АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО РАЙОНА «НЕРЧИНСКИЙ РАЙОН» ЗАБАЙКАЛЬСКОГО КРАЯ

РАСПОРЯЖЕНИЕ

03 июля 2020 г. № 360

г. Нерчинск

Об утверждении Инструкций по работе в информационных системах администрации муниципального района «Нерчинский район» Забайкальского края

Во исполнение требований Федерального закона от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации»; Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»; Федерального закона от 28 декабря 2010 года № Э90-ФЗ «О безопасности»; Указа Президента Российской Федерации от 12 мая 2009 года № 537 «О стратегии национальной безопасности Российской Федерации до 2020 года»; Указа Президента Российской Федерации от 09 сентября 2000 года № Пр-1895 «О Доктрине информационной безопасности Российской Федерации»; Указа Президента Российской Федерации от 07 февраля 2008 года № 212-Пр «Стратегия развития информационного общества в Российской Федерации»; Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденного постановлением Совета Министров - Правительства Российской Федерации от 15 сентября 1993 года № 912-51; Закона Забайкальского края от 20 ноября 2009 года № 276-ЗЗК «О государственных информационных системах Забайкальского края, а также в целях обеспечения безопасности информации, обрабатываемой в информационных системах администрации муниципального района «Нерчинский район» Забайкальского края:

1. Утвердить Инструкцию по организации парольной защиты в информационных системах администрации муниципального района «Нерчинский район» Забайкальского края (приложение 1).
2. Утвердить Инструкцию по антивирусной защите в информационных системах администрации муниципального района «Нерчинский район» Забайкальского края (приложение 2).
3. Утвердить Инструкцию по безопасной работе с ресурсами сети Интернет и электронной почтой в информационных системах администрации муниципального района «Нерчинский район» Забайкальского края (приложение 3).

4. Отделу по информационным технологиям администрации муниципального района «Нерчинский район» (Казанцева Т.Н.) довести данные инструкции до всех специалистов администрации муниципального района «Нерчинский район», работающих в информационных системах.

5. Контроль над выполнением настоящего распоряжения возложить на заместителя Главы муниципального района «Нерчинский район» по территориальному развитию Бутина А.Н.

Глава муниципального района
«Нерчинский район» Р.В. Сенотрусов

АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО РАЙОНА "НЕРЧИНСКИЙ РАЙОН" ЗАБАЙКАЛЬСКОГО КРАЯ
УПРАВЛЕНИЕ ДЕЛАМИ

Приложение 1
к распоряжению администрации муниципального
района «Нерчинский район»
от «03» июля 2020 г. № 360

Инструкция
по организации парольной защиты в информационных системах администрации муниципального района «Нерчинский район» Забайкальского края

1.Термины и определения

1. Автоматизированная система (АС) - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

2. Администратор безопасности информации - лицо, ответственное за защиту автоматизированной системы от несанкционированного доступа к информации.

3. Безопасность информации (Информационная безопасность) - состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами.

4. Пользователь (потребитель) информации - субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

5. Первичный пароль - комбинация символов (буквы, цифры, знаки препинания, специальные символы), устанавливаемые системным администратором при создании новой учетной записи.

6. Основной пароль – комбинация символов (буквы, цифры, знаки препинания, специальные символы), известная только сотруднику организации, используемая для подтверждения подлинности владельца учетной записи.

2. Общие положения

7. Инструкция по организации парольной защиты в информационных системах администрации муниципального района «Нерчинский район» Забайкальского края регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах, а также контроль за действиями пользователей системы при работе с паролями.

8. За организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в информационных

системах администрации муниципального района, контроль за действиями специалистов администрации муниципального района «Нерчинский район» возлагается на специалистов отдела по информационным технологиям администрации муниципального района «Нерчинский район», которые обязаны регулярно вносить данные в Журнал «О результатах периодической проверки состояния парольной защиты пользователей».

3. Требования к генерации, использованию, смене и прекращению действия паролей

9. Установку первичного пароля производит специалист отдела по информационным технологиям администрации муниципального района «Нерчинский район» (далее по тексту - специалист отдела) при создании новой учетной записи. Ответственность за сохранность первичного пароля лежит на специалисте отдела.

Первичный пароль может содержать несложную комбинацию символов, либо повторяющиеся символы.

При создании первичного пароля, специалист отдела обязан установить опцию, требующую смену пароля при первом входе в систему, а также уведомить владельца учетной записи о необходимости произвести смену пароля.

Первичный пароль так же используется при сбросе забытого пароля на учетную запись. В любом случае, при использовании первичного пароля все требования настоящего документа сохраняются.

10. Установку основного пароля производит пользователь при первом входе в систему с новой учетной записью.

Пользователь несет персональную ответственность за сохранение в тайне основного пароля. Запрещается сообщать пароль другим лицам, в том числе сотрудникам отвечающим за информационную безопасность, записывать его в рабочих тетрадях, блокнотах, на элементах оборудования рабочего места, а так же пересылать открытым текстом в электронных сообщениях.

11. Личные (основные) пароли должны генерироваться и распределяться централизованно либо выбираться пользователями автоматизированной системы самостоятельно с учетом следующих требований:

Каждый пароль должен выбираться и генерироваться пользователем с учетом следующих требований:

– максимальный срок действия пароля – 6 месяцев (ГОСТ ИСО/МЭК 17799-2005);

– минимальная длина пароля - не менее 8 символов;

– минимальный срок действия пароля – 1 день;

– в числе символов пароля обязательно должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);

– новый пароль не должен повторять 6 предыдущих значений.

12. Пароли к учетным записям, обеспечивающим административный или привилегированный доступ, должны отвечать следующим требованиям:

– максимальный срок действия пароля – 3 месяца (ГОСТ ИСО/МЭК 17799-2005);

– минимальная длина пароля - не менее 12 символов;

– минимальный срок действия пароля – 1 день;

– в числе символов пароля обязательно должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);

– пароль не должен повторять 8 предыдущих значений.

13. 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.

14. В случае, если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на специалисте отдела.

Для генерации «стойких» значений паролей могут применяться специальные программные средства.

15. Внеплановая смена личного пароля в случае прекращения полномочий работника должна производиться специалистом отдела немедленно после окончания последнего сеанса работы данного пользователя с АС.

16. Внеплановая смена всех паролей пользователей АС должна проводиться в случае компрометации пароля (потери электронного ключа) специалистом отдела.

В случае компрометации личного пароля пользователя АС должны быть немедленно предприняты меры в соответствии с положениями настоящей Инструкции, в зависимости от полномочий владельца скомпрометированного пароля.

17. Повседневный контроль за действиями исполнителей и обслуживающего персонала АС при работе с паролями, соблюдением правил их смены, хранения и использования возлагается на администратора безопасности информации ОМСУ. После предоставления текущего значения пароля для проверки на соответствие установленным требованиям, контролируемый пользователь обязан сменить свой пароль.

18. 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 в опечатанном личной печатью пенале или конверте (возможно вместе с персональными ключевыми носителями и идентификатором Touch Memory).

19. Восстановление забытого основного пароля пользователя (при отсутствии копии на бумажном или другом носителе, п.3.10) осуществляется специалистом отдела путем изменения (сброса) основного пароля пользователя на первичный пароль на основании письменной либо зарегистрированной электронной заявки пользователя.

Устная заявка пользователя на изменение пароля не является основанием для проведения таких изменений.

20. Для предотвращения угадывания паролей путем подбора, специалист отдела обязан настроить механизм блокировки учетной записи при трехкратном неправильном вводе пароля.

21. Разблокирование учетной записи пользователя осуществляется специалистом отдела на основании заявки владельца учетной записи *(возможен вариант автоматического разблокирования через продолжительный промежуток времени)*.

22. Повседневный контроль за действиями исполнителей и обслуживающего персонала автоматизированной системы при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на ответственных за информационную безопасность, периодический контроль – возлагается на специалиста отдела.

23. При наличии (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п.) технологической необходимости использования имен и паролей некоторых сотрудников в их отсутствие, такие сотрудники обязаны сразу же провести замену личных паролей с заменой их на бумажных и других дублирующих носителях.

24. Запрещается включение паролей в автоматизированный процесс регистрации, например с использованием хранимых макрокоманд или функциональных клавиш, а также коллективное использование индивидуальных паролей.

4. Установка пароля на BIOS

25. Для исключения угроз безопасности информации, связанной с внедрением вредоносного кода в BIOS, а также перевода BIOS к более ранним версиям, имеющим уязвимости и др., вход в систему BIOS должен быть защищен устойчивым паролем в соответствии с пунктом 3.4 настоящей инструкции.

26. Пароль на BIOS устанавливается только администратором безопасности информации ОМСУ, значения пароля записываются в специальном журнале, который хранится в опечатанном виде в сейфе (металлическом хранилище) администратора информационной безопасности. Вскрытие журнала производится в присутствии сотрудника, работающего на соответствующем АРМ с записью в журнале, где отражаются дата, время и цель вскрытия.

27. Замена пароля на BIOS или его сброс производится только с разрешения должностного лица ответственного за информационную безопасность

5. Ответственность за нарушение требований настоящей инструкции

28. За нарушение требований настоящей инструкции пользователи несут дисциплинарную ответственность в соответствии с действующим законодательством.

Приложение 2
к распоряжению администрации муниципального
района «Нерчинский район»
от «03» июля 2020 г. № 360

Инструкция
по организации антивирусной защиты в информационных системах администрации муниципального района «Нерчинский район» Забайкальского края

1. Общие положения

1. Инструкция по организации антивирусной защиты информационных системах администрации муниципального района «Нерчинский район» (далее - Инструкция) разработана в соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Доктриной информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации от 09.09.2000 г. №Пр-1895.

2. Настоящая Инструкция предназначена для организации порядка проведения антивирусного контроля, с целью предотвращения несанкционированных вредоносных воздействий на информационные ресурсы и персональные данные администрации муниципального района «Нерчинский район», и возникновения фактов заражения программного обеспечения (далее - ПО) сетевого оборудования и автоматизированных рабочих мест исполнителей компьютерными вирусами.

3. В настоящей Инструкции использованы следующие термины и определения:

Антивирусное ПО – набор программ для обнаружения компьютерных вирусов и других вредоносных программ и лечения инфицированных файлов, а также для профилактики – предотвращения заражения файлов или операционной системы вредоносным кодом.

Антивирусные базы – файлы, используемые антивирусным ПО при поиске вредоносных программ, периодически обновляемые разработчиком антивирусного ПО.

Антивирусный контроль – проверка информации (файла, сообщения и т.п.) на предмет наличия вредоносных программ.

Вредоносная программа – компьютерная программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информационные ресурсы.

Защищаемый компьютер – электронно-вычислительная машина (персональный компьютер или сервер), используемая для обработки данных.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес,

семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Пользователь – специалист администрации муниципального района «Нерчинский район» или другое лицо, использующее в работе средства электронно-вычислительной техники.

Съемный носитель информации – носитель информации, предназначенный для ее автономного хранения и независимого от места записи использования (отторгаемые жесткие магнитные диски, флэш-память, CD, DVD, дискеты и др.).

4. Требования настоящей Инструкции обязательны для выполнения всеми работниками администрации муниципального района «Нерчинский район», ведущими обработку конфиденциальной информации, персональных данных и другой информации с применением средств вычислительной техники.

5. Общее и методическое руководство обеспечением антивирусной защиты информационных систем и информационных систем персональных данных осуществляется отделом по информационным технологиям администрации муниципального района «Нерчинский район».

6. Пользователь отвечает за обеспечение устойчивой работоспособности и информационной безопасности вверенного ему объекта вычислительной техники при работе в информационных системах и при обработке персональных данных.

7. Техническое обслуживание средств вычислительной техники, уборка помещения и т.п. проводятся под контролем пользователя.

2. Установка антивирусного ПО

8. Установку антивирусного ПО производит специалист отдела по информационным технологиям администрации муниципального района «Нерчинский район» (далее по тексту - специалист отдела).

9. При установке должно использоваться только лицензионное антивирусное ПО, рекомендованное к применению.

10. Установка антивирусного ПО производится индивидуально на каждый защищаемый компьютер с обязательным предохранением настроек от изменения паролем.

11. Пользователям запрещается отключать средства антивирусной защиты и самостоятельно вносить изменения в настройки антивирусного ПО.

12. Ярлык для запуска антивирусного ПО должен быть вынесен на «Рабочий стол» операционной системы.

3. Порядок обновления антивирусных баз

13. Актуализация антивирусных баз на защищаемых компьютерах, подключенных к сети Интернет, локальной сети, должна осуществляться ежедневно в автоматическом режиме с сервера управления антивирусной защитой корпоративной сети передачи данных органов власти Забайкальского края или с сервера обновлений ЗАО «Лаборатория Касперского через единую защищенную точку доступа в сеть «Интернет» (по рабочим дням).

14. Обновление антивирусных баз на защищаемых компьютерах, не подключенных к локальной сети, должно осуществляться с использованием учтенных съемных носителей информации, в обязательном порядке проверяемых антивирусным ПО перед их использованием или принудительным подключением к локальной сети.

15. Проверка критических областей защищаемых компьютеров, заражение которых вредоносными программами может привести к серьезным последствиям, должна проводиться автоматически при каждой его загрузке.

16. Актуализация антивирусных баз на защищаемых компьютерах, подключенных к локальной сети, контролируется пользователем самостоятельно ежедневно и, в случае нарушения, пользователь должен не принимать никаких мер и срочно сообщить в отдел по информационным технологиям администрации муниципального района «Нерчинский район».

4. Требования к проведению антивирусного контроля

17. Пользователь осуществляет контроль за целевым использованием автоматизированного рабочего места, а также всех его внешних устройств.

18. Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, файлы данных, сообщения электронной почты и т.д.), получаемая и передаваемая по телекоммуникационным каналам, а также данные на съемных носителях информации. Контроль входящей и исходящей информации на защищаемых компьютерах должен осуществляться непрерывно посредством постоянно работающего компонента антивирусного ПО («монитора»).

19. Все программное обеспечение, устанавливаемое на защищаемые компьютеры, должно предварительно проверяться на наличие вредоносных программ.

20. Полная проверка сетевых ресурсов и рабочих станций на наличие компьютерных вирусов производится еженедельно, по четвергам.

21. Внеочередной антивирусный контроль всех дисков и файлов защищаемого компьютера должен выполняться:

– сразу после установки или изменения ПО;

– после подключения автономного компьютера к локальной сети;

– при возникновении подозрения на наличие вредоносных программ (нетипичная работа программ, появление графических и звуковых эффектов, искажение данных, пропадание файлов, частое появление сообщений о системных ошибках, сбоях и т.п.).

22. В сомнительных случаях для определения факта наличия или отсутствия вредоносных программ к проверке необходимо привлечь специалиста отдела.

Специалист отдела обязан регулярно вносить в Журнал информацию «О результатах периодической проверки состояния антивирусной защиты».

5. Действия пользователей при обнаружении вредоносных программ

23. В случае обнаружения при проведении антивирусной проверки вредоносных программ пользователи обязаны:

– приостановить все операции, связанные с обработкой файлов на защищаемом компьютере;

– немедленно поставить в известность о факте обнаружения вредоносных программ специалиста отдела, владельцев зараженных или поврежденных вредоносными программами файлов, а также смежные подразделения, использующие эти файлы в работе;

– совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

–провести лечение зараженных файлов (при необходимости привлечь специалиста отдела);

– в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл на отторгаемом носителе в отдел по информационным технологиям администрации муниципального района «Нерчинский район» для дальнейшей передачи его в организацию по антивирусной поддержке;

- по факту обнаружения зараженных вирусом файлов составить служебную записку в отдел по информационным технологиям администрации муниципального района «Нерчинский район», в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

6. Ответственность за выполнение требований Инструкции

24. Ответственность за организацию антивирусной защиты информации на компьютерах, эксплуатируемых пользователями администрации муниципального района «Нерчинский район», и их ознакомление с Инструкцией несет отдел по информационным технологиям администрации муниципального района «Нерчинский район».

25. Ответственность за соблюдение требований Инструкции на своих рабочих местах несут пользователи.

26. Ответственность за своевременное обновление антивирусных баз и получение новых лицензионных ключей (при истечении их срока действия) несет специалист отдела.

27. За нарушение требований Инструкции, пользователи несут дисциплинарную ответственность в соответствии с действующим законодательством.

Приложение 3
к распоряжению администрации муниципального
района «Нерчинский район»
от «03» июля 2020 г. № 360

Инструкция
по безопасной работе с ресурсами сети Интернет и электронной почтой в информационных системах администрации муниципального района «Нерчинский район» Забайкальского края

Для обеспечения информационной безопасности следуйте мерам предосторожности при работе в сети Интернет:

1. Ежедневно следите, чтобы Антивирус был обновлен и всегда «Активен».

2. Не переходите по ссылкам на подозрительные ресурсы, сайты, программы.

3. Не запускайте программы, вложенные в письма, даже если они пришли к Вам от заведомо знакомого лица. Помните, что вирусы с легкостью могут подделать любой почтовый адрес и указать в письме ваши правильные личные данные, украв их из адресной книги вашего знакомого.

4. Перед запуском любой программы или открытии любого файла (в том числе реквизиты, документы) проверьте их антивирусной программой.

5. При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.

6. Если в поступившем письме содержится:

просьба ввести логин/пароль или создать логин/пароль при переходе по ссылке, ссылка для перехода на сторонний сайт, который запрашивает доступ к вашему почтовому ящику от приложения или сайта, ссылка для перехода на сторонний сайт, который запрашивает доступ к вашему почтовому ящику от приложения или сайта, ни в коем случае не делайте этого!

Не передавайте никому Ваши логины/пароли, кроме как по письменному разрешению руководства (на бумаге) или устному запросу ваших коллег (по известному вам телефону или подойдите лично).

7. При работе с почтой ВСЕГДА смотрите на адрес отправителя, подделать почтовый адрес очень просто, для этого не нужно обладать какими-то особыми знаниями: он может быть похожим на настоящий, отличаться даже одной буквой, например, вместо буквы «о» использована цифра «0» (ноль);

При работе в почте gmail адрес отправителя может быть «настоящим», но с надписью: «Отправлено через …». Это означает, что злоумышленник использует реальный e-mail известного вам человека и отправляет его через специальные сервисы. E-mail будет «реальным», но если есть надпись «Отправлено через» – это сигнал незамедлительно обратиться устно (подойдите лично или позвоните по телефону) к отправителю письма.

8. Если кто-то просит ваши пароли – необходимо устное подтверждение просьбы.

9. Открывайте файлы только известного вам расширения (docx, png, xlsx и пр).

10. Не распаковывайте архивы, если полностью не уверены в отправителе (лучше удостовериться, что он действительно его посылал, так как подделать почту очень просто, для этого не нужно даже ее взламывать). Архив должен сразу вызывать подозрения, особенно если написано, что там docx или pdf-документ.

11. Если при открытии файла, он требует разрешить выполнение макросов, ни в коем случае не разрешайте, с 90% вероятностью это вирус. Для обычного документа макросы не нужны.

12. Не сохраняйте пароли от программ в памяти интернет-браузера, если к компьютеру есть доступ посторонним лицам.

13. Не допускайте к рабочему компьютеру посторонних лиц. В свое отсутствие всегда блокируйте экран.

14. Используйте Сл00ЖнЫе ПаР0Jли в рабочих программах.

15. Когда увольняется кто-то из сотрудников незамедлительно меняйте пароли на всех сервисах, к которым был доступ этому сотруднику. Это касается любых общих сервисов – почта, WuBook, PMS и пр.

16. Не нажимайте на баннеры и всплывающие окна, возникающие во время работы с Интернетом.

17. При возникновении подозрения о «заражении вирусом», «нетипичной работе ПК» – незамедлительно обратитесь в отдел по информационным технологиям администрации муниципального района «Нерчинский район», или проверьте компьютер с помощью установленного антивируса.

18. Будьте бдительны и уделяйте внимание повышению грамотности в вопросах информационной безопасности.

Не пытайтесь и не решайте проблему ПК самостоятельно. Доверьте решение проблемы специалистам.