

Приложение
к приказу Государственного комитета
Республики Узбекистан по статистике
от «20» февраля 2014 г. № 13

**Положение
о порядке использования сети Интернет и электронной почты
в системе Государственного комитета Республики Узбекистан
по статистике**

I. Область применения

1. Настоящее Положение определяет порядок использования сети Интернет и электронной почты пользователями корпоративной сети передачи данных в системе Государственного комитета Республики Узбекистан по статистике (далее – пользователи).

II. Термины и определения

2. В настоящем документе применены следующие термины и определения:

пользователь - пользователь корпоративной сети передачи данных в системе Госкомстата, которому разрешен доступ к сети Интернет и электронной почте. Каждому пользователю присваивается уникальный идентификатор пользователя и пароль для аутентификации;

администратор электронной почты и доступа в сеть Интернет (администратор) - лицо, ответственное за работу с сетью Интернет и электронной почтой, реализацию и непрерывность соблюдения установленных технических мер защиты информации;

инцидент информационной безопасности – единичное событие или ряд нежелательных не предвиденных событий информационной безопасности, из-за которых велика вероятность компрометации бизнес-информации и угрозы информационной безопасности.

III. Общие положения

3. Вопросы эффективного использования сети Интернет и электронной почты, а также беспрекословного выполнения требований информационной безопасности со стороны работников находятся под контролем у руководства Госкомстата.

4. Все пользователи, использующие сеть Интернет и электронную почту, должны быть ознакомлены под роспись с настоящим Положением и предупреждены об ответственности за ее нарушение.

5. Доступ к сети Интернет в системе Госкомстата должен использоваться исключительно в служебных целях для получения данных, необходимых для работы

конкретного работника. Использование технических средств для доступа в сеть Интернет в личных целях (в том числе в качестве развлекательного средства) не допускается.

6. Настройку, управление и контроль доступа в сеть Интернет в корпоративной сети передачи данных в системе Госкомстата осуществляет администратор электронной почты и доступа в сеть Интернет (далее – администратор).

7. Функции администраторов возлагаются на конкретных работников:

а) в центральном аппарате – приказом Госкомстата по представлению заместителя Председателя Госкомстата по вопросам внедрения ИКТ и обеспечения информационной безопасности;

б) в территориальном Управлении статистики – приказом территориального Управления по представлению штатного специалиста, ответственного за обеспечение информационной безопасности (далее – штатный специалист);

в) в Центре переподготовки кадров и статистических исследований – приказом Центра.

8. Обязательным условием получения пользователем параметров доступа (идентификатор и пароль) в сеть Интернет и к электронной почте является ознакомление его с настоящим Положением.

9. Параметры доступа в сеть Интернет и к электронной почте, а также почтовый адрес на корпоративном почтовом сервере выдаются:

а) в центральном аппарате – на основании рапорта заместителю Председателя Госкомстата по вопросам внедрения ИКТ и обеспечения информационной безопасности с предварительным визированием у начальника Управления информационной безопасности;

б) в территориальном Управлении статистики – на основании рапорта начальнику территориального Управления с предварительным визированием у штатного специалиста;

в) в Центре переподготовки кадров и статистических исследований – на основании рапорта директору Центра.

10. Пароль доступа и пароль к почтовому ящику должны быть известны только пользователю и быть достаточно сложными. Пароли могут быть заменены в любое время и в любом порядке по требованию пользователя или администратора.

Запрещается для доступа к сети Интернет:

а) использовать чужие параметры доступа;

б) предоставлять свои параметры доступа другим лицам;

в) использовать «групповые» имена (одно имя для группы пользователей).

IV. Требования по обеспечению информационной безопасности при использовании сети Интернет и электронной почты

11. При использовании сети Интернет в обязательном порядке должны применяться средства защиты информации (межсетевые экраны, антивирусные средства, средства криптографической защиты информации и другие), обеспечивающие прием и передачу информации только в установленном формате и только для конкретной технологии.

12. При доступе пользователей к сети Интернет должны быть обеспечены соответствующие механизмы аутентификации для пользователей и оборудования.

13. Одновременный доступ к сети Интернет под одними параметрами с нескольких компьютеров разрешается только в пределах одного Управления (Отдела) и при наличии письменного согласования такого режима между начальником соответствующего Управления (Отдела) и начальником Управления информационной безопасности (штатным специалистом).

14. На всех пользовательских программах, используемых для доступа к сети Интернет (браузеры и почтовые клиенты), должны быть настроены необходимые уровни безопасности.

15. Все файлы, загружаемые из сети Интернет, должны подвергаться антивирусной проверке, как на серверном, так и на пользовательском уровнях.

16. Доступ к нежелательным сайтам должен быть заблокирован согласно перечню, разрабатываемому Управлением информационной безопасности.

Серверные программы для обеспечения корпоративного выхода в сеть Интернет должны быть сконфигурированы так, чтобы к этим сайтам нельзя было получить доступ.

17. Предоставление особых режимов доступа конкретному пользователю и/или рабочей станции может быть обеспечено на временной основе при наличии письменного согласования между начальником соответствующего Управления (Отдела) и начальником Управления информационной безопасности (штатным специалистом).

18. В конце рабочего дня и при продолжительных перерывах в работе сеанс работы в сеть Интернет должен быть закрыт пользователем в обязательном порядке (или должен быть выключен компьютер).

19. Запрещается:

а) для доступа к сети Интернет подключать к компьютерам модемы или сотовые телефоны;

б) использовать внешние прокси-серверы (анонимайзеры);

в) оставлять без присмотра компьютеры, имеющие активный сеанс подключения к сети Интернет.

г) открывать сайты рекламного характера, так как такие сайты часто содержат объемную рекламу (перегрузка трафика) или побуждают пользователя произвести какие-либо действия с целью заражения компьютерным вирусом.

20. Запрещается распространять или демонстрировать в сети Интернет, а также получать с помощью сети Интернет:

а) файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности программ или компьютерного и телекоммуникационного оборудования;

б) специальные программные средства для получения незаконного (несанкционированного) доступа к защищенной компьютерной системе;

в) специальные вирусные программы;

г) компьютерные программы, предназначенные для несанкционированного уничтожения, блокирования, модификации, копирования или перехвата информации, хранящейся или передаваемой в компьютерной системе;

д) серийные номера к платным программным продуктам и программы для их генерации;

е) идентификаторы, пароли и прочие средства для получения незаконного доступа к платным ресурсам сети Интернет;

ж) материалы, носящие угрожающий, клеветнический или оскорбительный характер;

з) материалы, пропагандирующие национальную, расовую, этническую или религиозную вражду, нетерпимость или рознь;

и) материалы, пропагандирующие культ насилия или жестокости;

к) материалы, подстрекающие к насилию;

л) материалы, призывающие к совершению противоправной деятельности;

м) порнографические материалы;

н) программное обеспечение, предназначенное для организации или проведения азартных и других основанных на риске игр;

о) иную информацию, содержание и направленность которой запрещены законодательством Республики Узбекистан.

21. Пользователю рекомендуется:

а) при заполнении им различных анкетных форм на сайтах, по возможности, использовать вымышленные имена, фамилии, e-mail, адреса, телефоны, место работы, должность и другие существенные реквизиты;

б) не запускать большие (больше 3-5 Мбайт из зарубежного сегмента сети Интернет и 10-15 Мбайт из сети TAS-IX доменной зоны .UZ) загрузки во время рабочего дня, а также включать потоки данных (просмотры видео) во избежание ухудшения общей пропускной способности канала связи с сетью

Интернет. Администратор имеет право ограничить скорость большой загрузки или потока данных или прервать соединение. При наличии исходных или аналогичных информационных ресурсов в доменной зоне .UZ предпочтение должно отдаваться им, особенно для больших объемов информации.

22. При наличии аномального или подозрительного поведения веб-сайта (большое количество самостоятельно открывающихся окон, невозможность закрытия окон, переходы в незапрошенные сайты, навязчивые диалоги, остановка программы, активизация работы компьютера без явных причин и прочее) необходимо прекратить любую деятельность на компьютере и немедленно вызвать администратора.

23. Все действия пользователя в сети Интернет протоколируются в соответствующих электронных журналах и могут быть использованы для статистики и контроля выполнения пользователем регламентированных процедур доступа в сеть Интернет.

24. При фиксации администратором запрещенного или аномального поведения в сети Интернет пользовательской рабочей станции (нарушение регламента, признаки наличия троянской программы и прочее), пользователь может быть отключен от сети Интернет без предупреждения.

При повторных или злостных нарушениях регистрируется инцидент информационной безопасности и проводится служебная проверка по данному факту.

25. Администраторами должны проводиться разъяснительные работы с работниками по правильному и безопасному использованию сети Интернет вне рабочего места с обсуждением преимуществ использования для личной переписки национальных электронных почтовых сервисов и социальных сетей.

26. Все файлы, получаемые по электронной почте, должны подвергаться антивирусной проверке.

27. При работе с электронной почты запрещается:

а) использовать внешние почтовые ящики, как через веб-интерфейс, так и через почтовых клиентов. Допускается использовать только корпоративный почтовый сервер (stat и stat.uz);

б) обмен служебной информацией путём использования внешних электронных почтовых сервисов, социальных сетей (mail.ru, gmail.com, rambler.ru, yandex.ru, odnoklassniki.ru, facebook.com и другие) или сервисов мгновенных сообщений (например, ICQ, Google Talk и другие);

в) использовать адреса корпоративной электронной почты @stat.uz для заказа почтовых рассылок, для загрузки файлов, для передачи идентификационной информации при посещении различных веб-сайтов, и в других подобных случаях без предварительного согласования с администратором;

г) использовать корпоративный почтовый ящик для целей иных, кроме как для служебной переписки;

д) отправлять сообщения с вложенными файлами, общий объем которых превышает 2 Мегабайта, без предварительного согласования с администратором;

е) отправлять и получать любые вложения, имеющие расширения исполняемых файлов и программ, даже если они расположены внутри архивов;

ж) открывать любые вложенные файлы, имеющие подозрительные или очень длинные имена;

з) переходить по подозрительным ссылкам;

и) открывать любые вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами, даже если отправитель письма хорошо известен;

к) предоставлять кому бы то ни было пароль доступа к своему почтовому ящику.

28. При появлении в почтовом ящике повторяющихся писем от неизвестных адресатов («спам») следует сообщить об этом администратору для изменения настроек антиспамового фильтра почтового сервера.

29. При использовании сети Интернет и электронной почты запрещается распространять:

а) информацию касательно работы органов государственной статистики, не являющейся общедоступной;

б) персональные данные работников органов государственной статистики.

V. Ответственность за нарушение требований настоящего Положения

30. Работники, нарушившие требования настоящего Положения, несут ответственность в соответствии с установленным законодательством Республики Узбекистан порядком.

31. Нарушение требований, указанных в следующих пунктах настоящего Положения, расценивается как нарушение внутреннего распорядка:

пункт 5;

подпункты а) и б) пункта 19;

подпункты а), б) и в) пункта 27.

По всем фактам нарушения данных требований должна проводиться проверка, осуществляемая комиссией, состав которой определяется в:

центральном аппарате – заместителем Председателя Госкомстата по вопросам внедрения ИКТ и обеспечения информационной безопасности;

территориальном Управлении статистики – начальником территориального Управления статистики;

Центре переподготовки кадров и статистических исследований – директором Центра.

32. По результатам проверки должен составляться акт, который может служить основанием для наложения дисциплинарного взыскания.