

ОБЩИЕ РЕКОМЕНДАЦИИ И ПРАВИЛА ПОЛЬЗОВАНИЯ ЛОКАЛЬНОЙ СЕТЬЮ

Использование учетной записи:

Для надежной и безопасной работы в локальной сети администрация настоятельно рекомендует пользователям придерживаться следующих правил при работе с учетными записями:

1. Контролировать доступ к своей учетной записи, следить за содержимым своей общедоступной папки (если таковая имеется), за появлением файлов неизвестного происхождения (особенно скрытых).

ПОЛЬЗОВАТЕЛЯМ ЛОКАЛЬНОЙ СЕТИ КАТЕГОРИЧЕСКИ ЗАПРЕЩАЕТСЯ

1. Использовать вычислительную технику для несанкционированного доступа к другим компьютерам сети и нарушения системы безопасности в целом;
2. Подключать компьютеры к сети без специального разрешения системного администратора;
3. Категорически запрещается самовольно изменять IP-адреса компьютеров в сети, принадлежность компьютера к домену, сетевое имя компьютера, настройки шлюзов и основных серверов;
4. Распространять и использовать программное обеспечение и любые материалы, полностью или частично защищенные авторскими правами, без разрешения владельца;
5. Преднамеренно/непреднамеренно распространять компьютерные вирусы и зараженные ими файлы;
6. Перехватывать чужую информацию, передаваемую по сети;
7. Использовать программное обеспечение, ориентированное на нарушение системы безопасности сети ("тройанские кони", бэкдоры и другое шпионское программное обеспечение);
8. Обмениваться информацией, запрещенной действующим законодательством Республики Узбекистан: пропаганда насилия, разжигание расовых, национальных и религиозных распри, порнография, любая информация, несущая оскорбления и клевету, а также распространяемая с целью хищения чужих денежных

средств или имущества путем обмана или злоупотребления доверием;

9. Несанкционированный доступ (или его попытки) к закрытым ресурсам в сети. Участвовать в проведении "сетевых атак" и " сетевого взлома".

Эти действия определяются как:

- a. использование против компьютеров или оборудования компьютерных сетей специальных средств, позволяющих получить нелегальный доступ к содержащейся информации;
 - b. передача компьютерам или оборудованию компьютерных сетей бессмысленной или бесполезной информации, создающей паразитическую нагрузку на аппаратуру;
 - c. уничтожение/модификация программного обеспечения или данных, не принадлежащих пользователю, без согласования с владельцами или администраторами этого программного обеспечения или данных;
 - d. фальсификация своего сетевого адреса при передаче данных в сеть;
 - e. фальсификация контактной информации, предъявленной владельцам или администраторам ресурсов или сетей;
 - f. использование псевдонимов и анонимность, кроме случаев, когда право пользования соответствующими ресурсами или сетей разрешают анонимность при их использовании.
10. Сканировать порты на удаленных хостах. Это может быть расценено как попытка взлома, со всеми вытекающими последствиями;

Сканированием считается выдача запросов, в том числе и единичных, на предмет наличия того или иного сервиса или опрос наличия работающих машин на группу адресов, либо опрос диапазона портов с целью определения работающих сервисов на одной машине или группе машин, а также выдача запросов, обработка которых не санкционирована принимающей стороной, не предусматривается сетевым сервисом или не разрешена администрацией ресурса.

11. Сканировать диапазоны IP-адресов (всю легально предоставляемую информацию об удаленной сети можно получить средствами DNS, traceroute и т.п.);

- 12.Использовать сеть во вред другим пользователям, путем самостоятельного или с помощью третьих лиц, вмешательства в действие аппаратуры и оборудования, а также иным способом;
- 13.Использовать доступ к компьютерным сетям для создания "сетевого шума" или "спама";
- 14.Рассылать не затребованную информацию по e-mail (спам), писем с указанием чужого адреса отправителя, писем угрожающего или оскорбляющего характера, "mailbombing", т.е. отправку писем, переполняющих почтовый ящик получателя и препятствующих получению новой почты;
- 15.Распространять информацию, оскорбляющую честь и достоинство других пользователей и персонала компьютерных сетей;
- 16.Физически повреждать оборудование сети;
- 17.Устанавливать серверные операционные системы без специального разрешения системного администратора;
- 18.Пользователям, работающим с конфиденциальными документами категорически запрещается пользоваться на рабочем месте различного рода мессенджерами (ICQ, MSN, Miranda, QIP, Mail.Ru агентами, Google messenger и т.д.);
- 19.Просмотр видео и прослушивание аудио через сеть, за исключением случаев, связанных со служебной необходимостью;
- 20.Хранение на локальных и публичных сетевых дисках файлов, не относящихся к выполнению служебных обязанностей сотрудника (игры, видео, музыку, фотографии, виртуальные CD и т.п.);
- 21.Просмотр в рабочее время сайтов развлекательной направленности и сайтов, содержание которых не относится напрямую к служебным обязанностям работника;
- 22.Играть в рабочее время в онлайн игры;
- 23.Устанавливать нелицензионное программное обеспечение, а также свободно распространяемое (FreeWare) программное обеспечение, способное нарушить работу локальной сети;
- 24.Разрабатывать или распространять любые виды компьютерных вирусов, «троянских коней» или «логических бомб»;
- 25.Открывать файлы и запускать программы на локальном компьютере из непроверенных источников или принесённых с собой на

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УИТ

переносных носителях без предварительной проверки
антивирусной программой.

26. Самовольная организация доступа к локальной сети УИТ через
машины конечных пользователей или другие устройства.

27. Использование различных сайтов анонимайзеров;

28. Использовать локальную сеть в деятельности, противоречащих
законодательству Республики Узбекистан.

ИНСТРУКЦИЯ ПО ПАРОЛЬНОЙ ЗАЩИТЕ

Данная Положения регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационной системе а также контроль действий пользователей и обслуживающего персонала системы при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администратора по ИБ, содержащих механизмы идентификации и аутентификации (подтверждения подлинности) пользователей по значениям паролей.

Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ИС самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы, цифры и специальные символы (@, #, \$, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и т.д.), а также общепринятые сокращения;
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
- пользователь не имеет права сообщать личный пароль никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

В случае, если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на ответственного сотрудника по информационной безопасности. Для генерации «стойких» значений паролей могут применяться специальные программные средства.

В случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п. может возникнуть необходимость использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие. Эти сотрудники обязаны сразу же после смены своих паролей передать их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте или опечатанном пенале на хранение

ответственному за информационную безопасность подразделения (руководителю своего подразделения). Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе. Для опечатывания конвертов (пеналов) должны применяться личные печати владельцев паролей (при наличии), либо печать уполномоченного представителя отдела обеспечения информационной безопасности.

2. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в три месяца.

Внеплановая смена личного пароля или удаление учетной записи пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться уполномоченными сотрудниками отдела обеспечения информационной безопасности – администраторами соответствующих средств защиты немедленно после окончания последнего сеанса работы данного пользователя с системой

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и другие обстоятельства) администраторов средств защиты и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем ИС.

3. Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у ответственного за информационную безопасность или руководителя подразделения в опечатанном личной печатью пенале.

Повседневный контроль действий исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственных за информационную безопасность в подразделениях (руководителей подразделений), периодический контроль – возлагается на ответственного сотрудника по информационной безопасности.

ИНСТРУКЦИЯ ПО РАБОТЕ С СЕТЬЮ ИНТЕРНЕТ И КОРПОРАТИВНОЙ ЭЛЕКТРОННОЙ ПОЧТОЙ

Глобальная сеть Интернет предоставляет доступ к ресурсам различного содержания и направленности. УИТ оставляет за собой право ограничивать доступ к ресурсам сети Интернет, содержание которых не имеет отношения к исполнению служебных обязанностей, а так же к ресурсам, содержание и направленность которых запрещены международным законодательством и законодательством Республики Узбекистан, 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.

При работе с ресурсами сети Интернет недопустимо:

- (разглашение информации ограниченного доступа УИТ, ставшей известной сотруднику Организации по служебной необходимости либо иным путем;

- распространение защищаемых авторскими правами материалов, затрагивающих какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;

- публикация, загрузка и распространение материалов, содержащих 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, имени пользователей, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также размещения ссылок на вышеуказанную информацию.

При работе с ресурсами Интернет запрещается:

- фальсифицировать свой IP-адрес;
- переходить по ссылкам и открывать вложенные файлы входящих электронных сообщений, полученных от неизвестных отправителей;

- осуществлять попытки несанкционированного доступа к ресурсам сети, проведение сетевых атак и сетевого взлома и участие в них;

- загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом;

- использовать анонимные прокси-серверы;
- использовать программные и аппаратные средства, позволяющие получить доступ к ресурсу, запрещенному к использованию политикой УИТ.

Возможность получить доступ к ресурсу не является гарантией того, что запрошенный ресурс является разрешенным политиками УИТ.

Вся информация о ресурсах, посещаемых сотрудниками УИТ, протоколируется и, при необходимости, может быть предоставлена руководителям подразделений, а также руководству УИТ для детального изучения.

С КОРПОРАТИВНОЙ ЭЛЕКТРОННОЙ ПОЧТОЙ

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

Электронная почта является собственностью УИТ и может быть использована только в служебных целях. Использование электронной почты в других целях категорически запрещено.

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 **УИТ** запрещается:

- использовать адрес корпоративной почты для оформления подписок, без предварительного согласования с руководством;
- публиковать свой адрес, либо адреса других сотрудников на общедоступных Интернет ресурсах (форумы, конференции и т.п.);
- отправлять сообщения с вложенными файлами, общий объем которых превышает 20 Мегабайт.
- открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами, даже если отправитель письма хорошо известен;
- осуществлять массовую рассылку почтовых сообщений (более 10) внешним адресатам без их на то согласия. Данные действия квалифицируются как спам и являются незаконными.
- осуществлять массовую рассылку почтовых сообщений рекламного характера без предварительного согласования с руководством;
- 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, имени пользователей, 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 законодательством и законодательством Республики Узбекистан 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;

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