

**ДЕПАРТАМЕНТ ВНУТРЕННЕЙ И КАДРОВОЙ ПОЛИТИКИ
БЕЛГОРОДСКОЙ ОБЛАСТИ**

**Областное государственное автономное
профессиональное образовательное учреждение
«БЕЛГОРОДСКИЙ СТРОИТЕЛЬНЫЙ КОЛЛЕДЖ»**

Принято
Общим собранием

« 31 » августа 2015 г.
Протокол № 01

«УТВЕРЖДАЮ»
Директор ОГАПОУ «БСК»

Л.И.Шинкарев
Приказ от «03» 09 2015 г. № 115-Ок



ИНСТРУКЦИЯ

**Использования ресурсов глобальной сети интернет в
ОГАПОУ «БСК»**

Белгород, 2015

Общие положения.

Настоящая инструкция разработана для повышения эффективности работы сотрудников областного государственного автономного профессионального образовательного учреждения «Белгородский строительный колледж» (далее - колледж), использующих электронные информационные ресурсы глобальной сети Интернет, и повышения уровня информационной безопасности локальной информационно-вычислительной сети колледжа.

Руководство колледжа устанавливает постоянный контроль и полностью специфицирует виды информации, к которой разрешен доступ тому или иному работнику. В случае нарушения сотрудником колледжа данной инструкции, работник отстраняется от использования ресурсов сети Интернет.

1. Назначение доступа к ресурсам сети Интернет

Доступ к ресурсам сети Интернет предоставляется сотрудникам колледжа для выполнения ими прямых должностных обязанностей. Глобальная сеть Интернет используется для:

- доступа к всемирной паутине гипертекстовых страниц (WWW);
- доступа к файловым ресурсам Интернета (FTP);
- доступа к специализированным (правовым и др.) базам данных;
- контактов с официальными лицами других образовательных структур, с сотрудниками структурных подразделений колледжа и работниками отраслевых предприятий; производителями и потребителями товаров и услуг;
- обмена электронной почтой с официальными лицами по не конфиденциальным вопросам производственного характера;
- сбора информации о состоянии рынка продукции и услуг, используемых в сфере образования;
- повышения квалификации работников, необходимой для выполнения своих должностных обязанностей;
- поиска и сбора информации по управленческим, производственным, финансовым, юридическим вопросам, если эти вопросы напрямую связаны с выполнением работником его должностных обязанностей, и др.

2. Основные ограничения при работе в сети Интернет

Основными ограничениями при работе в сети Интернет являются следующие:

- запрещено посещение пользователем ресурсов с непристойным содержанием (эротико-порнографические ресурсы, нацистские или националистические ресурсы, ресурсы, призывающие к насилию);
- запрещено посещение игровых, развлекательных и прочих сайтов, не имеющих отношения к деятельности колледжа и деятельности пользователя;
- запрещено использование электронной почты, досок объявлений, конференций на компьютерах образовательного учреждения в личных целях в любое время;

- запрещена публикация корпоративного электронного адреса @gax.belsLru на досках объявлений, в конференциях и гостевых книгах;
- запрещена передача кому бы то ни было учетных данных пользователя;
- запрещено применение имен пользователей и паролей компьютеров колледжа на иных (сторонних) компьютерах;
- запрещены игры на компьютере автономно и в сети;
- запрещено единовременное скачивание больших объемов информации
- запрещено посещение ресурсов трансляции потокового видео и аудио (веб-камеры, трансляция ТВ и музыкальных программ в Интернете), создающих большую загрузку сети и мешающих нормальной работе остальных пользователей;
- запрещена загрузка материалов порнографического содержания, компьютерных игр, анекдотов, других развлекательных материалов; запрещена передача конфиденциальной информации третьей стороне; запрещено нанесение вреда электронной системе колледжа; запрещено проведение незаконных операций в глобальной сети Интернет;
- запрещены любые попытки деструктивных действий по отношению к нормальной работе электронной системы колледжа и сети Интернет (рассылка вирусов, ip-атаки и т.п.);
- запрещено нарушение закона об авторском праве: копирование и использование материалов, защищенных законом об авторском праве;
- запрещено совершении действий, противоречащих законодательству, а также настоящей инструкции.

3. Соблюдение субординации

Работа в сети Интернет, общение с другими организациями, может быть связана с необходимостью изложения своих взглядов по отдельным вопросам. Если сотрудник колледжа высказывает в сообщении собственное мнение, то он, по предварительному согласованию с руководителем образовательного учреждения, обязан предупредить об этом в конце сообщения фразой: "Прошу считать, что в сообщении указано мое личное мнение, которое необязательно отражает взгляды и политику колледжа".

4. Контроль использования ресурсов сети Интернет

Директор колледжа оставляет за собой право, в целях обеспечения безопасности электронной системы, производить выборочные и полные проверки всей электронной системы и отдельных файлов без предварительного уведомления работников.

После утверждения настоящей инструкции, все руководители структурных подразделений колледжа обязаны под личную роспись ознакомиться с инструкцией и её приложениями.

Согласовано с Советом обучающихся ОГАПОУ «БСК» Протокол от «31» августа 2015 г. № 3
--

Согласовано с Советом родителей ОГАПОУ «БСК» Протокол от «31» августа 2015 г. № 4
--

Обязанности информатизационного центра по обеспечению доступа к ресурсам сети интернет

Основными задачами информатизационного центра колледжа по обслуживанию доступа к сети Интернет являются:

- обеспечение достаточной пропускной способности и бесперебойного функционирования каналов доступа в сеть Интернет; выполнение различных требований отдельных групп пользователей;
- максимальная защита внутренних сетей от несанкционированного доступа из Интернет и вирусных атак;
- определение прав доступа отдельных пользователей к различным ресурсам Интернет, директивного ограничения потребления ресурсов для определенных пользователей.

Памятка по работе с корпоративной электронной почтой

Политика использования электронной почты является важнейшим элементом общекорпоративной политики информационной безопасности колледжа и неотделима от нее.

Электронная почта является собственностью колледжа и может быть использована **ТОЛЬКО** в служебных целях. Использование электронной почты в других целях запрещается.

Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию непосредственного либо вышестоящего руководителя.

При работе с корпоративной системой электронной почты сотрудникам колледжа запрещается:

- использовать адрес корпоративной почты для оформления подписок;
- публиковать свой адрес либо адреса других сотрудников колледжа на общедоступных Интернет-ресурсах (форумы, конференции и т.п.);
- открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами, даже если отправитель письма хорошо известен;
- осуществлять массовую рассылку почтовых сообщений рекламного характера;
- рассылать через электронную почту материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также ссылки на вышеуказанную информацию;
- распространять защищаемые авторскими правами материалы, затрагивающие какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;
- распространять информацию, содержание и направленность которой запрещены международным и российским законодательством, включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.;
- распространять информацию ограниченного доступа, предназначенную для служебного использования;
- предоставлять кому бы то ни было пароль доступа к своему почтовому ящику.

Памятка по работе в глобальной сети интернет

Настоящий документ описывает общепринятые нормы работы в сети Интернет, соблюдение которых является обязательным для всех пользователей. Действие этих норм распространяется на использование ресурсов сети. Здесь и далее словом «сеть» обозначены сеть Интернет и доступные из нее другие сети. При работе в глобальной сети являются недопустимыми:

- массовая рассылка не согласованных предварительно с руководством колледжа электронных писем (mass mailing). Под массовой рассылкой подразумевается как рассылка множеству получателей, так и множественная рассылка одному получателю. Здесь и далее под электронными письмами понимаются сообщения электронной почты, ICQ и других подобных средств личного обмена информацией;
- несогласованная рассылка электронных писем рекламного, коммерческого или агитационного характера, а также писем, содержащих грубые и оскорбительные выражения и предложения;
- размещение в любой конференции Usenet или другой конференции, форуме или электронном списке рассылки статей, которые не соответствуют тематике данной конференции или списку рассылки (off-topic). Здесь и далее под конференцией понимаются телеконференции (группы новостей) Usenet и другие конференции, форумы и электронные списки рассылки;
- размещение в любой конференции сообщений рекламного, коммерческого или агитационного характера, кроме случаев, когда такие сообщения явно разрешены правилами такой конференции либо их размещение было согласовано с владельцами или администраторами такой конференции предварительно;
- размещение в любой конференции статьи, содержащей приложенные файлы, кроме случаев, когда вложения явно разрешены правилами такой конференции либо такое размещение было согласовано с владельцами или администраторами такой конференции предварительно;
- рассылка информации получателям, высказавшим ранее явное нежелание получать эту информацию;
- контактных координат при совершении любого из вышеописанных действий, вне зависимости от того, из какой точки сети были совершены эти действия;
- запрет несанкционированного доступа и сетевых атак. Не допускается осуществление попыток несанкционированного доступа к ресурсам Сети, проведение или участие в сетевых атаках и сетевом взломе, за исключением случаев, когда атака на сетевой ресурс проводится с явного разрешения владельца или администратора этого ресурса.

В том числе запрещены:

- действия, направленные на нарушение нормального функционирования элементов Сети (компьютеров, другого оборудования или программного обеспечения), не принадлежащих пользователю;
- действия, направленные на получение несанкционированного доступа, в том числе привилегированного, к ресурсу сети (компьютеру, другому оборудованию или информационному ресурсу), последующее использование такого доступа, а также уничтожение или модификация программного обеспечения или данных, не принадлежащих пользователю, без согласования с владельцами этого

программного обеспечения или данных либо администраторами данного информационного ресурса;

- передача компьютерам или оборудованию Сети бессмысленной или бесполезной информации, создающей паразитную нагрузку на эти компьютеры или оборудование, а также промежуточные участки сети, в объемах, превышающих минимально необходимые для проверки связности сетей и доступности отдельных ее элементов.

Значительная часть ресурсов сети не требует идентификации пользователя и допускает анонимное использование. Однако в ряде случаев от пользователя требуется предоставить информацию, идентифицирующую его, и используемые им средства доступа к сети. При этом пользователю запрещается: использование идентификационных данных (имен, адресов, телефонов и т.п.) третьих лиц, кроме случаев, когда эти лица уполномочили пользователя на такое использование. В то же время пользователь должен принять меры по предотвращению использования ресурсов Сети третьими лицами от его имени (обеспечить сохранность паролей и прочих кодов авторизованного доступа);

- фальсификация своего IP-адреса, а также адресов, используемых в других сетевых протоколах, при передаче данных в Сеть;
- использование несуществующих обратных адресов при отправке электронных писем.