РОССИЙСКАЯ ФЕДЕРАЦИЯ
КАРАЧАЕВО-ЧЕРКЕССКАЯ РЕСПУБЛИКА

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «ДЕТСКИЙ САД «СКАЗКА» СТ.ЗЕЛЕНЧУКСКОЙ»

П Р И К А З

25.02.2015 **ст.Зеленчукская** **№ 28а**

О защите информации, содержащейся в информационной системе МБДОУ «Детский сад «Сказка» ст.Зеленчукской».

Во исполнение Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Решения коллегии Государственной технической комиссии России при Президенте Российской Федерации №7.2/02.03.2001г., приказа Федеральная служба по техническому и экспортному контролю Федеральная служба безопасности Российской Федерации от 31.08.2010 №416/489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования», в целях проведения работ по защите информации ограниченного доступа,

ПРИКАЗЫВАЮ:

1. Утвердить Положение о порядке организации и проведения работ по защите информации в МБДОУ «Детский сад «Сказка» ст.Зеленчукской» согласно приложению №1.
2. Утвердить должностную инструкцию для лица, ответственного за защиту информационной системы МБДОУ согласно приложению №2.
3. Ответственным за защиту информационной системы муниципального бюджетного дошкольного образовательного учреждения «Детский сад «Сказка» ст.Зеленчукской» от несанкционированного доступа к информации - администратором защиты (безопасности) информации – назначить главного бухгалтера Попову О.И.
4. Работники МБДОУ «Детский сад «Сказка» ст.Зеленчукской», осуществляющие свою трудовую деятельность с использованием автономных персональных электронно-вычислительных машин:

несут персональную ответственность за безопасность информации, обеспечивают конфиденциальность (т.е. сохранение втайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами;

ежемесячно обновляют авторизированные пароли на автономные персональные электронно-вычислительные машины в Книге учета авторизированных паролей на автономные персональные электронно-вычислительные машины детского сада.

5. Ответственным за хранение Книги учета авторизированных паролей на автономные персональные электронно-вычислительные машины МБДОУ «Детский сад «Сказка» ст.Зеленчукской» назначена бухгалтер Терентьева Е.Н.
6. Контроль за исполнением настоящего приказа оставляю за собой.

Заведующая МБДОУ
«Детский сад «Сказка» Т.А.Терентьева

С приказом ознакомлены:
Попова О.И.
Киселёва С.В.
Терентьева Е.Н.
Н.И.Рубанова

Приложение №1 к приказу
заведующей МБДОУ
от 25.02.2015 №28а

Положение
о порядке организации и проведения работ по защите информации в муниципальном бюджетном дошкольном образовательном учреждении «Детский сад «Сказка» ст.Зеленчукской»

1. Общие положения

1.1. Настоящее Положение о порядке организации и проведения работ по защите информации в управлении образовании администрации Зеленчукского муниципального района (далее – Положение) разработано на основании Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Решения коллегии Государственной технической комиссии России при Президенте Российской Федерации № 7.2/02.03.2001г., приказа Федеральная служба по техническому и экспортному контролю Федеральная служба безопасности Российской Федерации от 31.08.2010 № 416/489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования».

1.2. Под информацией, гребующей защиты, понимаются сведения о МБДОУ «Детский сад «Сказка» ст.Зеленчукской» (далее – ДОУ) и его деятельности, на распространение которых накладываются ограничения Указом Президента Российской Федерации «Об утверждении перечня сведений конфиденциального характера» от 06.03.1997 № 188, действующим законодательством и отраженные в Сводном перечне сведений конфиденциального характера, утвержденном Президентом Карачаево-Черкесской Республики от 06.09.2005 № 152.

1.3. Цель данного Положения - на основании действующих законодательных актов и руководящих документов по защите информации создать необходимые организационно - правовые основы для эффективной защиты конфиденциальной информации.

1.4. Положение определяет порядок организации в ДОУ работ по разработке и эксплуатации объектов информатизации и систем защиты информации (СЗИ).

1.5. Положение предназначено для практического использования специалистом, ответственным по защите информации, и его руководителем в ДОУ.

1.6. Требования настоящего Положения являются обязательными для исполнения всеми должностными лицами ДОУ.

1.7. За общее состояние и организацию работ по технической защите конфиденциальной информации отвечает заведующая МБДОУ.

Контроль выполнения требований настоящего Положения возлагается на специалиста, ответственного по защите информации.

1.8. Для оказания услуг в области защиты информации могут привлекаться специализированные организации, имеющие лицензию на этот вид деятельности.

1.9. Используемые программные средства защиты информации должны быть сертифицированы в соответствии с требованиями положения «О сертификации средств защиты информации», утвержденного постановлением Правительства Российской Федерации от 26.06.1995 № 608.

1.10. Положение может уточняться и корректироваться по мере необходимости.

2. Охраняемые сведения и потенциальные угрозы

2.1. Результатом защиты информации является предотвращение ущерба ДОУ из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию.

Целями технической защиты конфиденциальной информации в ДОУ являются:

- предотвращение несанкционированного доступа (НСД) к информации, ее разрушения, искажения, уничтожения, блокировки и несанкционированного копирования в системах и средствах автоматизации.

2.2. Замысел достижения целей защиты информации.

Замыслом достижения целей защиты информации является обеспечение защиты информации путем строгого соблюдения действующих норм и требований ФСТЭК России (Гостехкомиссии России), созданием СЗИ объектов информатизации.

2.3. Охраняемые сведения:

- конфиденциальная информация, обрабатываемая с использованием технических средств;

- сведения конфиденциального характера, содержащиеся в речевой информации.

2.4. Потенциальные угрозы информационной безопасности объектов.

В качестве угроз информационной безопасности объектов необходимо рассматривать:

- использование разведками иностранных государств технических средств для получения охраняемых сведений, а также воздействие на информационные ресурсы автоматизированных систем с целью разрушения, искажения и блокирования информации;

- несанкционированный удаленный доступ (из-за пределов контролируемых зон) в сети систем информатизации и связи объектов с целью получения информации ограниченного доступа;

- преднамеренные действия нарушителей и злоумышленников, незаконным путем проникших на объекты, посредством контактного несанкционированного доступа к элементам автоматизированных систем, к носителям информации, к вводимой и выводимой информации, к программному обеспечению, а также подключения к линиям связи;

- непреднамеренные действия персонала, приводящие к утечке, искажению, разрушению информации, подлежащей защите, в том числе ошибки проектирования, разработки и эксплуатации технических и программных средств автоматизированных систем.

2.5. Одной из возможных угроз информационным ресурсам автоматизированных систем при определенных условиях может являться компьютерная разведка, направленная на извлечение, систематизацию и специальную обработку открытой информации из информационно-вычислительных сетей, телекоммуникационных систем, а также информации об особенностях их построения и функционирования. Таким условием может быть несанкционированный выход с отдельных рабочих мест автоматизированных систем в глобальные информационные сети. Бесконтрольное подключение к информационно-вычислительным сетям общего пользования компьютерных средств и оргтехники, находящихся на защищаемых объектах, может служить предпосылкой к утечке охраняемой информации.

3. Порядок аттестации и ввода в эксплуатацию объектов информатизации

3.1. Все объекты информатизации должны быть аттестованы на соответствие установленным нормам и требованиям по защите информации.

3.2. Аттестация по требованиям безопасности информации является необходимым условием для ввода в эксплуатацию объектов информатизации.

3.3. В ДОУ аттестации подлежат следующие объекты информатизации:

- объекты вычислительной техники, используемые для обработки конфиденциальной информации.

3.4. Аттестационные испытания проводятся комиссией, формируемой аккредитованным ФСТЭК России органом по аттестации, по программе, согласованной с ДОУ.

3.5. Для проведения испытаний аттестационной комиссии ответственным по защите информации подготавливаются и представляются:

- технический паспорт на объект информатизации;

- акт классификации автоматизированной системы по требованиям защиты информации;

- состав программных средств, входящих в АС;

- состав и схемы размещения средств защиты информации;
- план контролируемой зоны;
- схемы и характеристики систем электропитания и заземления объекта информатизации;
- организационно-распорядительная документация разрешительной системы доступа персонала к защищаемым ресурсам АС (обсуждаемым вопросам);
- инструкции пользователям и администратору безопасности информации;
- инструкции по эксплуатации средств защиты информации;
- протоколы специальных исследований технических средств и систем;
- сертификаты соответствия требованиям по безопасности информации на используемые средства защиты информации.

3.6. Аттестационные испытания объекта информатизации проводятся до полного их завершения в соответствии с программой испытаний вне зависимости от промежуточных результатов испытаний и завершаются выдачей Аттестата соответствия.

3.7. Перечень характеристик, об изменениях которых требуется обязательно извещать орган по аттестации, указывается в Аттестате соответствия.

3.8. Разрешение на использование средств для обработки конфиденциальной информации.

3.9. По результатам аттестации специалистом по защите информации разрабатываются и доводятся до исполнителей инструкции, памятки и рекомендации о порядке выполнения мероприятий по защите информации.

3.10. Обсуждение и обработка конфиденциальной информации до окончания аттестации и распоряжения о вводе в строй объектов информатизации запрещается.

4. Организационные и технические мероприятия по защите конфиденциальной информации

4.1. Защита сведений конфиденциального характера в ДОУ достигается путем создания системы защиты информации, которая включает комплекс организационных и программных мероприятий, направленных на закрытие технических каналов утечки информации.

4.2. Мероприятия по защите информации являются составной частью деятельности ДОУ, проводятся с целью закрытия возможных технических каналов утечки информации.

5. Обязанности и права должностных лиц

5.1. Заведующая ДОУ:

- отвечает за организацию работ по защите информации в ДОУ;
- утверждает акты классификации АС.

5.2. Специалист по защите информации:

- осуществляет непосредственное руководство и координацию работ по защите информации в соответствии с руководящими документами по данному вопросу;
- разрабатывает организационно-распорядительные документы по вопросам защиты информации;
- специалист по защите информации имеет право:
- контролировать исполнение приказов и распоряжений вышестоящих организаций и заведующей ДОУ по вопросам сохранения конфиденциальной информации;
- требовать от работников представления письменных объяснений по фактам нарушения режима конфиденциальности;
- рекомендовать запрещать эксплуатацию систем обработки и передачи информации при несоблюдении требований по защите информации;
- готовить проекты договоров на выполнение работ по защите информации со сторонними организациями, имеющими необходимые лицензии;
- вносить предложения по совершенствованию системы защиты информации, изменению категорий объектов информатизации, степени конфиденциальности обрабатываемой информации.

5.3. Программист ДОУ:

- обеспечивает защиту информации, циркулирующей в АС, в том числе передаваемой по каналам связи, организовывает работы по проведению передачи информации, по аттестации объектов ВТ на соответствие нормативным требованиям;

- проводит систематический контроль работы средств защиты информации, применяемых на объектах ВТ, а также следит за выполнением комплекса организационных мероприятий по обеспечению безопасности информации;

- обобщает и анализирует сведения о противоправных устремлениях к информации, попытках преодоления систем защиты информации, используемых при этом методах и средствах;

- анализирует состояние защищенности информационных ресурсов сети, готовит предложения по совершенствованию систем защиты, систематизирует и распространяет положительный опыт работы;

- принимает меры по предупреждению угроз безопасности информации, возникающих в результате случайных ошибок персонала при обработке электронных документов с учетом специфики конкретного места обработки и применяемых средств защиты;

- принимает участие в оценке реальной опасности утечки информации, подлежащей защите при использовании технических средств, в разработке эффективных и экономически обоснованных мер по ее защите;

- организовывает работу по эксплуатации системы защиты информации в автоматизированных системах обработки электронных документов;

- проводит работы по внедрению программных средств защиты информации от несанкционированного доступа к ней на действующих автоматизированных системах и отдельных средствах вычислительной техники;

- обеспечивает эксплуатацию программных средств защиты информации на действующих автоматизированных системах и отдельных средствах вычислительной техники, контролирует работоспособность и эффективность функционирования этих средств;

- распределяет между пользователями средств вычислительной техники необходимые реквизиты криптографической защиты (пароли, ключи защиты и т.п.), формирует и распределяет между пользователями необходимые реквизиты защиты от НСД (в зависимости от системы защиты);

- проводит контроль целостности СЗИ, программного обеспечения с целью выявления несанкционированных изменений в них;

- контролирует проведение пользователями резервного копирования (архивирования) конфиденциальной информации, соблюдение мер специальной защиты при эксплуатации СВТ;

- не допускает подключения к локальной сети или к СВТ нештатных блоков и устройств, не прошедших специальные исследования, не имеющих предписания на эксплуатацию;

- проводит периодический контроль СВТ, подключенных к ЗЛВС, на предмет исключения несанкционированного изменения в составе, конструкции, конфигурации, размещении СВТ, а также в составе программного обеспечения;

- осуществляет контроль прав доступа сотрудников государственного органа к информационным ресурсам локальной вычислительной сети;

- осуществляет контроль разграничения прав доступа к защищаемой информации на несъемных носителях информации рабочих мест пользователей;

- регулярно анализирует содержимое системных журналов, проводит работы по выявлению возможных каналов утечки секретных сведений за счет несанкционированных доступов к информации и техническим средствам ВТ, ведет их учет;

- осуществляет контроль соблюдения требований по безопасности информации при использовании машинных носителей информации;

- разрабатывает и вводит установленным порядком необходимую учетную и объектовую документацию (журнал учета идентификаторов, инструкции пользователям и т.д.);

- определяет порядок и осуществляет контроль ремонта сертифицированных средств вычислительной техники;

- об имеющихся недостатках и выявленных нарушениях требований нормативных и руководящих документов по защите информации, а также в случае выявления попыток неправомерного доступа к охраняемым сведениям или попыток хищения, копирования, изменения сообщает заведующей ДОУ и незамедлительно принимает меры пресечения нарушений.

программист ДОУ имеет право:

- требовать от пользователей автоматизированных систем безусловного соблюдения установленной технологии обработки электронных документов и выполнения требований по информационной безопасности.

5.4. Пользователи объекта ВТ обязаны:

- строго соблюдать меры по защите информации и правила эксплуатации СВТ;

- обеспечивать сохранность комплекта ПЭВМ, машинных носителей информации и целостность установленного программного обеспечения;

- знать и соблюдать установленные требования по учету, хранению и пересылке машинных, бумажных и иных носителей информации;

- применять антивирусные программы при включении СВТ или при использовании гибких магнитных носителей информации;

- по окончании обработки конфиденциальной информации «обнулить» оперативную память компьютера путем перезагрузки или временного выключения ПЭВМ;

- перед началом обработки убедиться в работе средств защиты информации (генераторы шума и т.д.).

5.5. Администратор и пользователи АС ДОУ:

- лично отвечают за защиту информации, сохранность машинных и иных носителей информации;

- участвуют в определении правил разграничения доступа к информации в системах и средствах информатизации, используемых в ДОУ.

6. Планирование работ по защите конфиденциальной информации

6.1. Планирование работ по защите информации проводится на основании:

- рекомендаций актов проверок контрольными органами ФСТЭК России;

- результатов анализа деятельности в области защиты информации;

- рекомендаций и указаний ФСТЭК России;

- решений республиканской (районной) комиссии по информационной безопасности;

- рекомендаций актов проверок управления информационной безопасности Правительства Карачаево-Черкесской Республики.

7. Контроль состояния защиты конфиденциальной информации

7.1. С целью своевременного выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособность систем информатизации, осуществляется контроль состояния и эффективности защиты информации.

7.2. Контроль заключается в проверке по действующим методикам выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер.

7.3. Повседневный контроль выполнения организационных и технических мероприятий, направленных на обеспечение защиты информации.

7.4. Периодический контроль может осуществляться представителями ФСТЭК России, территориальных органов ФСБ России, Управления информационной безопасности Правительства Карачаево-Черкесской Республики.

7.5. Допуск представителей этих органов для проведения контроля состояния защиты информации осуществляется в установленном порядке по предъявлению служебных удостоверений и предписаний на право проверки, подписанных руководителем (заместителем) соответствующего органа.

7.6. К контролю эффективности мероприятий по защите информации могут привлекаться работники ДОУ.

7.7. Результаты проверок отражаются в техническом паспорте объекта информатизации.

7.8. Периодичность проверок объектов информатизации, где обрабатывается (обсуждается) конфиденциальная информация - 1 раз в год и при каждом изменении состава и расположения основных технических средств и систем.

7.9. Специалист, ответственный по защите информации, обязан присутствовать при всех проверках ДОУ по вопросам защиты информации.

7.10. По результатам проверок контролирующими органами ответственный по вопроасм безопасности в ДОУ с привлечением других заинтересованных специалистов в десятидневный срок разрабатывает план устранения выявленных недостатков.

7.11. Защита информации считается эффективной, если принимаемые меры соответствуют установленным требованиям и нормам.

Несоответствие мер установленным требованиям или нормам по защите информации является нарушением.

7.12. При обнаружении нарушений заведующая обязана принять необходимые меры по их устранению в сроки, согласованные с органом или лицом, проводившим проверку.

Ответственный за безопасность
в МБДОУ «Детский сад «Сказка»
ст.Зеленчукской» О.И.Попова

Приложение №2
к приказу заведующей МБДОУ
от 25.02.2015 №28а

«Утверждаю» .
Заведующая МБДОУ
«Детский сад «Сказка»
Т.А.Терентьева .

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ
лица, ответственного за информационную безопасность

1.Общие положения

1.1. Настоящее Положение определяет задачи, функции, обязанности, ответственность и права ответственного за работу в сети Интернет и за информационную безопасность (далее «ответственный за информационную безопасность»).
1.2.Ответственный за информационную безопасность назначается приказом заведующей, образовательного учреждения из числа сотрудников.
1.3. Ответственный за информационную безопасность подчиняется заведующей образовательного учреждения.
1.4. Ответственный за информационную безопасность в своей работе руководствуется настоящим Положением.
1.5. Ответственный за информационную безопасность в пределах своих функциональных обязанностей обеспечивает безопасность информации получаемой из сети Интернет и хранимой при помощи средств вычислительной техники в образовательном учреждении.
1.6. Ответственный за информационную безопасность в своей деятельности руководствуется Конституцией Российской Федерации, законом «Об образовании» Российской Федерации, решениями Правительства Российской Федерации, Уставом и другими локальными правовыми актами МБДОУ, правилами техники безопасности и противопожарной защиты.

3. Должностные обязанности

2.1.Ответственный за информационную безопасность:
- планирует использование ресурсов сети Интернет в образовательном учреждении на основании заявок педагогических и других работников образовательного учреждения;
- разрабатывает, согласует с педагогическим коллективом, представляет на педагогическом совете образовательного учреждения регламент использования сети Интернет в ДОУ включая регламент определения доступа к ресурсам сети Интернет;
- обеспечивает функционирование и поддерживает работоспособность средств и систем защиты информации в пределах, возложенных на него обязанностей;
- организует получение сотрудниками образовательного учреждения электронных адресов и паролей для работы в сети Интернет и информационной среде ДОУ;
- организует контроль за использованием сети Интернет в образовательном учреждении;
- организует контроль за работой оборудования и программных средств, обеспечивающих использование сети Интернет и ограничение доступа;
- проводит обучение персонала и пользователей вычислительной техники правилам безопасной обработки информации и правилам работы со средствами защиты информации;
- устанавливает по согласованию с заведующей критерии доступа пользователей.
- проводит текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических средств защиты информации;
- обеспечивает контроль целостности эксплуатируемого на средствах вычислительной техники программного обеспечения с целью выявления несанкционированных изменений в нём;

- организует контроль за санкционированным изменением ПО, заменой и ремонтом средств вычислительной техники;
- немедленно докладывает заведующей о выявленных нарушениях и несанкционированных действиях пользователей и сотрудников, а также принимает необходимые меры по устранению нарушений;
- систематически повышает свою профессиональную квалификацию, предметную компетентность, включая ИКТ-компетентность;
- обеспечивает информирование организаций, отвечающих за работу технических и программных средств, об ошибках в работе оборудования и программного обеспечения;
- соблюдает правила и нормы охраны труда, техники безопасности и противопожарной защиты, правила использования сети Интернет.

3. Должен знать

- дидактические возможности использования ресурсов сети Интернет;
- правила безопасного использования сети Интернет.

4. Права

Ответственный за информационную безопасность имеет право:
4.1.Определять ресурсы сети Интернет, используемые в учебном процессе на основе запросов педагогов и по согласованию с руководителем образовательного учреждения.
4.2. Требовать от сотрудников и пользователей компьютерной техники безусловного соблюдения установленной технологии и выполнения инструкций по обеспечению безопасности и защиты информации, содержащей сведения ограниченного распространения и электронных платежей.
4.3. Готовить предложения по совершенствованию используемых систем защиты информации и отдельных их компонентов.

5. Ответственность

Ответственный за информационную безопасность несет ответственность
5.1. За выполнение правил использования Интернета и ограничения доступа, установленного в образовательном учреждении;
5.2. За качество проводимых им работ по обеспечению защиты информации в соответствии с функциональными обязанностями, определенными настоящем Положением.

С инструкцией ознакомлена Попова
зав. МБДОУ д/с "Сказка"
с. Зеленчукское
Мария Терентьевна