АДМИНИСТРАЦИЯ НОЖАЙ-ЮРТОВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА ЧЕЧЕНСКОЙ РЕСПУБЛИКИ

366220, ЧР, Ножай-Юртовский район, с. Ножай-Юрт, ул. А.Кадырова , 3 nojayurt@mail.ru.т/ф 8 (87148) 2-22-57

РАСПОРЯЖЕНИЕ

«16» 03 2015 г. № 78

О Политике информационной безопасности администрации Ножай-Юртовского муниципального района Чеченской Республики

В целях обеспечения информационной безопасности в администрации Ножай-Юртовского муниципального района и во исполнение Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

1.Утвердить прилагаемую Политику информационной безопасности администрации Ножай-Юртовского муниципального района;

2.Ознакомить работников администрации Ножай-Юртовского муниципального района с Политикой информационной безопасности.

3. Ответственность за организацию и проведение работ по обеспечению информационной безопасности администрации Ножай-Юртовского муниципального района возложить на заместителя начальника организационного отдела администрации.

4.Контроль за выполнением настоящего распоряжения возложить на заместителя главы - управляющего делами администрации Ножай-Юртовского муниципального района Чеченской Республики Мадаеву А.Х..

5.Настоящее распоряжение вступает в силу со дня его подписания.

Глава администрации
Ножай-Юртовского муниципального района А-К. У. Гарбаев

УТВЕРЖДЕНА
распоряжением администрации
Ножай-Юртовского муниципального
района Чеченской Республики
от «16» 03 2015 г. № 88

Политика информационной безопасности Администрации Ножай-Юртовского муниципального района Чеченской Республики

1. Общие положения

Политика информационной безопасности в администрации Ножай-Юртовского муниципального района предполагает создание совокупности взаимоувязанных нормативных и организационно-распорядительных документов, определяющих порядок обеспечения безопасности информации в информационных системах, управления и контроля информационной безопасности, а также выдвигающих требования по поддержанию подобного порядка.

Политика информационной безопасности отражает позицию администрации Ножай-Юртовского муниципального района по вопросу обеспечения информационной безопасности.

Политика информационной безопасности направлена на:

нормативное регулирование процесса обмена защищаемой информацией администрации Ножай-Юртовского муниципального района с взаимодействующими структурами, юридическими и физическими лицами;

установление определенного организационно-правового режима использования информационных ресурсов Ножай-Юртовского муниципального района;

разработку системы нормативных документов, действующих на правах стандартов и определяющих степень конфиденциальности информации, требуемый уровень защищенности объектов информатизации администрации Ножай-Юртовского муниципального района, ответственность должностных лиц и сотрудников за соблюдение этих требований;

реализацию комплекса организационных, инженерно-технических, технических и аппаратно-программных мероприятий по предупреждению несанкционированных действий с информацией и защиту ее от утечки по техническим каналам;

предоставление пользователям необходимых сведений для сознательного поддержания установленного уровня защищенности объектов информатизации администрации Ножай-Юртовского муниципального района;

организацию постоянного контроля эффективности принятых мер защиты и функционирования системы обеспечения информационной безопасности;

создание в администрации Ножай-Юртовского муниципального района резервов и возможностей по ликвидации последствий нарушения режима

защиты информации и восстановления системы обеспечения информационной безопасности.

2.Цель обеспечения информационной безопасности

Основной целью является обеспечение информационной безопасности администрации Ножай-Юртовского муниципального района, что предполагает эффективное информационное обслуживание и управление всеми средствами комплексной защиты информации, адекватное отражение угроз информационной безопасности.

Главная цель принимаемых мер защиты информации состоит в том, чтобы гарантировать целостность, достоверность, доступность и конфиденциальность информации во всех ее видах и формах, включая документы и данные, обрабатываемые, хранимые и передаваемые в информационно - вычислительных и телекоммуникационных системах (далее - информационные системы) администрации Ножай-Юртовского муниципального района, независимо от типа носителя этих данных. Организация информационных ресурсов должна обеспечивать их достаточную полноту, точность и актуальность, чтобы удовлетворять потребности администрации Ножай-Юртовского муниципального района, не жертвуя при этом основными принципами информационной безопасности, описанными в данной Политике.

Ответственность за организацию и проведение работ по обеспечению информационной безопасности администрации Ножай-Юртовского муниципального района несет заместитель начальника организационного отдела администрации Ножай-Юртовского муниципального района. Методическое руководство и контроль за эффективностью предусмотренных мер защиты осуществляет управляющий делами администрации Ножай-Юртовского муниципального района, в случае его отсутствия – начальник отдела по организационным и общим вопросам.

3. Объекты информационной безопасности

Объектом защиты в контексте данной Политики являются информационные ресурсы администрации Ножай-Юртовского муниципального района, обрабатываемые в информационных системах и ее функциональных подсистемах, содержащие сведения доступ к которым ограничен, и используемые в процессах сбора, обработки, накопления, хранения и распространения в границах информационных систем.

Основными объектами защиты администрации Ножай-Юртовского муниципального района являются:

информационные ресурсы, содержащие сведения, отнесенные к государственной тайне;

информационные ресурсы ограниченного распространения, в том числе, содержащие конфиденциальные сведения;

информационные ресурсы, представляющие коммерческую ценность;

программные информационные ресурсы, а именно, системное программное обеспечение;

физические информационные ресурсы:

а) компьютерное аппаратное обеспечение всех видов; носители информации всех видов (электронные, бумажные и проч.);

б) все расходные материалы и аксессуары, которые прямо или косвенно взаимодействуют с компьютерным программным обеспечением;

в) технические сервисы (отопление, освещение, энергоснабжение, кондиционирование воздуха и т.п.).

Следует также отметить, что указанные выше основные объекты защиты являются наиболее ценными ресурсами, и, следовательно, по отношению к ним должны применяться самые эффективные правила и методы защиты. Их доступность, целостность и конфиденциальность могут иметь особое значение для обеспечения имиджа администрации Ножай-Юртовского муниципального района, эффективности его функционирования и т.д. Доступность, целостность и конфиденциальность в обязательном порядке. должны учитываться при разработке организационно- распорядительной документации по обеспечению информационной безопасности для системы в целом и для каждого ее ресурса в отдельности.

4.Задачи обеспечения информационной безопасности

Основными задачами обеспечения информационной безопасности администрации Ножай-Юртовского муниципального района являются:

инвентаризация и систематизация всех информационных ресурсов;

обеспечение безопасности информационных ресурсов (уменьшение риска их случайной или намеренной порчи, уничтожения или хищения);

сведение к минимуму финансовых, временных и прочих потерь, связанных с нарушением информационной безопасности и физическими неисправностями программного обеспечения, а также осуществление мониторинга и реагирование по случаям инцидентов;

обеспечение безопасной, четкой и эффективной работы сотрудников администрации Ножай-Юртовского муниципального района с его информационными ресурсами;

сведение к минимуму финансовых затрат на поддержание функционирования программного обеспечения и автоматизированной системы в целом на должном уровне (обновление программного обеспечения, бесперебойное обеспечение системы расходными материалами и др.);

сведение пользования информационными ресурсами к единой системе организационно-распорядительной документации.

5.Принципы обеспечения информационной безопасности

При построении системы защиты необходимо придерживаться следующих принципов:

применение разнородных систем обеспечения информационной безопасности;

достоинства одних частей системы обеспечения информационной безопасности должны перекрывать недостатки других;

система обеспечения информационной безопасности должна строиться многоуровневой;

в зоне максимальной безопасности должны располагаться особо важные информационные ресурсы;

непрерывность и целенаправленность процесса обеспечения информационной безопасности;

усиление защиты информации во время нештатных ситуаций;

обеспечение возможности регулирования уровня информационной безопасности без изменения функциональной базы системы информационной безопасности;

обеспечение простоты в применении механизмов защиты для сотрудников администрации района.

6. Оценка рисков

Для оценки рисков при составлении и последующем пересмотре организационно-распорядительных документов необходимо систематически рассматривать следующие аспекты:

ущерб, который может нанести деятельности администрации Ножай-Юртовского муниципального района серьезное нарушение информационной безопасности, с учетом возможных последствий нарушения конфиденциальности, целостности и доступности информации;

реальную вероятность нарушения защиты угрозы утечки информации.

7.Требования в отношении обучения вопросам информационной безопасности

Основной целью обучения является:

обеспечение уверенности в осведомленности сотрудников администрации Ножай-Юртовского муниципального района об угрозах и проблемах, связанных с информационной безопасностью, об ответственности в соответствии с законодательством;

знание работы администрации района, правильного использования средств обработки информации прежде чем им будет предоставлен доступ к информации или услугам;

оснащение работников администрации Ножай-Юртовского муниципального района всем необходимым для соблюдения требований политики безопасности при выполнении служебных обязанностей.

Работники администрации Ножай-Юртовского муниципального района должны знать и выполнять требования организационно-распорядительных документов в области информационной безопасности, требования обеспечения безопасности обработки информации на средствах вычисли -

тельной техники, правила работы в сети Интернет, уметь работать с системой электронного документооборота; операционными системами на уровне пользователя, антивирусным программным обеспечением, офисным программным обеспечением.

Заместитель начальника организационного отдела администрации, ответственный за обеспечение информационной безопасности, должен обучать сотрудников администрации Ножай-Юртовского муниципального

района использованию средств обработки защиты информации, чтобы свести к минимуму возможные риски безопасности.

8.Правила физической защиты

Перед внедрением и использованием нового программного обеспечения или иного ранее не использовавшегося информационного ресурса необходимо разработать для него правила обеспечения безопасности и использовать их наряду с правилами, изложенными в данном разделе.

Перед установкой и использованием какого-либо компьютерного обеспечения в обязательном порядке следует ознакомиться с информацией, предоставленной разработчиком, и строго ей следовать.

Перед проведением крупной модернизации или ремонта, перед выполнением манипуляций непосредственно с носителями информации необходимо выполнить резервное копирование данных.

После выполнения процесса модернизации программного обеспечения необходимо обязательно провести внеплановое техническое обслуживание всей системы.

При размещении компьютерного оборудования в помещении, а также в процессе его эксплуатации, приоритетным является обеспечение для него безопасного функционирования, соответствующего положениям, изложенным в прилагаемой к нему документации. В период простоя устройства необходимо обеспечить сохранность его работоспособности и внешнего вида.

Все приобретенное компьютерное программное обеспечение должно регистрироваться в специальном журнале с указанием информации о его покупке. Также следует тщательно регистрировать все действия по модернизации компьютерного программного обеспечения.

Всю документацию на компьютерное оборудование и программное обеспечение должны обязательно сохраняться.

Следует в полном объеме и неукоснительно соблюдать правила эксплуатации компьютерных компонентов.

Техническое обслуживание компьютерного оборудования и программного следует производить регулярно, желательно в соответствии с заранее составленным расписанием и с учетом рекомендаций разработчиков данного оборудования и программ (с данными рекомендациями следует

внимательно ознакомиться до выполнения каких-либо действий по обслуживанию).

Техническим обслуживанием считаются также и мероприятия по резервному копированию данных, которые должны неукоснительно исполняться. Они должны выполняться строго регулярно и не реже, чем раз в неделю. Если это возможно, стоит сделать повторную копию данных и разместить ее на хранение, отдельно от первой. Сразу же после проведения резервного копирования данных необходимо каким-либо способом убедиться в работоспособности и корректности полученной копии.

Резервному копированию в обязательном порядке подлежат:

все конфиденциальные данные сотрудников в автоматизированной системе;

все исходные материалы для разработки собственного программного обеспечения и прочих проектов;

такие данные системы, без которых невозможна ее нормальная работа;

все прочие важные данные, которые записаны на физически ненадежных носителях информации и носителях, поддерживающих операции перезаписи;

любые другие данные по решению уполномоченных сотрудников администрации Ножай-Юртовского муниципального района.

Во время резервного копирования данных, а также во время записи любой информации на носители информации однократной записи, нельзя производить другие виды работ на той компьютерной системе, при помощи которой осуществляется эта запись.

Все носители (электронные, бумажные) с конфиденциальной информацией и резервными копиями должны храниться в недоступном для посторонних, защищенном от света и других вредоносных воздействий месте с соблюдением правил безопасного хранения для данного вида носителя информации. Носителям с особо ценной информацией следует уделять повышенное внимание.

Все расходные материалы следует использовать максимально эффективно, не допуская нерационального их использования.

Желательно предпринять ряд мер по энергосбережению для тех устройств, которые временно не используются или находятся в состоянии ожидания.

Запрещается курить, употреблять пищу и напитки непосредственно вблизи компьютера. Необходимо предпринять меры, чтобы обезопасить компьютерное оборудование от повреждения в данном случае.

В течение внедрения и использования программного обеспечения или иного ранее не использовавшегося информационного ресурса необходимо приложить все усилия, чтобы научиться эффективно его применять.

Необходимо в обязательном порядке записать все наиболее важные установки и настройки системы в состоянии ее нормального функционирования. Подобные записи приравниваются к программной документации, и должны соответствующим образом обслуживаться.

Необходимо размещать системы вывода информации (мониторы, дисплеи и т.д.) компьютеров так, чтобы они не были видны со стороны двери, окон и тех мест в помещениях, которые не контролируются.

Необходимо предпринять ряд мер, благодаря которым компьютерные системы пользователя будут обеспечены стабильным электропитанием. Обязательным является использование хотя бы простых средств по обеспечению надежности электропитания системы (сетевые фильтры, заземление и т.д.).

При возникновении какой-либо аварийной ситуации необходимо немедленно прекратить эксплуатацию аварийного устройства. Немедленно поставить в известность заместитель начальника организационного отдела администрации.

Следует составить подробные технологические схемы для проведения различного рода мероприятий, связанных с программным обеспечением (техническое обслуживание, правила техники безопасности, резервное копирование данных и т.п.).

Необходимо рассмотреть возможность применения различных систем автоматизированного мониторинга текущего состояния аппаратных информационных ресурсов, и при первой же возможности внедрить их, по крайней мере, на наиболее важных и ответственных участках.

В течение процесса списания компьютерной техники, носителей информации и др. необходимо позаботиться о том, чтобы после выполнения процедуры переноса основных информационных ресурсов со списываемой техники, было произведено полное и безвозвратное уничтожение содержащейся на ней конфиденциальной и любой другой информации.

Необходимо обязательно разработать план действий по продолжению работы и обеспечению безопасности данных на случай, если выйдут из строя какие-либо программные части компьютерной системы. Данный план должен систематически проверяться на актуальность и при необходимости пересматриваться.

9.Правила внешнего доступа

После установки системы и перед первым выходом в сеть необходимо в обязательном порядке принять комплекс мер по установлению защиты от вредоносного воздействия сети.

В системе должны быть предприняты все возможные меры для предотвращения распространения в ней компьютерных вирусов и прочей потенциально опасной для ее безопасности информации. Все сотрудники администрации Ножай-Юртовского муниципального района обязаны принимать участие в реализации этих мер и никакими своими действиями не должны препятствовать их проведению.

Необходимо строго контролировать с помощью соответствующего программного обеспечения всю входящую и исходящую информацию на

наличие вирусов и прочей потенциально опасной информации. Необходимо также тщательно настроить параметры безопасности того программного и обеспечения, которое непосредственно будет иметь доступ в сеть.

Система должна подвергаться периодической проверке антивирусными средствами (не реже чем раз в месяц) и другими средствами, обеспечивающими безопасность в системе (если таковые имеются). В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники обязаны: приостановить работу на компьютере, немедленно поставить в известность о факте обнаружения зараженных вирусом файлов заместитель начальника организационного администрации Ножай-Юртовского муниципального района, владельца зараженных файлов, смежные отделы, использующие эти файлы в работе. Все внешние носители информации, полученные из сомнительных или неизвестных источников, должны подвергаться полному антивирусному сканированию перед использованием.

Необходимо регулярно обновлять версии программного обеспечения, связанного с обеспечением безопасности системы; устанавливать официальные обновления программ, которые имеют прямое или косвенное отношение к работе с сетью. Сюда же относятся и обновления, связанные с управлением аппаратным обеспечением системы (драйвера устройств и т.п.).

При обнаружении зараженных вирусами данных, эти данные должны немедленно и безвозвратно удаляться. Исключение составляют лишь важные данные, для которых имеет смысл попробовать применить процедуры восстановления.

Следует с большой осторожностью относиться к программам, в которых присутствуют определенного рода уязвимости для несанкционированного проникновения.

Необходимо внимательно проанализировать систему данных сотрудников и обеспечить ее структурированное хранение на носителях информации. Все данные должны классифицироваться согласно их применению.

10. Правила доступа в Internet

Программное обеспечение, обеспечивающее защиту системы от проникновения, должно быть задействовано в полном объеме на протяжении всего сеанса связи с Интернетом.

Допускается временное отключение части программного обеспечения, обеспечивающего защиту системы, в тех случаях, когда без этого невозможно выполнить какой-либо вид работы. После выполнения данного вида работ отключенные части системы защиты должны быть вновь задействованы.

Сотрудники администрации Ножай-Юртовского муниципального района допускаются к использованию Интернета только после прохождения инструктажа, в котором разъяснялась бы Политика безопасности данной системы.

Сотрудники должны стараться предоставлять о себе как можно меньше информации в сеть, а тем более не должны разглашать любую конфиденциальную информацию.

Все файлы, полученные из Интернета, перед их использованием должны пройти дополнительную антивирусную проверку.

После каждого сеанса связи с Интернетом необходимо проводить очистку системы от ненужных служебных данных, которые появились в результате соединения с сетью.

11. Правила безопасности электронной почты

Наиболее важные сообщения, полученные по электронной почте должны архивироваться.

Все ранее сохраненные почтовые сообщения, потерявшие свою актуальность, должны быть тщательным образом безвозвратно уничтожены со всех носителей информации.

Необходимо в обязательном порядке сканировать каждое исходящее и получаемое сообщение электронной почты на наличие потенциально опасного содержимого. Почтовые сообщения, не удовлетворяющие установленным требованиям, должны немедленно и безвозвратно удаляться.

Необходимо на всех используемых почтовых ящиках установить, при необходимости, ограничения на содержимое и размер принимаемых сообщений и отсеивать те сообщения, которые не удовлетворяют установленным критериям.

После отправки письма по электронной почте необходимо хранить его до тех пор, пока не будет уверенности (подтверждения) в том, что оно достигло получателя. Это же касается и любых других способов передачи информации. Все файлы (особенно исполнимые и файлы больших размеров), полученные вместе с сообщением электронной почты без какого-либо запроса со стороны сотрудника администрации Ножай-Юртовского муниципального района (особенно от неизвестного адресата) должны немедленно и безвозвратно удаляться без оценки их полезности. Если нет полной уверенности в необходимости удаления данного сообщения, необходимо, в случае если адресат известен и только в этом случае, дополнительно связаться с ним (не по электронной почте) и попросить у него подтверждения в посылке сообщения.

Сотрудники администрации Ножай-Юртовского муниципального района не должны участвовать в рассылке посланий, передаваемых по цепочке, не должны отвечать на оскорбительные и провокационные сообщения. Такие послания должны быть безвозвратно удалены из системы. Также необходимо принять все возможные меры по обеспечению прекращения получения из данного источника подобной информации в будущем.

12. Правила управления доступом

В отношении всех работников администрации Ножай-Юртовского муниципального района необходимо осуществлять комплекс мер по обеспечению их работы в автоматизированной, в частности регистрацию, выделение определенных информационных ресурсов и установление четких не избыточных, а только необходимых, прав доступа к ним.

Использование имен и паролей для доступа к информационным ресурсам:

необходимо использовать пароли везде, где это целесообразно;

следует придерживаться следующих правил составления и использования паролей - пароль должен состоять не менее чем из шести символов, состоять из произвольных комбинаций букв, цифр и других символов или же представлять собой бессмысленную комбинацию слов, включающую буквы верхнего регистра;

запрещено использовать одинаковые пароли для доступа к разным информационным ресурсам;

хранение паролей осуществляется операционной системой, и установленный ею уровень защиты не может быть ослаблен;

запрещено сообщать свои пароли третьим лицам в какой бы то ни было форме;

пароли запрещается писать на компьютерных терминалах, помещать в общедоступные места;

все имена и пароли для доступа к каким-либо информационным ресурсам, которые не используются, подлежат надежной блокировке;

система должна предотвращать попытки регистрации и перерегистрации тех сотрудников, чьи имена и пароли для входа в систему не соответствуют установленным правилам;

при получении доступа к какому-либо информационному ресурсу при помощи процесса авторизации по имени и паролю сотрудник не должен произносить эти данные вслух при вводе их в систему;

13. Управление непрерывностью работы

Основной целью управления непрерывностью работы администрации Ножай-Юртовского муниципального района является противодействие прерывания работы и защита рабочих процессов от последствий при значительных сбоях или бедствиях.

Необходимо обеспечивать управление непрерывностью работы с целью минимизации отрицательных последствий, вызванных нарушениями безопасности. Последствия от нарушений безопасности и отказов в обслуживании необходимо анализировать, по результатам анализа разрабатывать и внедрять планы обеспечения непрерывности работы с целью восстановления рабочих процессов в течение требуемого времени при их нарушении.

Планирование должно сопровождаться оценкой рисков с целью определения последствий этих прерываний (как с точки зрения масштаба повреждения, так и периода восстановления). Оценка риска должна распространяться на все рабочие процессы и не ограничиваться только средствами обработки информации. В зависимости от результатов оценки рисков необходимо разработать стратегию для определения общего подхода к обеспечению непрерывности работы. Необходимо, чтобы план обеспечения непрерывности работы предусматривал следующие мероприятия по обеспечению информационной безопасности:

определение и согласование всех обязанностей должностных лиц и процедур на случай чрезвычайных ситуаций;

внедрение в случае чрезвычайных ситуаций процедур, обеспечивающих возможность восстановления рабочего процесса в течение требуемого времени;

особое внимание следует уделять оценке зависимости работы от внешних факторов и существующих контрактов;

документирование согласованных процедур и процессов;

соответствующее обучение сотрудников действиям при возникновении чрезвычайных ситуаций, включая кризисное управление.

14. Ответственность за нарушение политики безопасности

Все сотрудники администрации Ножай-Юртовского муниципального района несут ответственность за нарушение требований настоящей Политики информационной безопасности согласно действующему законодательству в области защиты информации.

15. Сопровождение правил

Все без исключения положения данного документа имеют одинаково равную силу и должны неукоснительно соблюдаться.

Политика информационной безопасности должна в обязательном порядке периодически пересматриваться.

Регулярно должна проводиться оценка текущего состояния имеющихся у сотрудников информационных ресурсов. В результате этой оценки в соответствующие документы по безопасности должны вноситься необходимые изменения.

Если возникли непредвиденные обстоятельства, требующие срочного пересмотра Политики информационной безопасности, то такой пересмотр может быть осуществлен до планового пересмотра.

При возникновении серьезных проблем с безопасностью системы (при успешном взломе системы безопасности) возникшая проблема должна быть немедленно проанализирована, а организационно-распорядительные документы по информационной безопасности - пересмотрены в соответствии с проведенным анализом. При этом нужно рассматривать проблему в целом

и излишне не фокусировать внимание на отдельных деталях.

Копия политики информационной безопасности должна находиться в доступном для сотрудников администрации Ножай-Юртовского муниципального района месте.