**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ БОДАЙБИНСКИЙ РАЙОН**

**АДМИНИСТРАЦИЯ ГОРОДА БОДАЙБО И РАЙОНА**

**РАСПОРЯЖЕНИЕ**

26.02.2018г. г. Бодайбо № 147-р

Об утверждении парольной, антивирусной

политики, правил работы со съемными

носителями, правил резервного копирования

при обработке персональных данных в

Администрации г. Бодайбо и района

Во исполнение постановления Администрации г. Бодайбо и района от 15.01.2018 № 2-п «Об определении политики в отношении персональных данных, обрабатываемых в органах местного самоуправления муниципального образования г. Бодайбо и района», в соответствии с Федеральным законом от 06.10.2003 № 131-ФЗ "Об общих принципах организации местного самоуправления в Российской Федерации", Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных", руководствуясь ст. 31 Устава муниципального образования города Бодайбо и района:

1. Утвердить:

1) Парольную политику в отношении защиты персональных данных,

обрабатываемых в Администрации г. Бодайбо и района (приложение № 1 к настоящему распоряжению);

2) Антивирусную политику в отношении защиты персональных данных, обрабатываемых в Администрации г. Бодайбо и района (приложение № 2 к настоящему распоряжению);

3) Правила работы со съемными носителями информации в Администрации г. Бодайбо и района (приложение № 3 к настоящему распоряжению);

4) Правила резервного копирования информации в Администрации г. Бодайбо и района(приложение № 4 к настоящему распоряжению).

2. Главному специалисту по кадровой работе юридического отдела Администрации г. Бодайбо и района Зацаренко О.А. ознакомить с настоящим распоряжением специалистов, осуществляющих обработку персональных данных, либо имеющих доступ к персональным данным.

3. Ведущему аналитику-специалисту отдела организационной работы Кравец С.В. организовать и провести обучение на рабочих местах специалистов, осуществляющих обработку персональных данных, либо имеющих доступ к персональным данным, по внедрению утвержденных положений.

МЭР Е.Ю. ЮМАШЕВ

Приложение № 1

к распоряжению Администрации г. Бодайбо и района

от 26.02.2018 г. № 147-р

**Парольная политика в отношении защиты персональных данных,**

**обрабатываемых в Администрации г. Бодайбо и района**

1. **Общие положения**

1.1. Настоящая Политика устанавливает стандарты создания паролей, их защиту, хранение и частоту изменения при обработке персональных данных в информационных системах Администрации г. Бодайбо и района. Пароли – один из важнейших аспектов информационной безопасности, так как плохо подобранный пароль повышает потенциальный риск несанкционированного доступа в информационную систему.

1.2. Настоящая Политика относится ко всем специалистам Администрации г. Бодайбо и района, которые имеют или ответственны за доступ к конфиденциальной информации всех уровней на любой системе, оборудовании, имеющем доступ (или хранящем конфиденциальную информацию) к информационной системе Администрации г. Бодайбо и района.

**2. Требования к паролям**

2.1. Пароли системных учетных записей (администратора домена, локального администратора, root и т. д.) должны изменяться ежеквартально.

2.2. Все пароли системных учетных записей, а также пароли приложений и активного оборудования необходимо хранить в базе данных в зашифрованном виде, доступ к которой ограничен.

2.3. Срок действия паролей учетных записей домена должен составлять не более 9 месяцев. Рекомендуемый интервал смены пароля 6 месяцев.

2.4. Пароль учетной записи пользователя, имеющего административные привилегии, полученные при помощи членства в группе или при помощи программ, должен быть уникален по отношению к другим паролям учетных записей данного пользователя.

2.5. Запрещается передача паролей пользователям при помощи почтовых сообщений либо иным другим открытым способом через Интернет.

2.6. Пароль, полученный пользователем, необходимо сменить при первом входе в систему.

1. **Инструкция по созданию пароля**
	1. Специалист Администрации г. Бодайбо и района использует пароли для различных целей. Среди них: доступ к учётной записи пользователя, к веб-интерфейсам, к электронной почте, для защиты хранителя экрана, доступ к маршрутизаторам. Поскольку очень мало систем поддерживают токены с одноразовыми паролями (динамические пароли, которые используются только один раз), следует выбрать стойкий пароль.

3.2. Признаки слабых паролей:

- содержат менее восьми символов;

- являются словами, которые содержатся в словарях (русских или иностранных);

- являются часто употребляемым словом;

- содержат фамилию, кличку животного, имена друзей, сотрудников,

вымышленных персонажей и т. д.;

- содержат компьютерные термины и названия, команды, названия сайтов, компаний, оборудования, программного обеспечения;

- содержат название учреждения (организации) и географические наименования, например "Бодайбо" или их производные;

- содержат даты рождения и иную личную информацию, например, адреса и номера телефонов; слово или число по шаблону типа аааббб, qwerty, zyxwvuts, 12345 и т.д.;

- предыдущий пример, вводимый в обратной последовательности.

- два предыдущих примера с цифрой в начале или конце пароля (например, Бодайбо 1).[править]

3.3. Параметры сильных паролей:

- содержат сочетание букв верхнего и нижнего регистров (например, a z, A-Z);

- включают цифры и знаки пунктуации (например, 0-9,!@#$%^&\*()\_+|~-=\`{}[]:";'<>?,./);

- состоят из восьми и более символов;

- не являются словом на любом языке, диалекте, сленге, жаргоне и т.д.;

- не основаны на персональной информации, например, фамилии, дате

рождения и т.д.;

- никогда не записываются и не хранятся on-line.

3.4. Следует создавать легко запоминаемые пароли. Один из способов создания таких паролей – использовать песни, стихи или другие легко запоминающиеся фразы.

1. **Правила парольной защиты**

4.1. Не использовать один и тот же пароль для доступа к учётным записям пользователей Администрации г. Бодайбо и района и к другим ресурсам (например, доступ в интернет из дома, системам электронной коммерции и т.д.). По возможности не использовать один и тот же пароль для доступа к различным ресурсам внутри организации.

4.2. Не сообщать свой пароль другому лицу. Не указывать свой пароль в анкетах или опросниках. Все пароли являются конфиденциальной информацией Администрации г. Бодайбо и района.

4.3. Не хранить пароль на рабочем месте.

4.4. Сменить пароль при его разглашении.

1. **Стандарт разработки приложений**

5.1. Разработчики приложений должны обеспечить в своих программах следующие меры безопасности:

- приложения должны поддерживать аутентификацию отдельных пользователей, а не групп;

- приложения не должны хранить пароли в открытом или легко раскрываемом виде;

- приложения должны обеспечивать своего рода передачу прав, чтобы один пользователь мог выполнять функции другого, не зная его пароль.

Подготовил:

Ведущий аналитик-специалист

отдела организационной работы С.В. Кравец

Приложение № 2

к распоряжению Администрации г. Бодайбо и района

от 26.02.2018 г. № 147-р

**Антивирусная политика в отношении защиты персональных**

**данных, обрабатываемых в Администрации г. Бодайбо и района**

1. **Общие положения**

1.1. Настоящая Антивирусная политика определяет требования по защите информационных систем и персональных данных Администрации г. Бодайбо и района от угроз информационной безопасности, причина возникновения которых связана с распространением вредоносного программного обеспечения.

1.2. Требования антивирусной политики минимизируют вероятность возникновения негативных последствий для информационных систем персональных данных Администрации г. Бодайбо и района.

1. **Содержание Антивирусной политики**

2.1. Специалисты Администрации г. Бодайбо и района должны всегда использовать полученное из доверенного источника и принятое в качестве стандарта в Администрации г. Бодайбо и района антивирусное программное обеспечение, поддерживать антивирусное программное обеспечение в актуальном состоянии.

2.2. Никогда не открывать вложения к сообщениям электронной почты, полученным из неизвестных, подозрительных или непроверенных источников. Такие вложения должны незамедлительно удаляться.

2.3. Сообщения электронной почты, содержащие спам, цепочки сообщений и другую нежелательную почту должны удаляться без пересылки.

2.4. Не следует скачивать информацию из неизвестных или подозрительных источников.

2.5. Необходимо избегать предоставления общего доступа к логическим дискам с правами чтения/записи в случае, если это не требуется в рамках выполнения основной деятельности.

2.6. Прежде чем использовать носители информации, полученные от неизвестных или подозрительных источников, следует сканировать их на отсутствие вирусов.

2.7. Необходимо резервировать важные данные и настройки системы регулярно. Резервные копии хранить в безопасном месте.

2.8. В случае необходимости запуска приложения, конфликтующего с установленным антивирусным программным обеспечением, необходимо выполнить полную проверку рабочей станции на наличие вирусов, отключить антивирусное программное обеспечение и запустить необходимое приложение. Должно быть доподлинно известно, что запускаемое приложение не приведет к негативным последствиям. После выполнения задач, связанных с использованием приложения, возобновить работу антивирусного программного обеспечения. При отключенном антивирусном программном обеспечении запрещается запускать любые приложения (электронная почта или открытие общего доступа к файловым ресурсам), в результате действий которых автоматизированное рабочее место может быть подвержено инфицированию вредоносным программным обеспечением.

Подготовил:

Ведущий аналитик-специалист

отдела организационной работы С.В. Кравец

Приложение № 3

к распоряжению Администрации г. Бодайбо и района

от 26.02.2018 г. № 147-р \_

**Правила работы со съемными носителями информации**

**в Администрации г. Бодайбо и района**

1. Ограничить доступ к компьютеру посторонних лиц. При временном отсутствии на рабочем месте – блокировать компьютер (win + L или Ctrl+Alt+Delete).

1. Не оставлять в компьютере носители с информацией, если они не используются для работы.

2. Перед началом работы с устройством проверить его антивирусом на наличие вредоносных программ.

3. Исключить копирование с данного носителя файлов сомнительного содержания и установку нелицензионного программного обеспечения.

4. Категорически запрещается передавать съемные носители и пароли от компьютера другим лицам.

5. Не рекомендуется использовать свои пароли для доступа к ресурсам сети с компьютеров других пользователей.

6. Все находящиеся на хранении и в обращении съемные носители с персональными данными подлежат учёту. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

7. Учет и выдачу съемных носителей персональных данных по прилагаемой форме осуществляет ведущий аналитик-специалист по информатизации отдела организационной работы (далее – уполномоченный сотрудник), на которого возложены функции хранения носителей персональных данных. Специалисты получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

8. Запрещается:

- хранить съемные носители с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

- выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому, в гостиницах и т. д.

9. При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные.

Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного

пользования. Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения управляющего делами.

10. О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений немедленно ставится в известность управляющий делами. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы персонального учета съемных носителей персональных данных.

11. Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению.

Уничтожение съемных носителей с конфиденциальной информацией осуществляется уполномоченной комиссией. По результатам уничтожения

носителей составляется акт.

Подготовил:

Ведущий аналитик-специалист

отдела организационной работы С.В. Кравец

Приложение № 4

к распоряжению Администрации г. Бодайбо и района

от 26.02.2018 г. № 147-р

**Правила резервного копирования информации**

**в Администрации г. Бодайбо и района**

1. **Общие положения**

1.1. Резервному копированию подлежит информация следующих основных категорий:

- личные каталоги пользователей на файловых серверах;

- информация, необходимая для восстановления серверов и систем управления базами данных;

- информация автоматизированных систем, в том числе баз данных;

- рабочие копии установочных компонентов программного обеспечения рабочих станций.

1. **Создание резервных копий**

2.1. Резервное копирование данных информационной системы производится ведущим аналитиком-специалистом по информатизации отдела организационной работы, в должностные обязанности которого входят функции по обеспечению работоспособности данной информационной системы (далее – уполномоченный сотрудник).

2.2. Для создания резервных копий данных применяются компактные (сменные) носители информации (CD/DVD, внешние жесткие диски и т.п.), зарегистрированные в соответствии с правилами работы с документами, содержащими информацию ограниченного доступа.

2.3. Технология создания резервных копий определяется правилами эксплуатации технических и программных средств.

2.4. Носители созданных резервных копий данных должны быть промаркированы уполномоченным сотрудником. Маркировка должна содержать номер копии, дату ее создания, наименование информационной системы данных.

2.5. Уполномоченным сотрудником после создания резервной копии заводится Реестр приема/передачи электронного носителя копии данных.

2.6. Резервное копирование производится ежемесячно не позднее 15-го числа месяца.

2.7. При создании резервных копий допускается их архивирование специальными программными средствами.

1. **Передача резервных копий**

3.1. Передача электронного носителя резервной копии с данными, содержащими конфиденциальную информацию, должна осуществляться при строгом соблюдении правил работы с носителями, содержащими информацию ограниченного доступа.

3.2. В течение рабочего дня после создания резервной копии электронный носитель с ней помещается в специальный контейнер и опечатывается. На контейнер наносится маркировка, соответствующая маркировке электронного носителя информации.

3.3. Контейнеры, используемые для хранения электронных носителей информации, должны быть зарегистрированы в соответствующем журнале.

1. **Хранение резервных копий**

4.1. Хранение резервных копий осуществляется в течение 3-х месяцев.

4.2. Использование носителей информации при резервном хранении

должно подчиняться принципу ротации носителей, при котором для записи текущей копии используется носитель с самой ранней датой создания предыдущей копии.

4.3. Для хранения носителей резервных копий должны использоваться помещения, создающие оптимальные условия для физической сохранности и защиты от воздействия неблагоприятных факторов.

4.4. Удаление электронных данных резервной копии для повторного использования носителя информации производится не ранее истечения срока хранения (3 месяца) с составлением акта.

1. **Восстановление электронных данных**

5.1. Восстановление электронных данных из резервной копии производится на специализированных рабочих местах, оснащенных необходимым оборудованием уполномоченным сотрудником.

5.2. Основанием для инициирования процедуры восстановления служит мотивированная заявка начальника отдела на имя мэра г. Бодайбо и района.

5.3 Восстановление утраченных данных производится из резервной копии, обеспечивающей минимальную потерю данных, содержащихся в информационном ресурсе.

Подготовил:

Ведущий аналитик-специалист

отдела организационной работы С.В. Кравец