к МИС общего пользования любой пользователь МИС имеет возможность:

получить информацию об адресной структуре сети;

установить типы и версии используемого сетевого программного обеспечения (сетевое оборудование, операционные системы, прикладные и служебные сервисы);

получить информацию о пользователях сети;

попытаться подключиться к информационным ресурсам сети;

вызвать отказ в обслуживании легальных пользователей.

Кроме явных, то есть непосредственно направленных на сеть организации, внешних угроз информационной безопасности, существуют угрозы, связанные с неумышленным распространением зловредного программного кода самими сотрудниками организации. К зловредному программному коду относят вирусы, троянские программы, «опасные» компоненты прикладных протоколов.

По этим причинам самым опасным с точки зрения безопасности информации является несанкционированное использование модемов, подключенных к рабочим станциям пользователя. Причем подключение не обязательно может использоваться для доступа в Интернет (возможны соединения к серверам других организаций, и к отдельным компьютерам, например домашним).

3. Технические средства защиты информации

К техническим средствам защиты информации при работе с информационными сетями общего пользования, в том числе Интернет относятся: системы разграничения прав доступа, межсетевые экраны, системы построения защищенных виртуальных сетей (Virtual Private Network – VPN), системы обнаружения атак, системы анализа защищенности, системы антивирусной защиты и т.д.

3.1. Системы разграничения доступа

Система разграничения доступа запрещает посторонним лицам доступ к ресурсам автоматизированной системы и позволяет разграничить права пользователей при работе на компьютере, при этом контролируются права локальных, удаленных и терминальных пользователей.

3.2 Межсетевые экраны (МСЭ)

Межсетевой экран представляет собой локальное (однокомпонентное) или функционально-распределенное средство, реализующее контроль за информацией, поступающей в автоматизированную систему (АС) и/или выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации, то есть ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС.

Межсетевые экраны позволяют осуществить: контроль доступа на межсетевом уровне, протоколирование информационных потоков, сокрытие топологии защищаемой сети, реагирование на несанкционированные действия.

Средствами МСЭ могут быть выявлены следующие виды атак: сканирование сетевых портов, атаки на отказ в обслуживании, изучение топологии внутренней сети, использование слабостей протоколов прикладного уровня, распространение вирусов и спама.

К дополнительным службам МСЭ относятся: средства резервного копирования и восстановления, средства обеспечения высокой доступности, сетевая служба имен (split DNS).

Основные показатели защищенности МСЭ: управление доступом, идентификация и аутентификация, регистрация событий и оповещение, контроль целостности, восстановление работоспособности.

3.3. Системы построения защищенных виртуальных сетей

Системы построения защищенных виртуальных сетей позволяют организовать прозрачное для пользователей соединение локальных вычислительных сетей с помощью шифрования.

3.4. Системы обнаружения атак

К системам обнаружения атак можно отнести: системы обнаружения атак на уровне сети, системы обнаружения атак на уровне хоста. Системы обнаружения атак используют:

- системы обнаружения аномального поведения пользователя (большое число соединений за короткий промежуток времени, высокая загрузка центрального процессора, использование периферийных устройств, которые обычно пользователем не используются и т.д.);
- системы обнаружения злоупотребления (обнаружение уже известной атаки по шаблону или «сигнатуре»).

3.5. Системы анализа защищенности

Средства анализа защищенности предназначены для поиска в вычислительной технике и ее компонентах различных уязвимостей, которые могут быть использованы злоумышленниками для реализации атак;

4. Организация работы с международными информационными сетями

4.1. Общие требования

На технических средствах должно находиться только программное обеспечение, необходимое для его функционирования. Владельцам открытых и общедоступных государственных информационных ресурсов необходимо осуществлять их включение в состав объектов международного информационного обмена только при использовании сертифицированных средств защиты информации, обеспечивающих ее целостность и доступность, в том числе криптографических для подтверждения достоверности информации.

Владельцам и пользователям указанных ресурсов необходимо осуществлять размещение технических средств, подключаемых к открытым информационным системам, сетям и сетям связи, используемым при международном информационном обмене, включая сеть "Интернет", вне помещений, предназначенных для ведения закрытых переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну.

4.2. Резервное копирование

При размещении информации в сетях общего пользования, необходимо иметь копию такой информации, для ее восстановления в случае разрушения, изменения или блокирования по причине несанкционированного доступа либо неисправности оборудования. Также необходимо иметь резервную копию системы для восстановления информации в случае ее разрушения.

4.3. Аппаратно - программная защита

Для фильтрации входящих и исходящих сообщений, а также обнаружения атак, рекомендуется использовать межсетевые экраны.

Для работы с открытыми информационными ресурсами в режиме реального времени (on-line) как правило, используют технологию VPN. Для передачи информации конфиденциального характера по открытым каналам связи необходимо использовать сертифицированные средства криптографической защиты.

Программное обеспечение, устанавливаемое на АС МИС общего пользования, должно быть сертифицировано и иметь все последние обновления.

4.4. Организационные меры

Пользователь обязан:

строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами;

знать и строго выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемых на персональных компьютерах;

хранить в тайне свой аутентификатор (пароль доступа), а также информацию о системе защиты;

знать порядок входа и регистрации в сети;

знать данную инструкцию;

знать правила работы со средствами защиты информации;

при пользовании электронной почтой запрещается передача сведений, содержащих конфиденциальную информацию без применения специальных мер защиты (сертифицированных средств криптографической защиты информации);

запрещается копирование или распространение информации с нарушением авторских прав или условий программных лицензий;

запрещается распространение противозаконных материалов.

С целью предотвращения заполнения почты ненужной почтовой (рекламной и др.) информацией - спамом не рекомендуется размещать адрес своего электронного ящика на досках объявлений. Для фильтрации данных сообщений необходимо использование белого и черного списка для настройки почтовой службы, а также сообщить о наличии спама администратору сети, провайдеру.

Администратор обязан:

обеспечить обновление антивирусных баз;

проверять технические средства на наличие/отсутствие вредоносного кода и целостность (запрещается использование при отключенных или неисправных средствах защиты информации).

Администратор обеспечивает выдачу аутентификаторов (имя пользователя/электронный адрес) и идентификаторов (пароль) пользователя, а также регулярную смену идентификаторов. В случае прекращения полномочий пользователя по работе с МИС (перевод на другую должность, не предусматривающую работу с МИС или увольнение), администратор удаляет учетную запись пользователя.

Администратор обеспечивает ведение журнала приема-передачи информации средствами МИС на электронных носителях.

4.5. Антивирусная защита

АС МИС общего пользователя оснащаются, в обязательном порядке, антивирусным программным обеспечением, обновление антивирусной базы которого производится

непосредственно перед каждым началом работы. Антивирусное программное обеспечение настраивается на проверку всех файлов без исключения. При использовании съемных накопителей информации для передачи информации, каждый из них должен быть проверен на отсутствие вредоносного программного обеспечения.

При отправке электронных сообщений необходимо заполнять поле тема. Не рекомендуется открывать для чтения почтовые сообщения, адресат которых неизвестен или почтовое отправление носит подозрительный характер (реклама или запрос информации неизвестной фирмы, спам, и т.д.)

Если обнаружено, что почтовое отправление, пришедшее от адресата, заражено вредоносным кодом, администратору необходимо:

срочно принять все меры по предотвращению дальнейшего распространения заражения путем прекращения приема передачи сообщений;

провести сканирование и лечение системы антивирусными средствами (при необходимости обновить базы данных антивирусного программного обеспечения);

Запрещается хранение вредоносного кода, на каких-либо носителях информации.

При обнаружении вредоносного кода необходимо произвести его удаление антивирусными средствами. Удаление зараженных файлов средствами операционной системы может привести к безвозвратному разрушению информации.

5. Организация доступа к МИС в КГИОП

Доступ к МИС в КГИОП осуществляется с использованием единой мультисервисной телекоммуникационной сети исполнительных органов государственной власти Санкт-Петербурга (ЕМТС).

Доступ к сети интернет осуществляется с использованием межсетевого экрана КГИОП через proxy-сервер узла телематических служб (УТС) Комитета по информатизации и связи. Администраторами УТС ведется фильтрация нецелевого контента сети Internet.

Для доступа к электронной почте используется почтовый сервер УТС. Адреса электронной почты, контроль учетных, нежелательной почты и антивирусная защита обеспечивается администраторами УТС.

Сотрудникам запрещается использование на рабочих местах сети КГИОП любых других способов подключения к МИС и электронной почте.