

ИНСТРУКЦИЯ
доступа и использования ресурсов сети Интернет
и электронной почты в УИТ

1. Общие положения

1.1. Целью ввода в действие данной Инструкции является обеспечение защиты информационных ресурсов, недопущение распространения информации, содержащей призывы к насильственному изменению конституционного строя, пропаганду войны, насилия и порнографии, разжигания религиозной и национальной розни, ущемления чести и достоинства человека и другой конфиденциальной информации, запрещенной к распространению действующим законодательством в Республике Узбекистан.

Настоящая Инструкция регулирует вопросы подготовки и распространения информационных ресурсов для оперативного обмена информацией в Университете Инха в городе Ташкент (далее - УИТ).

Настоящая Инструкция разработана в соответствии с:

- Законом Республики Узбекистан: "О связи", "Об информатизации", "О средствах массовой информации", "О гарантиях и свободе доступа к информации".
- Постановлением Кабинета Министров Республики Узбекистан от 5 февраля 1999 г. № 52 "О создании национальной сети передач данных и упорядочении доступа к мировым информационным сетям", Постановлением Кабинета Министров Республики Узбекистан от 6 июня 2002 г. № 200 "О мерах по дальнейшему развитию компьютеризации и внедрению информационно-коммуникационных технологий".
- Стандартом O'z DSt ISO/IEC 2382-8:2007 Информационные технологии. Информационная безопасность. Термины и определения, O'z DSt 1135:2007 Информационная технология. Требования к базам данных и обмену информации между органами государственного управления и государственной власти на местах, O'z DSt ISO/IEC 27002:2008 Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасностью.
- Нормативными актами: №ПП-614-2007г., ПКМ №242-2007г., №ПП-1572-2011г., ПКМ №296-2011г., ПКМ №170-2013г. и ПКМ №33-З-2015г.
- Нормативными документами: O'z DSt 2814:2014, O'z DSt 2815 2014, O'z DSt 2816 2014, O'z DSt 2817:2014, O'z DSt ISO/IEC 27001:2009,

Oz DSt ISO/IEC 27002:2008, O'z DSt ISO/IEC 27003:2014, O'z DSt ISO/IEC 27005:2013, O'z DSt ISO/IEC 27035:2015.

Действие настоящей Инструкции распространяется на все подразделения УИТ.

1.2. Инструкция предназначена для сотрудников, преподавателей и студентов УИТ, выполнение должностных обязанностей которых связано с использованием персональных компьютеров, и определяет их полномочия, обязанности и ответственность при использовании информационных ресурсов глобальной компьютерной сети Интернет.

1.3. Инструкция является обязательной для выполнения всеми сотрудниками, преподавателями и студентами - пользователями Информационной сети УИТ в части, касающейся их.

1.4. В Инструкции использованы следующие сокращения и основные понятия:

- ПК - персональный компьютер;
- ИС - информационная сеть;
- пользователь - сотрудник, преподаватель и студент УИТ, выполнение должностных обязанностей которого связано с использованием ПК в ИС УИТ;
- информационные ресурсы - отдельные документы и отдельные массивы документов, базы данных, другие виды информационного обеспечения в ИС с использованием ПК;
- администратор - сотрудник ИТ-службы, ответственный за подключение к глобальной сети Интернет и обеспечение работоспособности, надежности сети, сохранности и защиты информационных ресурсов;
- трафик - объем информации, полученной пользователем из глобальной компьютерной сети Интернет;
- развлекательные сайты: сайты знакомств, игровые сайты, порнографические сайты, а также любые сайты, которые не относятся к направлению деятельности сотрудника, преподавателя и студента;
- Chat – ресурс, предоставляющий возможность вести разговор в реальном времени.

1.5. Руководители структурных подразделений, пользователи и администраторы обязаны знать и выполнять нормативные правовые акты, затрагивающие вопросы информатизации, защиты информации и информационной безопасности в части соблюдения требований и ограничений по использованию информационных ресурсов.

1.6. Руководители структурных подразделений в обязательном порядке организуют ознакомление пользователей с нормативными правовыми актами, указанными в настоящей Инструкции.

1.7. Доступ к глобальной компьютерной сети Интернет осуществляется с рабочего ПК пользователя. Ответственность за действия на компьютере

другого сотрудника несет пользователь ПК, с которого совершено это действие.

1.8. Работа пользователей в глобальной компьютерной сети Интернет отслеживается с помощью специального программного обеспечения. На основе логов проводится анализ по следующим параметрам:

- перечень используемых ресурсов;

1.9. Настоящая Инструкция может уточняться и дополняться в установленном порядке.

2. Требования, предъявляемые к пользователю

2.1. Пользователю запрещается:

- посещение пользователем ресурсов с непристойным содержанием (эротико-порнографические ресурсы, нацистские или националистические ресурсы, ресурсы, призывающие к насилию);
- посещение игровых, развлекательных и прочих сайтов, не имеющих отношения к деятельности УИТ и деятельности пользователя;
- использование электронной почты, досок объявлений, конференций на компьютерах УИТ в личных целях в любое время;
- публикация корпоративного электронного адреса @inha.uz на досках объявлений, в конференциях и гостевых книгах;
- использование личных и некорпоративных E-mail адресов. В случае если пользователю в служебных целях необходимо завести почтовый ящик в домене, отличном от @inha.uz, необходимо разрешение вышестоящего руководителя пользователя, согласованное с информационной службой, только в домене .UZ;
- передача кому бы то ни было учетных данных пользователя;
- применение имен пользователей и паролей компьютеров УИТ на иных (сторонних) компьютерах;
- игры на компьютере автономно и в сети;
- посещение ресурсов трансляции потокового видео и аудио (вебкамеры, трансляция ТВ - и музыкальных программ в Интернете), создающих большую загрузку сети и мешающих нормальной работе остальных пользователей;
- загрузка материалов порнографического содержания, компьютерных игр, анекдотов, других развлекательных материалов;
- передача конфиденциальной информации третьей стороне;
- подключение к электронной сети под другим логином и паролем;
- нанесение вреда электронной системе УИТ;
- проведение незаконных операций в глобальной сети Интернет;
- создание личных веб-страниц и хостинг (размещение web- или ftp-сервера) на компьютере пользователя;
- любые попытки деструктивных действий по отношению к нормальной работе электронной системы УИТ и сети Интернет (рассылка вирусов, ip-атаки и т.п.);

- нарушение закона об авторском праве: копирование и использование материалов и программ, защищенных законом об авторском праве;
- совершение действий, противоречащих законодательству, а также настоящей Инструкции.

2.2. Пользователь обязан знать и уметь пользоваться антивирусным программным обеспечением. При обнаружении вируса он должен сообщить об этом администратору. Пользователю запрещается производить какие-либо действия с информацией, зараженной вирусом.

2.3. Пользователь обязан информировать администратора о любых нарушениях, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационных ресурсов или сбоям в работе сети.

3. Требования предъявляемые к администратору

3.1. Администратор обязан:

- производить подключение к сети Интернет только через специализированное устройство (Firewall) для обеспечения защиты информационной сети;
- знать и правильно использовать аппаратно-программные средства защиты информации и обеспечивать сохранность информационных ресурсов с помощью этих средств;
- оказывать методическую и консультационную помощь пользователям по вопросам, входящим в его компетенцию;
- вести учет и анализ использования ресурсов сети Интернет;
- информировать руководителей структурных подразделений о любых нарушениях требований настоящей Инструкции и других негативных ситуациях, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационных ресурсов или сбоям в работе сети.

3.3. Администратор имеет право:

- при обнаружении доступа к развлекательным сайтам запретить доступ к сайту;
- при обнаружении использования пользователем программных продуктов, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационных ресурсов или сбоям в работе сети, запретить доступ к сети Интернет.

4. Инструкция по работе с корпоративной электронной почтой

4.1. Инструкция использования электронной почты является важнейшим элементом общекорпоративной политики информационной безопасности УИТ и неотделима от нее.

4.2. Корпоративная электронная почта является собственностью УИТ и может быть использована ТОЛЬКО в служебных целях. Использование электронной почты в других целях категорически запрещено.

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

4.4. При работе с корпоративной системой электронной почты сотрудникам УИТ запрещается:

- использовать адрес корпоративной почты для оформления подписок;
- публиковать свой адрес либо адреса других сотрудников УИТ на общедоступных Интернет-ресурсах (форумы, конференции и т.п.) за исключением случаев служебной необходимости;
- 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 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 способы и методы изготовления и применения взрывчатых веществ или 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.

5. Порядок предоставления доступа к сети

5.1. Система контроля интернет-доступа в Общества предусматривает следующие автоматические ограничения:

- запрет входа на определенные сайты;
- запрет определенных интернет-протоколов;
- антивирусную проверку интернет-трафика с автоматическим отказом принимать вирусный файл;
- запрет скачивания определенных типов файлов;
- автоматическое отключение пользователя и (или) групп пользователей от платных ресурсов при достижении ими ежедневного, еженедельного или ежемесячного лимита.

Кроме того, система контроля интернет-доступа осуществляет сбор статистики использования Интернета пользователем. Настоящая статистика доступна системному администратору и может служить причиной отключения определенных ресурсов и принятия решений об изменении прав доступа пользователя к Интернету.

5.2. Ограничения доступа

По мнению руководства УИТ, возможны следующие ограничения доступа к Интернету для пользователей:

- ограничение доступа к сети Интернет с рабочего места;
- ограничение доступа к внешней электронной почте: mail.ru, mail.yandex.ru, mail.e1.ru и др.;
- ограничение доступа к icq, mail.ru-агенту, Telegram, Skype и другим интернет-пейджерам;
- ограничение к развлекательным сайтам по списку;
- ограничение доступа к социальным сетям: odnoklassniki.ru, vk.ru, facebook.com и другим;
- ограничение к работным сайтам с объявлениями о вакансиях и резюме;
- ограничение на количество использованного в день трафика.

5.3. Регламент предоставления доступа:

Пользователю предоставляется доступ к Интернету исходя из служебной необходимости после определения необходимых ограничений доступа (см. п. 4.1) с помощью служебной записки на имя системного администратора от руководителя отдела, одобренной руководством УИТ.

5.4. Порядок разрешения споров:

В случае возникновения претензий или вопросов, касающихся конкретного запрещенного сайта, типа файла, невозможности продолжения работы в сети Интернет, пользователь обращается к администратору. Если претензию не удастся разрешить двум сторонам – тогда вопрос рассматривается руководством УИТ.

6. Особые правила

6.1. Вышеперечисленные требования Инструкции доступа и использования ресурсов сети Интернет и электронной почты в УИТ обязательны к безусловному исполнению всеми сотрудниками, преподавателями, студентами, рабочими, служащими и руководителями УИТ, в случае игнорирования данных требований, в отношении виновных лиц могут быть применены меры административного реагирования, в соответствии с действующим законодательством Республики Узбекистан, вплоть до привлечения к уголовной ответственности.

6.2. По мере обновления законодательной базы Республики Узбекистан относительно защиты информации, внедрения новейших технологий и новейших программных продуктов предназначенных защите информации в данную Инструкции доступа и использования ресурсов сети Интернет и электронной почты в УИТ могут вноситься изменения и дополнения по согласованию с руководством УИТ.