КГУ «Управление архитектуры и градостроительства города Алматы»

УТВЕРЖДЕНО

Начальник Управления архитектуры и градостроительства города Алматы

_____ Ахмеджанов А. Т.

«14» января 2019 г.

М. П.

Правила использования сети интернет и электронной почты Информационной системы «3D автоматизированная геоинформационная система города Алматы» 3DГЕО.СМИБ.ПР.09.г01.19

г. Алматы
2019 г.

1. Область применения

Целью настоящего документа является описание правил использования сети интернет и электронной почты, и определение порядка действий ответственных сотрудников Организации, а также определение ответственности при проведении этих мероприятий или нарушении требований настоящего Документа.

Настоящий документ обязателен для исполнения в рамках проекта ИС.

2. Нормативные ссылки

Настоящий документ содержит указания к практическому исполнению требований изложенных в нормативных документах согласно п. 3 Нормативные ссылки действующей Политики информационной безопасности.

3. Термины, определения и сокращения

В настоящем документе используются термины и сокращения, принятые в действующей Политике информационной безопасности.

4. Общие положения

Доступ к электронной почте предоставляется всем сотрудникам проекта ИС, на рабочем месте которых установлен персональный компьютер, подключенный к сети Интернет, согласно утверждённым политикам и процедурам ИБ.

Доступ к сети Интернет и службам Интернет-сообщений предоставляется по заявке, согласованной с СОИБ в порядке и по форме согласно утвержденной Политике информационной безопасности.

При этом обоснование доступа к сети Интернет должно содержать указание на необходимость постоянной оперативной работы.

Доступ к Интернету служащим ГО и МИО предоставляется с рабочих станций, подключенных к ЛС внешнего контура ГО и МИО, размещенных за пределами режимных помещений, определяемых в соответствии с Инструкцией по обеспечению режима секретности в Республике Казахстан.

Взаимодействие ведомственной электронной почты ГО с внешними электронными почтовыми системами должно осуществляться только через единый шлюз электронной почты.

Доступ к сети Интернет должен осуществляться только через специализированный proxy-сервер настроенный для мониторинга и контроля доступа в Интернет.

5. Обеспечение информационной безопасности

Пользователи электронной почты и сети Интернет обязаны:

– осуществлять доступ в Интернет только с закрепленной за ними рабочей станции;

– осуществлять контроль за систематическим обновлением антивирусных баз на закрепленной за ними рабочей станции в установленном документами по ИБ порядке;

– немедленно завершить работу в сети Интернет, обратиться к СОИБ, запустить антивирусную проверку рабочей станции в случаях отклонений в нормальном функционировании рабочей станции, а также выдачи предупреждений антивирусных программ;

– проверять на наличие вирусов информацию, полученную из сети Интернет и электронной почты;

– в случае изменения регистрационных данных работника, имеющего доступ в сеть Интернет (ФИО, имя пользователя, IP-адрес и MAC-адрес рабочей станции), в течение суток сообщить новые данные менеджеру проекта и ответственному за обеспечение ИБ.

При использовании электронной почты и служб Интернет сотрудникам проекта запрещается:

– использовать ресурсы для агитации или рекламы коммерческих предприятий, пропаганды религиозных или политических идей, иных целей, не связанных с выполнением служебных обязанностей;

– опубликовывать адреса электронной почты на общедоступных Интернет ресурсах (форумы, конференции, социальные сети и т.п.);

– создавать оскорбительные или провокационные сообщения. Таковыми считаются сообщения, содержащие сексуальные домогательства, расовые оскорбления, дискриминацию по половому признаку или другие комментарии, затрагивающие в оскорбительной форме вопросы возраста или сексуальной ориентации, религиозные или политические пристрастия, национальность или состояние здоровья, а также другую информацию, запрещенную законодательством Республики Казахстан;

– использовать вложения графических, видео, исполняемых и т.п. файлов, не относящихся к служебной деятельности;

– предоставлять кому-либо учетную запись и пароль для доступа к электронной почте и получать доступ к электронным сообщениям других пользователей (за исключением случаев, санкционированных руководством);

– открывать или запускать файлы, прикрепленные к почтовым сообщениям, в случае отсутствия достаточной уверенности в надежности источника;

– осуществлять вложение файлов при использовании служб Интернет-сообщений.

– использовать Интернет в целях передачи и распространения материалов, содержащих конфиденциальную информацию с ограниченным доступом и/или распространением в открытом (незашифрованном) виде с использованием средств криптографической защиты информации;

– запрашивать и отправлять сообщения, содержащие сведения составляющие государственные секреты и иную служебную и/или конфиденциальную информацию с ограниченным доступом и/или распространением в открытом (незашифрован с использованием государственных шифровальных средств – средств криптографической защиты информации (СКЗИ)) виде, а также с использованием зарубежных почтовых серверов;

– пользоваться групповой рассылкой в личных целях;

– использовать ресурсы для рассылки писем-пирамид, писем «счастья», сообщений рекламного характера и другой подобной информации, не имеющей отношения к служебной деятельности;

– распространять вредоносные файлы и программы, а также программное обеспечение и материалы, защищенные авторским правом;

– использовать учетные записи других почтовых систем и пользователей;

– получать доступ к электронным сообщениям других пользователей (за исключением случаев, санкционированных руководством или их владельцем);

– распространять в сети Интернет оскорбительные и провокационные заявления;

– посещать веб-сайты, содержащие материалы террористической, экстремисткой, антиконституционной и иной деструктивной направленности;

– посещать сомнительные и вредоносные сайты, а также сайты, информация на которых не связана с исполнением функциональных обязанностей;

– загружать (передавать) вредоносные файлы и программы, программное обеспечение и материалы, защищенные авторским правом, а также мультимедийные файлы всех типов;

– использовать службы Интернет-чатов;

– разглашать присвоенное имя пользователя, пароль, ключи шифрования, сертификаты, ЭЦП учетной записи ИС;

– предоставлять доступ в сеть Интернет с закрепленной рабочей станции другим лицам;

– скачивать из сети Интернета, а также передавать информацию, не связанную с выполнением служебных обязанностей, нелицензионное программное обеспечение, мультимедийные и графические файлы, игры и т.д.;

– играть в онлайн-игры, прослушивать и просматривать мультимедийные файлы из сети Интернет онлайн;

– переходить по подозрительным ссылкам;

– регистрироваться и вести общение в социальных сетях (Мой мир, Одноклассники, Вконтакте и т.д.) и на сайтах, не связанных с выполнением служебных обязанностей;

– игнорировать предупреждения антивирусного программного обеспечения;

– открывать или запускать любые файлы, приведенные в Приложении 1, прикрепленные к почтовым сообщениям или полученные из сети Интернет, в случае отсутствия достаточной уверенности в надежности источника;

– подключаться к сети Интернет посредством мобильного телефона, коммуникатора, беспроводной сети, неслужебной рабочей станции, в том числе ноутбука, менять настройки доступа в сеть Интернет на закрепленной рабочей станции.

а. Требования к оформлению электронного сообщения

Все электронные письма должны быть оформлены в соответствии с требованиями:

- тему письма,
- должно содержать приветствие получателя,
- дату, время отправки,
- предупреждение о конфиденциальности: «Данное сообщение (включая любые вложения) может содержать конфиденциальную информацию и быть предназначенным исключительно для лица или организации, которой оно адресовано. Если Вы не являетесь надлежащим адресатом, то настоящим Вы уведомлены, что любое раскрытие, копирование, распространение или использование содержания этого сообщения строго запрещено. Если Вы получили это сообщение по ошибке, пожалуйста, поставьте нас в известность об этом немедленно, ответив на это письмо, и затем удалите его из своей системы. Спасибо».

6. Проведение проверок и ответственность

СОИБ осуществляет плановые (в рамках внутреннего аудита) и внеплановые (согласно приказа руководства Организации) проверки исполнения требований настоящего документа.

СОИБ проводит анализ инцидентов информационной безопасности по фактам нарушений требований защиты информации при работе с электронной почтой и Интернет.

В случае обнаружения фактов или выявления потенциальной угрозы информационной безопасности СОИБ немедленно информирует руководство Организации.

Содержимое электронного почтового ящика работника может быть проверено СОИБ без предварительного уведомления, а также по требованию руководства Организации с целью обеспечения безопасности, но только в присутствии его владельца.

За нарушения норм, предусмотренных настоящим документом, к сотрудникам Организации по представлению отчета СОИБ, может быть проведено служебное расследование и по его результатам применены меры дисциплинарного взыскания.

7. Ответственность

СОИБ несет ответственность за:

a) контроль исполнения требований настоящего документа,
b) исполнение настоящей Инструкции.

Сотрудники проекта ИС:

a) исполнение настоящей Инструкции.

Пользователи ИС:

a) исполнение настоящей Инструкции.

Приложение 1

Расширения файлов, запрещенных к загрузке из сети Интернет Информационной системы «3D автоматизированная геоинформационная система города Алматы» 3DГЕО.СМИБ.ПР.09-01.r01.19

.ACE	.BPL	.IT	.MIZ	.MTM	.STM	.WAL
.AIF	.CAB	.ITZ	.MOD	.NSV	.STZ	.WAV
.AIFC	.CDA	.LH	.MOV	.OGG	.TAR	.WAX
.AIFF	.COM	.LHA	.MPL	.PIS	.TGZ	.WM
.ARJ	.DAT	.LZH	.MP2	.PPS	.TIF	.WMA
.ASF	.DIVX	.MLV	.MP3	.PPT	.UC2	.WMV
.ASX	.DLL	.M2V	.MP4	.RAR	.ULT	.WMX
.AU	.DOC	.M3U	.MPA	.RMI	.UNIX	.WVX
.AVI	.EXE	.MDZ	.MPE	.S3M	.UUE	.XLS
.B4S	.GZ	.MID	.MPEG	.S3Z	.VOB .	.XMZ
.BAT	.IFO	.MIDI	.MPG	.SND	.VOC	.ZIP
				.SCR		