ПОЛОЖЕНИЕ
о порядке использования информационно-телекоммуникационных сетей международного информационного обмена и электронной почты в Санкт-Петербургском государственном бюджетном профессиональном образовательном учреждении «Политехнический колледж городского хозяйства» (СПб ГБПОУ «ПКГХ»)

1. **Общие положения**

1.1. Положение о порядке использования информационно-телекоммуникационных сетей международного информационного обмена и электронной почты в СПб ГБПОУ «ПКГХ» (далее – Положение) разработано на основании Федерального закона «Об информации, информационных технологиях и о защите информации», Доктрины информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации 09.09.2000 № Пр-1895, Специальных требований и рекомендаций по защите конфиденциальной информации (СТР-К), утвержденных приказом Государственной технической комиссии при Президенте Российской Федерации 30.08.2002 № 282, Указа Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» и других нормативных правовых актов и методических документов в области защиты информации.

1.2. Положение определяет основные требования по организации работы в области защиты информации, общий порядок обращения с документами и другими материальными носителями информации при подключении и использовании информационно-телекоммуникационных сетей международного информационного обмена и электронной почты в СПб ГБПОУ «ПКГХ».

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

SMTP – протокол приема-передачи электронной почты;

TELNET – протокол для подключения к удаленным системам, присоединенным к международным информационным системам (далее – 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 текстовой, 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.

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

2. Источники угроз информационной безопасности

2.1. Подключение средств вычислительной техники к информационно-телекоммуникационным сетям международного информационного обмена представляет реальную угрозу создания разветвленных систем регулярного несанкционированного контроля информационных процессов и ресурсов, несанкционированного доступа (далее – НСД) в автоматизированные системы (далее – АС).

2.2. 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
- 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.

2.3. Кроме явных, то есть непосредственно направленных на сеть СПб ГБПОУ «ПКГХ», внешних угроз информационной безопасности, существуют внутренние угрозы, связанные с неумышленным распространением зловредного программного кода самими работниками СПб ГБПОУ «ПКГХ». 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 сеть «Интернет» (возможны соединения к серверам других организаций и отдельным компьютерам, например, домашним).

3. Технические средства защиты информации

К техническим средствам защиты информации при работе с информационными сетями общего пользования, в том числе сетью «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

Межсетевой экран (далее – МСЭ) представляет собой локальное (однокомпонентное) или функционально-распределенное средство, реализующее контроль за информацией, поступающей в 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 уязвимости 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.

МСЭ делятся на пять классов в соответствии с руководящим документом «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», утвержденным решением председателя Государственной технической комиссии при Президенте Российской Федерации 25.07.1997.

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

АС МИС общего пользования не должны иметь логических и физических каналов (линий) связи с объектами вычислительной техники, на которых ведется обработка информации ограниченного распространения, а также для которых установлены особые правила доступа к информационным ресурсам, либо допуск к ним должен быть разграничен.

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 МСЭ.

Для работы с открытыми информационными ресурсами в режиме реального времени (on-line), как правило, используют технологию VPN. Для передачи конфиденциальной информациипо 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

4.4.1. Приказом СПб ГБПОУ «ПКГХ» назначаются ответственные за эксплуатацию АС МИС, допущенные к работам в МИС общего пользования из числа работников СПб ГБПОУ «ПКГХ».

4.4.2. Ответственный за эксплуатацию АС МИС обязан обеспечить своевременное обновление антивирусной программы на рабочем месте пользователя.

4.4.3. Ответственный за эксплуатацию АС МИС 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 из АС МИС

4.4.4. Пользователь АС МИС обязан:

- **строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АС;**
- **знать и строго выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемых на персональных компьютерах;**
- **хранить в тайне свой аутентификатор (пароль доступа в автоматизированную систему), а также информацию о системе защиты установленной на АС;**

4.4.5. Пользователи, работающие на АС МИС общего пользования, обязаны:

- знать порядок входа в МИС общего пользования и регистрации в сети;
- знать Положение;
- знать правила работы со средствами защиты информации установленными на АС.

4.4.6. Пользователям, работающим на АС МИС общего пользования, запрещается:

- передача сведений, содержащих конфиденциальную информацию без применения специальных мер защиты (сертифицированных средств криптографической защиты информации) при использовании электронной почты;
- копирование или распространение информации с нарушением авторских прав или условий программных лицензий;
- распространение противозаконных материалов.

4.4.7. С целью предотвращения заполнения почты ненужной почтовой (рекламной и др.) информацией – спамом не рекомендуется размещать адрес своего электронного ящика на досках (доски объявлений или BBS) объявлений. Для фильтрации данных сообщений необходимо использование антивирусного программного обеспечения и антиспам-фильтров для настройки почтовой службы, а также сообщить о наличии спама администратору сети Смольного.

4.5. Антивирусная защита

АС МИС общего пользования в обязательном порядке оснащаются 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. АС МИС общего пользования регулярно, не реже одного раза в неделю, проверяются на отсутствие вредоносного программного кода.

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 данной АС МИС;
- провести сканирование и лечение системы антивирусными средствами (при необходимости обновить базы данных антивирусного программного обеспечения);
- поставить в известность руководителя подразделения, а также абонента с которым осуществлялась связь в период заражения для проверки АС антивирусными средствами.
- сообщить адресату о наличии у него заражения, для последующего принятия адресатом срочных мер.

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. Работа в информационно-телекоммуникационной сети «Интернет»

5.1. Доступ к информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет») для отдельных сотрудников (работников) СПб ГБПОУ «ПКГХ» предоставляется по служебной записке руководителя соответствующего структурного подразделения СПб ГБПОУ «ПКГХ».

5.2. Пользователи используют поиск информации в сети «Интернет» только в случае, если это необходимо для выполнения своих должностных обязанностей.

5.3. По использованию сетью «Интернет» ведется статистика, которая хранится на электронных носителях.

5.4. Действия любого пользователя, подозреваемого в нарушении правил пользования сетью «Интернет», могут быть запротоколированы и использоваться для принятия

решения о применении к нему санкций.
5.5. Сотрудникам (работникам), пользующимся сетью «Интернет», запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим или нарушает действующее законодательство Российской Федерации.
5.6. При необходимости переноса рабочих материалов, полученных из сети «Интернет», на персональный компьютер пользователя, требуется их проверка при помощи антивирусных программ, согласно Инструкции по организации антивирусной защиты в СПб ГБПОУ «ПКГХ».

6. Порядок осуществления доступа и обмена данными с внешними информационными ресурсами и по электронной почте

6.1. Установка и настройка программного обеспечения для работы с электронной почтой или ресурсами сети «Интернет» осуществляется сотрудником отдела информатизации образовательного и производственного процессов СПб ГБПОУ «ПКГХ». Пользователям запрещается изменение любых параметров, касающихся способов подключения и используемых протоколов.
6.2. При работе с электронной почтой или ресурсами сети «Интернет» пользователям запрещается:

- обмен информацией для служебного пользования, а также информацией ограниченного доступа, по электронной почте или с использованием ресурсов сети «Интернет»;
- использование ресурсов сети «Интернет» для развлечения и получения информации, не относящейся к функциональным обязанностям пользователя;
- предоставление доступа к электронной почте или к ресурсам сети «Интернет»

с использованием данных своей учетной записи другим лицам;

- публикация своего служебного адреса электронной почты

в электронных каталогах, на поисковых машинах и других ресурсах сети «Интернет» в целях, не связанных с исполнением своих должностных обязанностей;

- подписка по электронной почте на различные рекламные материалы, листы рассылки, электронные журналы и т.д., не связанные с выполнением пользователем должностных обязанностей;
- открытие (запуск на выполнение) файлов, полученных по электронной почте или из ресурсов сети «Интернет», без предварительной проверки их антивирусным программным обеспечением.

Пользователи не должны позволять кому-либо посылать письма от чужого имени.

7. Ответственность пользователя

7.1. Пользователь компьютера отвечает за информацию, хранящуюся на его компьютере, технически исправное состояние компьютера и вверенной техники.
7.2. Пользователь несет личную ответственность за весь информационный обмен между его компьютером и другими компьютерами в сети и за ее пределами.
7.4. За нарушение требований Положения пользователь может быть отстранен от работы в сети.