АДМИНИСТРАЦИЯ
ГОРОДА РОСТОВА-НА-ДОНУ

РАСПОРЯЖЕНИЕ

24.04.2017 № 102

О внесении изменений в распоряжение Администрации города Ростова-на-Дону от 09.09.2014 № 375 «Об утверждении Положения о локальной вычислительной сети Администрации города Ростова-на-Дону»

В соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 19.12.2016), в целях повышения информационной безопасности:

1. Внести в распоряжение Администрации города Ростова-на-Дону от 09.09.2014 № 375 «Об утверждении Положения о локальной вычислительной сети Администрации города Ростова-на-Дону» следующие изменения:

1.1. В приложении:

1.1.1. В абзаце четвертом пункта 1.2 раздела 1 после слов «Администрация города» слова «отдел электронно-информационных технологий» заменить словами «управление информационных технологий».

1.1.2. Раздел 4 дополнить пунктами 4.7, 4.8, 4.9, 4.10 следующего содержания:

«4.7. Порядок эксплуатации помещений, в которых располагаются рабочие станции пользователей, серверное и телекоммуникационное оборудование ЛВС, организуется таким образом, чтобы исключалась или значительно затруднялась возможность неконтролируемого проникновения или пребывания в них посторонних лиц. При оставлении работниками этих помещений они запираются на ключ.

4.8. Помещение, в котором располагаются сервера ЛВС (далее – серверное помещение), оборудуется охранной и пожарной сигнализацией, прочными входными дверьми с надежными замками и приспособлениями для опечатывания.

4.9. В нерабочее время серверное помещение сдается под охрану

(наблюдение). При этом охранная сигнализация должна быть включена, окна надежно закрыты, двери опечатаны, съемные машинные носители информации ограниченного доступа и аппаратные аутентификаторы убраны в надежно запираемые шкафы (ящики, хранилища), средства вычислительной техники выключены либо заблокированы.

4.10. Доступ работников Администрации города Ростова-на-Дону в серверное помещение осуществляется по списку, утверждаемому начальником управления информационных технологий Администрации города Ростова-на-Дону (далее – управление ИТ).

Уборка и другие необходимые хозяйственные работы в серверном помещении должны производиться в присутствии ответственных лиц, которым разрешен доступ в это помещение. Во время уборки и хозяйственных работ должны быть приняты меры по недопущению несанкционированного доступа к техническим средствам и защищаемой информации».

1.1.3. В разделе 5:

1.1.3.1. Пункт 5.1 изложить в редакции:

«5.1. Администратор ЛВС назначается правовым актом Администрации города Ростова-на-Дону».

1.1.3.2. В пункте 5.3 после слов «ЛВС обеспечивает» слова «отдел ЭИТ» заменить словами «управление ИТ».

1.1.3.3. В пункте 5.8 после слов «прохождения инструктажа, проводимого» слова «отделом ЭИТ» заменить словами «управлением ИТ».

1.1.3.4. Пункт 5.8 дополнить абзацем третьим следующего содержания:

«После проведения инструктажа пользователю сообщаются реквизиты присвоенной ему учетной записи в ЛВС, включающие в себя имя пользователя (логин), имя домена и пароль, специально созданный работниками управления ИТ для осуществления пользователем первого доступа к ЛВС (далее – первичный пароль)».

1.1.3.5. В пункте 5.10 после слов «до сведения» слова «отдела ЭИТ» заменить словами «управления ИТ».

1.1.3.6. В подпункте 5.11.2 пункта 5.11 после слов «сообщать об этом в» слова «отдел ЭИТ» заменить словами «управление ИТ».

1.1.3.7. Пункт 5.11 дополнить подпунктом 5.11.10 следующего содержания:

«5.11.10. При выходе из рабочего кабинета, в том числе временном, выключать компьютер или блокировать его с помощью запуска парольной заставки».

1.1.3.8. В подпункте 5.12.8 пункта 5.12 после слов «без согласования с» слова «отделом ЭИТ» заменить словами «управлением ИТ».

1.1.3.9. Подпункт 5.12.11 пункта 5.12 изложить в редакции:

«5.12.11. Использовать при работе в ЛВС неучтенные машинные носители информации».

1.1.3.10. В подпункте 5.17.2 пункта 5.17 после слов «настоящего раздела» слова «отдел ЭИТ» заменить словами «управление ИТ».

1.1.4. Дополнить разделами 9, 10, 11 следующего содержания:

«9. Порядок парольной защиты ЛВС

9.1. Парольная защита ЛВС осуществляется путем реализации комплекса организационных и технических мер по генерации и/или созданию, использованию, хранению, уничтожению паролей пользователей в процессе их идентификации и аутентификации при доступе к ЛВС и ее ресурсам.

9.2. Соблюдение требований порядка парольной защиты ЛВС является обязательной мерой безопасности и защиты информации, применяемой пользователями ЛВС в отношении всех рабочих станций, серверов и программных ресурсов ЛВС, с целью предотвращения несанкционированного доступа к ним.

9.3. Организационно-методическое обеспечение процесса организации парольной защиты ЛВС и периодический контроль выполнения работниками Администрации города Ростова-на-Дону требований порядка парольной защиты ЛВС осуществляет управление ИТ.

Работники Администрации города Ростова-на-Дону обязаны предъявлять значения своих паролей доступа к ЛВС работникам управления ИТ, проводящим контроль выполнения требований порядка парольной защиты ЛВС, с обязательной последующей сменой пароля.

9.4. Используемые в ЛВС пароли доступа должны соответствовать следующим требованиям к сложности паролей.

9.4.1. Пароли доступа к ЛВС должны состоять из комбинации прописных и строчных букв английского алфавита, арабских цифр и специальных символов (например: @, #, $, %, ^, &, * и т.п.).

9.4.2. Пароли доступа к программным и информационным ресурсам ЛВС и к базовой системе ввода/вывода (BIOS) рабочих станций и серверов ЛВС должны состоять из комбинации прописных и строчных букв английского алфавита и арабских цифр.

9.4.3. Пароли администратора ЛВС для доступа к ЛВС и к базовой системе ввода/вывода (BIOS) рабочих станций и серверов ЛВС должны состоять не менее чем из 8, но не более чем из 32 знаков.

9.4.4. Пароль пользователя ЛВС для доступа к ЛВС должен состоять не менее чем из 6, но не более чем из 16 знаков.

9.4.5. Пароли администратора и пользователя ЛВС для доступа к программным и информационным ресурсам ЛВС должны состоять не менее чем из 6, но не более чем из 14 знаков.

9.4.6. Пароли доступа не должны содержать личных имен, фамилий, кличек домашних животных, номеров телефонов, дат рождения, географических названий, общепринятых сокращений и других данных, которые могут быть подобраны путем анализа информации о владельце пароля.

В качестве пароля не может быть использован один и тот же повторяющийся символ либо повторяющаяся комбинация из нескольких символов, либо комбинация символов, набираемых в закономерном порядке

на клавиатуре (например: qwerty, 1234567 или 1qazxsw2 и т. п.).

9.4.7. При смене паролей доступа, новые пароли должны отличаться от заменяемых не менее чем шестью знаками.

Ранее использованные пароли не могут быть применены для осуществления парольной защиты вновь в течение трех лет.

9.5. Срок использования пароля пользователя ЛВС для доступа к ЛВС не должен превышать 180 дней.

9.6. Срок использования пароля администратора ЛВС для доступа к ЛВС не должен превышать 90 дней.

9.7. Первичный пароль, созданный работниками управления ИТ, должен быть сменен пользователем при первом доступе к ЛВС. В дальнейшем пароли для доступа к ЛВС создаются пользователями самостоятельно с учетом требований пункта 9.4 настоящего Положения.

9.8. В случае осуществления нескольких, повторяющихся одна за другой, неуспешных попыток аутентификации (ввода неправильного пароля) программно-техническое средство или учетная запись пользователя ЛВС должны быть заблокированы. Количество повторяющихся неуспешных попыток аутентификации, после которых программно-техническое средство или учетная запись пользователя ЛВС блокируются, устанавливается оператором ЛВС, но не должно превышать 10 попыток.

Разблокирование программно-технического средства или учетной записи пользователя ЛВС производится управлением ИТ на основании заявки, подписанной руководителем структурного подразделения Администрации города Ростова-на-Дону.

9.9. Резервные копии паролей администраторов для доступа к ЛВС, ее программным и информационным ресурсам и к базовой системе ввода/вывода (BIOS) рабочих станций и серверов ЛВС оформляются в виде парольной карты по форме согласно приложению № 2 к настоящему Положению.

Каждая парольная карта в отдельном опечатанном конверте (упаковке) сдается администраторами ЛВС и информационных ресурсов ЛВС на хранение в отдел информационной безопасности управления ИТ по журналу парольных карт. Форма журнала парольных карт приведена в приложении № 3 к настоящему Положению. На конверте указывается номер парольной карты и дата согласно журналу парольных карт.

Для опечатывания конвертов (упаковок) с парольными картами применяются оттиски мастичных печатей, номерные пломбировочные наклейки и иные средства, позволяющие осуществлять контроль за их вскрытием. На оттиск мастичной печати и номерную пломбировочную наклейку наносится дата опечатывания и роспись лица, опечатавшего конверт с парольной картой. Места нанесения и количество оттисков мастичной печати и номерных пломбировочных наклеек выбираются таким образом, чтобы исключалась возможность бесконтрольного вскрытия конверта или извлечения из него парольной карты.

9.10. Вскрытие конверта (упаковки) с парольной картой в отсутствие

работника, его опечатавшего, допускается по письменному указанию начальника управления ИТ, оформленному в журнале парольных карт. По прибытии на рабочее место работник, конверт (упаковка) с парольной картой которого был вскрыт, производит замену раскрытых паролей, оформляет новую парольную карту и передает ее на хранение в соответствии с пунктом 9.9 настоящего Положения.

9.11. В случае увольнения (перевода на другую работу) работника Администрации города Ростова-на-Дону, являющегося пользователем ЛВС, должна производиться смена пароля, соответствующего учетной записи этого пользователя. Смену пароля производит оператор ЛВС.

9.12. Руководители структурных подразделений Администрации города Ростова-на-Дону должны своевременно информировать управление ИТ об увольнении и иных кадровых перемещениях подчиненных работников, являющихся пользователями ЛВС.

9.13. В случае увольнения (перевода на другую работу) работников Администрации города Ростова-на-Дону, которые выполняли функции по администрированию ЛВС и ее системы защиты информации, производится внеплановая смена паролей всех пользователей ЛВС.

О необходимости проведения внеплановой смены паролей всех пользователей ЛВС начальник управления ИТ письменно информирует руководителей структурных подразделений Администрации города Ростова-на-Дону.

Руководители структурных подразделений Администрации города Ростова-на-Дону, получив информацию о необходимости проведения внеплановой смены паролей всех пользователей ЛВС, организуют эту работу в подчиненных подразделениях, и по ее окончании письменно информируют об этом начальника управления ИТ.

9.14. При выявлении факта компрометации пароля или возникновении подозрения о компрометации пароля производится его замена. Пользователь ЛВС, обнаруживший компрометацию пароля или обстоятельства, указывающие на то, что пароль мог стать доступен постороннему лицу, обязан незамедлительно прекратить использование скомпрометированного пароля, письменно сообщить о случившемся в управление ИТ и произвести смену пароля. Хранение значения пароля в доступном для других лиц месте (ящик рабочего стола, поверхность монитора, клавиатуры и т.п.) рассматривается как компрометация пароля.

Управление ИТ организует проведение разбирательства по факту произошедшей или предполагаемой компрометации пароля и принятие мер по локализации последствий инцидента информационной безопасности.

Использование в ЛВС паролей, в отношении которых имеются сведения или предположения об их компрометации, запрещается.

9.15. В целях усиления процесса аутентификации пользователей в ЛВС совместно с паролями могут использоваться аппаратные средства аутентификации (далее – аппаратные аутентификаторы).

Аппаратные аутентификаторы регистрируются в управлении ИТ,

закрепляются за конкретными пользователями ЛВС и выдаются им под роспись. Работники Администрации города Ростова-на-Дону, получившие в пользование аппаратные аутентификаторы, обязаны обеспечить выполнение требований информационной безопасности при их эксплуатации. Хранение аппаратных аутентификаторов должно осуществляться в надежно запираемых шкафах (ящиках, хранилищах). В случае увольнения (перевода на другую работу) работника Администрации города Ростова-на-Дону, числящийся за ним аппаратный аутентификатор перезакрепляется за другим пользователем ЛВС.

При убытии с рабочего места, в том числе кратковременном, пользователям ЛВС запрещается оставлять аппаратный аутентификатор подключенным к рабочей станции, а также в местах, к которым возможен бесконтрольный доступ иных лиц.

В случае утраты (потери, хищения и т.п.) аппаратного аутентификатора, работник, допустивший утрату, незамедлительно письменно сообщает об этом в управление ИТ, выключает рабочую станцию и не осуществляет подключений к ЛВС до выяснения обстоятельств и локализации последствий утраты аппаратного аутентификатора. Управление ИТ производит блокировку утраченного аппаратного аутентификатора в ЛВС.

Парольная и иная защищаемая информация, содержащаяся на пришедших в негодность и не подлежащих ремонту аппаратных аутентификаторах, уничтожаются (стирается) с оформлением соответствующего акта.

10. Порядок антивирусной защиты ЛВС

10.1. Антивирусная защита ЛВС, включающая обнаружение компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования защищаемой информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации, обеспечивается оператором ЛВС и осуществляется всеми пользователями ЛВС.

10.2. Средства антивирусной защиты применяются на входящих в состав ЛВС автоматизированных рабочих местах, серверах, средствах межсетевого экранирования, узлах электронной почты, мобильных технических средствах (флэш-накопители, внешние накопители на жестких дисках, ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные съемные носители информации, портативные вычислительные устройства, устройства связи с возможностью обработки информации), в среде виртуализации (гипервизор, виртуальные машины, в том числе их операционные системы и программное обеспечение, виртуальное аппаратное обеспечение и т.п.) и иных точках доступа к ЛВС, где возможно внедрение вредоносных компьютерных программ (компьютерных вирусов) через съемные машинные носители информации или сетевые подключения,

в том числе к сетям общего пользования.

10.3. Установка, конфигурирование средств антивирусной защиты и централизованное управление ими производится администраторами информационной безопасности ЛВС. Средства антивирусной защиты должны быть сконфигурированы так, чтобы осуществлялось оповещение в масштабе времени, близком к реальному, администраторов информационной безопасности ЛВС об обнаружении вредоносных компьютерных программ (компьютерных вирусов).

10.4. Периодически, но не реже одного раза в неделю, все программно-аппаратные ресурсы ЛВС подвергаются проверке на наличие вредоносных компьютерных программ (компьютерных вирусов), для чего средствам антивирусной защиты предоставляется к ним соответствующий доступ.

10.5. При загрузке, открытии или исполнении в ЛВС файлов из внешних источников (съемные машинные носители информации, сетевые подключения и т.п.) производится их антивирусная проверка в масштабе времени, близком к реальному. Использование в ЛВС незарегистрированных съемных машинных носителей информации, которые могут являться источниками вредоносных компьютерных программ (компьютерных вирусов), запрещается.

10.6. При реализации антивирусной защиты в ЛВС обеспечивается проверка работоспособности, актуальность версии программного обеспечения и базы данных признаков вредоносных компьютерных программ (компьютерных вирусов) средств антивирусной защиты (далее – антивирусная база).

10.7. Обновление антивирусной базы на всех компонентах ЛВС проводится регулярно в автоматическом режиме с периодичностью выпуска соответствующих обновлений производителем программного обеспечения средств антивирусной защиты, контролем целостности обновлений, получением уведомлений о необходимости обновления и непосредственном обновлении антивирусной базы и регистрацией событий о неуспешном ее обновлении.

Сервер ЛВС получает обновления антивирусной базы на официальном сайте производителя программного обеспечения средств антивирусной защиты. Обновление антивирусной базы рабочих станций и иных компонентов ЛВС осуществляется централизовано с сервера ЛВС.

10.8. Анализ содержания файлов-отчетов о результатах проверок программно-аппаратных ресурсов ЛВС и событиях, происходивших в ходе работы средств антивирусной защиты, проводится администраторами информационной безопасности ЛВС ежеквартально.

10.9. Выполнение действий по реагированию на обнаружение в ЛВС программно-аппаратных ресурсов, подвергшихся заражению вредоносными компьютерными программами (компьютерными вирусами), осуществляется централизовано.

При получении уведомления в виде звукового сигнала или сообщения на дисплее рабочей станции об обнаружении вредоносной компьютерной

программы (компьютерного вируса) пользователь ЛВС, не выключая компьютер, прекращает обработку информации и следует указаниям, содержащимся в уведомлениях, формируемых средством антивирусной защиты, осуществляющим действия по предотвращению заражения программно-аппаратных ресурсов ЛВС или локализации последствий такого заражения. Обработка информации на компьютере может быть продолжена только после получения уведомления, сформированного средством антивирусной защиты, об окончании лечения или удалении зараженных компьютерным вирусом файлов.

10.10. О всех фактах обнаружения вредоносной компьютерной программы (компьютерного вируса) пользователи ЛВС письменно информируют оператора ЛВС с указанием обстоятельств инцидента информационной безопасности и предполагаемого источника (отправителя, владельца и т.п.) зараженного файла, компьютерного вируса.

10.11. При получении информации о возникновении инцидента информационной безопасности, связанного с обнаружением вредоносной компьютерной программы (компьютерного вируса), оператор ЛВС организует:

проведение анализа инцидента, в том числе определение источников и причин его возникновения, а также оценки последствий инцидента;

принятие мер по устранению инцидента и последствий внедрения в ЛВС вредоносной компьютерной программы (компьютерного вируса);

принятие мер по предотвращению повторного возникновения инцидента, связанного с внедрением в ЛВС вредоносной компьютерной программы (компьютерного вируса).

11. Порядок предоставления доступа к информационно-телекоммуникационной сети общего пользования «Интернет»

11.1. Доступ к информационно-телекоммуникационной сети общего пользования «Интернет» (далее – сеть «Интернет») предоставляется работникам Администрации города Ростова-на-Дону, которым такой доступ необходим для исполнения должностных обязанностей.

11.2. Доступ к сети «Интернет» предоставляется оператором ЛВС на основании заявок руководителей структурных подразделений Администрации города Ростова-на-Дону. В заявке указывается фамилия, инициалы, должность, номер кабинета, рабочий телефон работника, которому необходимо предоставить доступ к сети «Интернет», инвентарный номер закрепленного за ним компьютера, перечень информационных ресурсов в сети «Интернет» (доменных имен и (или) сетевых адресов сайтов), к которым необходимо предоставить доступ, с приведением тематики получаемой информации и обоснованием необходимости ее получения.

11.3. Подключение к сети «Интернет» производится только с использованием специально предназначенных для этого средств защиты информации, в том числе шифровальных (криптографических) средств,

прошедших в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю.

11.4. Посещение сайтов и использование информационных ресурсов сети «Интернет» в целях, не связанных с исполнением должностных обязанностей, запрещается.

В случае нарушения пользователем ЛВС требований законодательства Российской Федерации и настоящего Положения по вопросам использования информационных ресурсов в сети «Интернет» оператор ЛВС блокирует ему доступ к сети «Интернет» до проведения разбирательства по факту инцидента информационной безопасности и устранения его последствий.

11.5. Контроль доступа пользователей ЛВС к информационным ресурсам сети «Интернет» обеспечивается управлением ИТ».

1.1.5. Дополнить приложением № 2 согласно приложению № 1 к распоряжению.

1.1.6. Дополнить приложением № 3 согласно приложению № 2 к распоряжению.

2. Контроль за выполнением распоряжения оставляю за собой.

Глава Администрации
города Ростова-на-Дону В.В. Кушнарев

Распоряжение вносит
управление информационных
технологий Администрации
города Ростова-на-Дону

Приложение № 1
к распоряжению Администрации
города Ростова-на-Дону
от 24.04.2017 № 102

Парольная карта

рег. № _____ от «___»_____20__г.

администратора _____

(наименование роли администратора (выполняемые функции в ЛВС)

_____

(Ф.И.О.)

№ п/п	Значение пароля	Имя домена (имя компьютера, наименование ресурса)	Имя пользователя в домене (логин)	Дата установки пароля и роспись	Дата удаления пароля и роспись

Начальник общего
отдела Администрации
города Ростова-на-Дону П.П. Волошин

Приложение № 2
к распоряжению Администрации
города Ростова-на-Дону
от 24.04.2017 № 102

Журнал парольных карт

№ п/п	Функции (роль) администратора - владельца парольной карты, Ф.И.О.	Наименование объекта доступа по паролю	Номер печати, которой опечатан конверт с парольной картой	Ф.И.О., роспись принявшего конверт с парольной картой на хранение и дата	Ф.И.О., роспись в обратном приеме конверта с парольной картой	Указание и росписи о вскрытии конверта с парольной картой
1	2	3	4	5	6	7

Начальник общего
отдела Администрации
города Ростова-на-Дону П.П. Волошин