МАРИЙ ЭЛ РЕСПУБЛИКЫН
ЧОНГЫМАШ,
АРХИТЕКТУР ДЕН
ИЛЕМ-КОММУНАЛ
ОЗАНЛЫК
МИНИСТЕРСТВЫЖЕ

МИНИСТЕРСТВО
СТРОИТЕЛЬСТВА,
АРХИТЕКТУРЫ И ЖИЛИЩНО-
КОММУНАЛЬНОГО
ХОЗЯЙСТВА
РЕСПУБЛИКИ МАРИЙ ЭЛ

П Р И К А З

от 20 июня 2016 г. № 280

Об утверждении Инструкции по информационной безопасности в локальной вычислительной сети Министерства строительства, архитектуры и жилищно-коммунального хозяйства Республики Марий Эл и информационно-телекоммуникационной сети «Интернет»

В целях упорядочения доступа должностных лиц Министерства строительства, архитектуры и жилищно-коммунального хозяйства Республики Марий Эл к информационным ресурсам локальной вычислительной сети Министерства строительства, архитектуры и жилищно-коммунального хозяйства Республики Марий Эл и информационно-телекоммуникационной сети «Интернет»

п р и к а з ы в а ю :

1. Утвердить прилагаемую Инструкции по информационной безопасности в локальной вычислительной сети Министерства строительства, архитектуры и жилищно-коммунального хозяйства Республики Марий Эл и информационно-телекоммуникационной сети «Интернет».

2. Руководителям структурных подразделений Министерства строительства, архитектуры и жилищно-коммунального хозяйства Республики Марий Эл (далее – Министерства):

при работе с информационными ресурсами Министерства руководствоваться настоящей Инструкцией;

обеспечить ознакомление всех сотрудников структурных подразделений Министерства с настоящей Инструкцией.

3. Возложить обязанности по администрированию доступа должностных лиц Министерства к локальной вычислительной сети

Министерства и информационно-телекоммуникационной сети «Интернет» на главного специалиста-эксперта Зарубина К.В., консультанта Кузнецова А.Ю.

4. Приказ Минстроя и ЖКХ Республики Марий Эл от 14 сентября 2015 г. № 485 «Об утверждении Инструкции по информационной безопасности в локальной вычислительной сети Министерства строительства, архитектуры и жилищно-коммунального хозяйства Республики Марий Эл и информационно-телекоммуникационной сети «Интернет» признать утратившим силу.

Министр Э.В.Варенова

Зарубин К.В.
63-80-46

УТВЕРЖДЕНА
приказом Министерства строительства,
архитектуры и ЖКХ Республики Марий Эл
от 20 июня 2016 г. № 280

ИНСТРУКЦИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ МИНИСТЕРСТВА СТРОИТЕЛЬСТВА, АРХИТЕКТУРЫ И ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА РЕСПУБЛИКИ МАРИЙ ЭЛ И ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ»

1. Общие положения.

1.1. Целью инструкции по информационной безопасности в локальной вычислительной сети Министерства строительства, архитектуры и жилищно-коммунального хозяйства Республики Марий Эл и информационно-телекоммуникационной сети «Интернет» (далее – Инструкция) Министерства строительства архитектуры и жилищно-коммунального хозяйства Республики Марий Эл (далее – Министерство) является регулирование работы администраторов информационной безопасности и пользователей, распределения сетевых ресурсов коллективного пользования и поддержания необходимого уровня защиты информации, ее сохранности и соблюдения прав доступа к информации. Более эффективного использования сетевых ресурсов и уменьшить риск умышленного или неумышленного неправильного их использования.

1.2. Инструкция является обязательной для выполнения всеми сотрудниками - пользователями локальной вычислительной сети Министерства и информационно-телекоммуникационной сети «Интернет» в части, касающейся их.

1.3. В инструкции используются следующие сокращения и основные понятия:

ПК – персональный компьютер;

ПО – программное обеспечение;

ЛВС – локальная вычислительная сеть Министерства;

сеть Интернет - информационно-телекоммуникационная сеть «Интернет»;

пользователь – сотрудник Министерства, выполнение должностных обязанностей которого связано с использованием ПК в ЛВС Министерства и сети Интернет;

информационные ресурсы - отдельные документы и отдельные массивы документов, базы данных, другие виды информационного обеспечения с использованием ПК;

администратор – сотрудник ИТ службы, ответственный за подключение к ЛВС, сети Интернет и обеспечение работоспособности, надежности сети, сохранности и защиты информационных ресурсов (администратор информационной безопасности);

ИТ служба – отдел формирования информационных ресурсов в градостроительстве Министерства;

1.4. 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.

1.5. Доступ к ЛВС и сети Интернет осуществляется с рабочего ПК пользователя. Ответственность за действия на ПК другого человека, несет пользователь ПК с которого совершено это действие.

1.6. Работа в ЛВС и сети Интернет каждому работнику разрешена только на определенных ПК, в определенное время и только с разрешенным ПО и сетевыми

ресурсами. При возникновении необходимости работы на других ПК и с другим ПО, необходимо получить разрешение у администратора.

1.7. Для получения допуска к работе в ЛВС и сети Интернет, работнику необходимо пройти инструктаж, регистрацию у администратора.

1.8. По уровню ответственности и правам доступа к ЛВС пользователи разделяются на следующие категории: администраторы и пользователи.

1.9. Пользователь подключенного к ЛВС компьютера - лицо, за которым закреплена ответственность за данный компьютер. Пользователь должен принимать все необходимые меры по защите информации и контролю за соблюдением прав доступа к ней.

1.10. Каждый сотрудник пользуется индивидуальным именем пользователя для своей идентификации в ЛВС, выдаваемым администратором.

1.11. Каждый сотрудник должен пользоваться только своим именем пользователя и паролем для входа в ЛВС, передача их кому - либо запрещена.

1.12. Для работы на ПК кроме закрепленного пользователя необходимо разрешение администратора. Никто не может давать разрешение даже на временную работу на ПК без разрешения администратора.

1.13. В случае нарушения правил пользования ЛВС, связанных с закрепленным за пользователем ПК, пользователь сообщает администратору, который проводит расследование причин и выявление виновников нарушений и принимает меры к пресечению подобных нарушений. Если виновником нарушения является пользователь данного ПК, администратор имеет право отстранить виновника от использования ПК или принять иные меры.

1.14. В случае появления у пользователя ПК сведений или подозрений о фактах нарушения настоящих правил, а в особенности о фактах несанкционированного доступа к информации, размещенной на контролируемом им ПК пользователь должен немедленно сообщить об этом администратору.

1.15. Администратор дает разрешение на подключение компьютера к ЛВС и сети Интернет. Самовольное подключение является серьезнейшим нарушением правил пользования ЛВС и сети Интернет.

1.16. Администратор информирует пользователей обо всех плановых профилактических работах, которые могут привести к частичной или полной неработоспособности ЛВС и сети Интернет на ограниченное время.

1.17. Администратор имеет право отключить компьютер пользователя от ЛВС и сети Интернет в случае, если с данного ПК производились попытки несанкционированного доступа к информации на других ПК, и в случаях других серьезных нарушений настоящей инструкции.

2. Требования к пользователю ЛВС.

2.1. Соблюдать правила работы в ЛВС, оговоренные настоящей инструкцией.

2.2. При доступе к внешним ресурсам, соблюдать правила, установленные администратором для используемых ресурсов.

2.3. Немедленно сообщать администратору об обнаруженных проблемах в использовании предоставленных ресурсов, а также о фактах нарушения настоящей инструкции кем-либо. Администратор, при необходимости, с помощью других специалистов, должен провести расследование указанных фактов и принять соответствующие меры.

2.4. Не разглашать известную им конфиденциальную информацию (имена пользователей, пароли), необходимую для безопасной работы в ЛВС.

2.5. Немедленно отключать от ЛВС ПК, который подозревается в заражении вирусом. ПК не должен подключаться к ЛВС до тех пор, пока администратор не удостоверится в удалении вируса.

2.6. Обеспечивать беспрепятственный доступ администратору к сетевому оборудованию и ПК пользователей.

2.7. Выполнять предписания администратора, направленные на обеспечение безопасности ЛВС.

2.8. В случае обнаружения неисправности компьютерного оборудования или ПО, пользователь должен обратиться к администратору.

3. Пользователи ЛВС имеют право:

3.1. Использовать в работе предоставленные им сетевые ресурсы в оговоренных в настоящей инструкции рамках, если иное не предусмотрено по согласованию с отделом ИТ. Администратор вправе ограничивать доступ к некоторым сетевым ресурсам вплоть до их полной блокировки, изменять распределение трафика и проводить другие меры, направленные на повышение эффективности использования сетевых ресурсов.

3.2. Обращаться к администратору по вопросам, связанным с распределением ресурсов ПК. Какие-либо действия пользователя, ведущие к изменению объема используемых им ресурсов, или влияющие на загруженность или безопасность системы (например, установка на ПК коллективного доступа), должны санкционироваться администратором.

3.3. Обращаться за помощью к администратору при решении задач использования ресурсов ЛВС и сети Интернет.

3.4. Вносить предложения по улучшению работы с ресурсом.

4. Пользователям ЛВС запрещено:

4.1. Допускать к работе с ПК и сетью Интернет посторонних лиц.

4.2. Использовать ПО, не предназначенное для выполнения прямых служебных обязанностей без согласования с администратором.

4.3. Самостоятельно устанавливать прикладное, операционное, сетевое и другие виды ПО, а также осуществлять обновления, если эта работа не входит в его должностные обязанности.

4.4. Повреждать, уничтожать или фальсифицировать информацию, не принадлежащую пользователю.

4.5. Вскрывать ПК, сетевое и периферийное оборудование; подключать к ПК дополнительное оборудование без ведома администратора, изменять настройки BIOS ПК, а также производить загрузку ПК с дисков или флэш-накопителей.

4.6. Самовольно подключать ПК к ЛВС, а также изменять IP-адрес ПК, выданный администратором. Передача данных в сеть с использованием других IP-адресов в качестве адреса отправителя является распространением ложной информации и создает угрозу безопасности информации на других ПК.

4.7. Получать и передавать в сеть информацию, противоречащую законодательству и нормам морали общества, представляющую коммерческую или государственную тайну, распространять через сеть информацию, задевающую честь и достоинство граждан, а также рассылать обманные, беспокоящие или угрожающие сообщения.

4.8. Обхождение учетной системы безопасности, системы статистики, ее повреждение или дезинформация.

4.9. Использовать иные формы доступа к сети Интернет, за исключением разрешенных администратором: пытаться обходить установленный межсетевой экран при соединении с информационно-телекоммуникационной сети «Интернет».

4.10. Осуществлять попытки несанкционированного доступа к ресурсам ЛВС и сети Интернет, проводить или участвовать в сетевых атаках и сетевом взломе.

4.11. Использовать ЛВС и сеть Интернет для совершения коммерческих сделок, распространения рекламы, коммерческих объявлений, порнографической информации,

призывов к насилию, разжиганию национальной или религиозной вражды, оскорблений, угроз и т.п.

4.12. Пользователи должны уважать право других пользователей на личную информацию. Это означает, что пользователь (администратор) не имеет права пользоваться чужими именами и паролями, читать чужую почту, причинять вред данным (кроме случаев, указанных выше), принадлежащих другим пользователям.

4.13. Производить действия, направленные на взлом (несанкционированное получение привилегированного доступа) рабочих станций и сервера ЛВС, равно как и любых других ПК в сети Интернет.

4.14. Закрывать доступ к информации паролями без согласования с администратором.

4.15. Использовать ПО для удаленного доступа.

4.16. Нарушение закона об авторском праве: копирование и использование материалов, защищенных законом об авторском праве.

4.17. 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.

4.18. Распространять информацию ограниченного доступа, предназначенную для служебного использования.

4.19. Подключать к ПК мобильные телефоны, смартфоны, модемы, USB-модемы, фотоаппараты, планшетные компьютеры, электронные книги, непроверенные флэш-накопители и т.п.

5. Работа с электронной почтой:

5.1. Электронная почта Министерства предоставляется сотрудникам только для выполнения своих служебных обязанностей. Использование ее в личных целях запрещено.

5.2. Запрещено использовать личную электронную почту для служебных целей.

5.3. Входящие письма должны проверяться на наличие вирусов или других вредоносных программ.

5.4. Запрещено публиковать электронные адреса и персональные данные сотрудников Министерства на общедоступных Интернет-ресурсах (форумы, конференции и т.п.).

5.5. Никто из посетителей или временных служащих не имеет права использовать электронную почту Министерства.

5.6. Исходящие сообщения могут быть выборочно проверены, чтобы гарантировать соблюдение правил работы с электронной почтой.

5.7. Пользователи не должны позволять кому-либо посылать письма от чужого имени.

5.8. В качестве клиентов электронной почты могут использоваться только утвержденные администратором почтовые программы.

5.9. Конфиденциальная информация не может быть послана с помощью электронной почты.

5.10. Запрещено открывать или запускать приложения, полученные по электронной почте от неизвестного источника и (или) не затребованные пользователем.

5.11. Запрещено осуществлять массовую рассылку не согласованных предварительно электронных писем. Под массовой рассылкой подразумевается как рассылка множеству получателей, так и множественная рассылка одному получателю (спам).

5.12. Запрещено использовать несуществующие обратные адреса при отправке электронных писем.

5.13. Запрещено переходить по ссылкам в электронных письмах.

5.14. Запрещено использование на рабочих местах иностранных коммуникационных Интернет-сервисов электронной почты (Gmail, Yahoo, Microsoft и т.д.).

5.15. Запрещено использование на рабочих местах для служебной переписки следующих коммуникационных Интернет-сервисов электронной почты - Mail.ru, Yandex.ru, Rambler.ru и т.д.

5.15. Запрещено рассылать через электронную почту материалы, содержащие вирусы или другие компьютерные коды, файлы или ПО, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или ПО для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и ПО для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в сети Интернет, а также ссылки на вышеуказанную информацию.

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

6. Работа в сети Интернет:

6.1. Доступ к сети Интернет осуществляется с рабочего ПК пользователя. Ответственность за действия на ПК другого человека, несет пользователь ПК с которого совершено это действие.

6.2 Пользователи используют ПО для поиска информации в сети Интернет только в случае, если это необходимо для выполнения своих должностных обязанностей.

6.3. Использовать ресурсы сети Интернет разрешается только в служебных целях, использование её ресурсов не должно потенциально угрожать ЛВС Министерства.

6.4. Работа пользователей в сети Интернет отслеживается с помощью специального ПО. На основе логов (истории посещений) проводится анализ по следующим параметрам: перечень используемых ресурсов, объем трафика.

6.5. Статистика работы пользователей с сетью Интернет доступна только администратору, руководителю ИТ службы, министру и может служить причиной отключения определенных ресурсов, и принятия решений об изменении прав доступа пользователя к сети Интернет.

6.6. Все ПО, используемое для доступа к сети Интернет, должно быть утверждено администратором.

6.7. Все файлы, загружаемые с помощью сети Интернет, должны проверяться на вирусы утвержденным администратором.

6.8. Запрещено размещать в гостевых книгах, форумах, конференциях сообщения, содержащие грубые и оскорбительные выражения.

6.9. Запрещено получать доступ к информационным ресурсам ЛВС, сети Интернет, не являющихся публичными, без разрешения их собственника.

6.10. Запрещено посещение пользователем ресурсов с непристойным содержанием (эротико-порнографические ресурсы, нацистские или националистические ресурсы, ресурсы, призывающие к насилию).

6.11. Запрещено посещение игровых, развлекательных и прочих сайтов, не имеющих отношения к деятельности Министерства и деятельности пользователя.

6.12. Запрещено посещение ресурсов трансляции потокового видео и аудио (веб-камеры, трансляция ТВ- и музыкальных программ в сети Интернет), создающих большую загрузку сети и мешающих нормальной работе остальных пользователей.

6.13. Запрещена загрузка материалов порнографического содержания, компьютерных игр, других развлекательных материалов.

6.14. Запрещено переходить по сомнительным ссылкам и рекламным баннерам на сайтах, ведущие на другие ресурсы сети Интернет, а также нажимать на всплывающие окна и сообщения.

6.15. Запрещено использование на рабочих местах сервисов обмена «мгновенными сообщениями» (ICQ, QIP, WatsApp, Telegram, Mail.ru-агент, Jabber, Skype и др.).

6.16. Запрещено использование на рабочих местах иностранных поисковых систем (Google, Yahoo, Bing и др.).

6.17. Запрещено использование на рабочих местах коммуникационных облачных сервисов (iCloud, Google Drive, Dropbox, SkyDrive, Облако Mail.ru, Яндекс.Диск и т.д.).

6.18. Запрещено использование на рабочих местах файлообменных сервисов (RapidShare, iFolder, DepositFiles, MediaFire, LetitBit, Box.net, UploadBOX, Drop.io, narod.yandex.ru, magaupload и т.д.).

6.19. Запрещено использование на рабочих местах социальных сетей (Google+, Facebook, Twitter, Одноклассники, ВКонтакте и т.д.).

6.20. Запрещено использование ПО для работы с P2P сетями (µTorrent, BitTorrent и т.п.).

6.21. Запрещено создание личных веб-страниц и хостинг (размещение web- или ftp-сервера) на ПК пользователя.

6.22. Запрещены любые попытки деструктивных действий по отношению к нормальной работе ЛВС Министерства и сети Интернет (рассылка вирусов, ip-атаки и т.п.).

6.23. В Министерстве действует система контроля доступа к сети Интернет, предусматривающая автоматические ограничения.

7. Резервное копирования информации:

7.1. Пользователи ПК обязаны хранить копию важной информации на файловом сервере Министерства в соответствующей папке структурного подразделения или на внешнем накопителе, который необходимо хранить в надежном месте.

7.2. Начальники структурных подразделений, заместители начальников структурных подразделений обязаны контролировать выполнение сотрудниками резервного копирования информации.

7.3. Резервному копированию подлежит только служебная информация.

8. Ответственность:

8.1. Пользователь ПК отвечает за информацию, хранящуюся на его ПК, технически исправное состояние ПК и вверенной техники.

8.2. Администратор отвечает за бесперебойное функционирование вверенной ему ЛВС.

8.3. Администратор обязан контролировать исполнение пользователями ПК в ЛВС соблюдения положений Инструкции, а также осуществлять проверку знания настоящей Инструкции.

8.4. Пользователь несет личную ответственность за весь информационный обмен между его ПК и другими ПК в ЛВС и за ее пределами.

8.5. За нарушение настоящей инструкции пользователь может быть отстранен от работы с ЛВС и сетью Интернет.

8.6. Нарушение данной инструкции, повлекшее уничтожение, блокирование, модификацию либо копирование охраняемой законом компьютерной информации, нарушение работы ПК пользователей или ЛВС, может повлечь административную или уголовную ответственность в соответствии с действующим законодательством.