**Согласовано:**

Председатель ПК

Кругликова Ю.А.

«09» 01 2018г

**Утверждаю:**

Заведующий МАДОУ

Андреева Т.П.

«09» 01 2018г

# ПОЛОЖЕНИЕ

**« О защите персональных данных»**

**Муниципального автономного дошкольного**

**образовательного учреждения.**

**«Детский сад №14 «Вишенка»**

**г.Прокопьевск**

2018г

**Положение о защите персональных данных**

1. Общие положения

1.1. Настоящее Положение об обработке и защите персональных данных в дошкольном образовательном учреждении (далее - Положение) регулирует порядок получения, обработки, использования, хранения и обеспечения конфиденциальности персональных данных в автономном дошкольном образовательном учреждении «Детский сад № 14 «Вишенка» (далее - МАДОУ) на основании Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" (далее - Закон № 152-ФЗ), Федерального закона от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации", постановления Правительства РФ от 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", а также в соответствии с уставом МАДОУ и локальными актами.
1.2. Целью данного Положения является защита персональных данных сотрудников, воспитанников и их родителей (законных представителей) от несанкционированного доступа, неправомерного их использования или утраты.
1.3. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.
1.4. Настоящее Положение утверждается и вводится в действие приказом заведующего и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным сотрудников, воспитанников и их родителей (законных представителей).

2. Понятие и состав персональных данных

2.1. Персональные данные сотрудников, воспитанников и их родителей (законных представителей) – информация, необходимая работодателю в связи с трудовыми отношениями и касающиеся конкретного работника. Под информацией о сотрудниках, воспитанников и их родителей (законных представителей) понимаются сведения о фактах, событиях и обстоятельствах жизни работника, воспитанника, родителя (законного представителя) позволяющие идентифицировать его личность.
2.2. В состав персональных данных работников входят документы, содержащие информацию о паспортных данных, образовании, отношении к воинской обязанности, семейном положении, месте жительства, состоянии здоровья, а также о предыдущих местах их работы.
2.3. Комплекс документов, сопровождающий процесс оформления трудовых отношений работника при его приеме, переводе и увольнении.
2.3.1. Информация, представляемая работником при поступлении на работу должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:
– паспорт или иной документ, удостоверяющий личность;
– трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства, либо трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;
– страховое свидетельство государственного пенсионного страхования;
– документы воинского учета — для военнообязанных и лиц, подлежащих воинскому учету;
– документ об образовании, о квалификации или наличии специальных знаний — при поступлении на работу, требующую специальных знаний или специальной подготовки;
– свидетельство о присвоении ИНН (при его наличии у работника).

2.3.2. При оформлении работника в МАДОУ, заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные работника:
– общие сведения (Ф.И.О. работника, дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);
– сведения о воинском учете;
– данные о приеме на работу;
В дальнейшем в личную карточку вносятся:
– сведения о переводах на другую работу;
– сведения об аттестации;
– сведения о повышении квалификации;
– сведения о профессиональной переподготовке;
– сведения о наградах (поощрениях), почетных званиях;
– сведения об отпусках;
– сведения о социальных гарантиях;
– сведения о месте жительства и контактных телефонах.
2.3.3. В МАДОУ создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:
2.3.3.1. Документы, содержащие персональные данные работников (комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекс материалов по анкетированию, тестированию; проведению собеседований с кандидатом на должность; подлинники и копии приказов по личному составу; личные дела и трудовые книжки работников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации работников; служебных расследований; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству, руководителям структурных подразделений; копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения).
2.4. Данные документы являются конфиденциальными.

## 3. Обработка персональных данных

3.1. Под обработкой персональных данных понимается получение, хранение, комбинирование, передача или любое другое использование персональных данных сотрудников, воспитанников и их родителей (законных представителей).
3.2. В целях обеспечения прав и свобод человека и гражданина руководитель и его представители при обработке персональных данных сотрудников, воспитанников и их родителей (законных представителей) обязаны соблюдать следующие общие требования:
3.2.1. Обработка персональных данных сотрудников, воспитанников и их родителей (законных представителей) может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.
3.2.2. При определении объема и содержания, обрабатываемых персональных, данных сотрудников, воспитанников и их родителей (законных представителей) руководитель должен руководствоваться Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами.
3.2.3. Получение персональных данных осуществляется путем представления их сотрудниками, и родителями (законных представителями) воспитанников.
3.2.4. Персональные данные следует получать у них самих. Если персональные данные сотрудников, воспитанников и их родителей (законных представителей) возможно, получить только у третьей стороны, то они должен быть уведомлен об этом заранее и от

них должно быть получено письменное согласие. Работодатель должен сообщить о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.
3.2.5. Заведующий учреждения и лица, ответственные за защиту персональных данных не имеют права получать и обрабатывать персональные данные сотрудников, воспитанников и их родителей (законных представителей) об их политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений данные о частной жизни (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) могут быть получены и обработаны только с его письменного согласия.
3.2.6.Заведующий не имеет право получать и обрабатывать персональные данные сотрудников, воспитанников и их родителей (законных представителей) об их членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.
3.3. К обработке, передаче и хранению персональных данных работника могут иметь доступ сотрудники бухгалтерии; делопроизводитель; оператор.
3.4. Использование персональных данных возможно только в соответствии с целями, определившими их получение.
3.4.1. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.
3.5. Передача персональных данных сотрудников, воспитанников и их родителей (законных представителей) возможна только с их согласия или в случаях, прямо предусмотренных законодательством.
3.5.1. При передаче персональных данных сотрудников, воспитанников и их родителей (законных представителей) ответственные должны соблюдать следующие требования: не сообщать персональные данные третьей стороне без письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом; предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами; разрешать доступ к персональным данным работников только специально уполномоченным лицам, определенным приказом по организации, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций; не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции; передавать персональные данные работника представителям работников в порядке, установленном Трудовым Кодексом, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.
3.5.2. Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.
3.5.3. При передаче персональных данных за пределы организации руководитель не должен сообщать эти данные третьей стороне без письменного согласия сотрудников, родителей (законных представителей) воспитанников, за исключением случаев, когда это

необходимо в целях предупреждения угрозы жизни и здоровью или в случаях, установленных федеральным законом.
3.6. Все меры конфиденциальности при сборе, обработке и хранении персональных данных сотрудников, воспитанников и их родителей (законных представителей) распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

## 4. Доступ к персональным данным

4.1. Внутренний доступ (доступ внутри организации).
4.1.1. Право доступа к персональным данным имеют: заведующий дошкольным учреждением, сотрудники бухгалтерии, делопроизводитель, сам работник, носитель данных, другие сотрудники организации при выполнении ими своих служебных обязанностей.
4.1.2. Перечень лиц, имеющих доступ к персональным данным работников, определяется приказом директора организации.
4.2. Внешний доступ.
4.2.1. К числу массовых потребителей персональных данных вне организации можно отнести государственные функциональные структуры: налоговые инспекции, правоохранительные органы, органы статистики, военкоматы, органы социального страхования, пенсионные фонды, подразделения муниципальных органов управления.
4.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.
4.2.3. Организации, в которые сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.
4.2.4. Другие организации. Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника. Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника.

## 5. Угроза утраты персональных данных

5.1 Защита персональных данных представляет собой предупреждение нарушения доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечение безопасности информации в процессе управленческой и производственной деятельности организации.
5.2. Защита персональных данных сотрудников, воспитанников и их родителей (законных представителей) от неправомерного их использования или утраты должна быть обеспечена руководителем организации за счет его средств и в порядке, установленном федеральным законом.

## 6. Права и обязанности работника

6.1. Закрепление прав сотрудников, воспитанников и их родителей (законных представителей), регламентирующих защиту их персональных данных, обеспечивает сохранность полной и точной информации о них.
6.2. Работники и их представители должны быть ознакомлены под расписку с документами организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.
6.3. Сотрудники и родители (законные представители) воспитанников ставят руководителя в известность об изменении фамилии, имени, отчества, даты рождения, что

получает отражение в персональных данных на основании представленных документов. При необходимости в документах работников изменяются данные об образовании, профессии, специальности, присвоении нового разряда и пр.

## 7. Заключительные положения

7.1.Изменения в Положение вносятся согласно установленному в МАДОУ порядку. Право ходатайствовать о внесении изменений в Положение имеет заведующий и его заместители.

Согласованно:
Председатель ПК
Назарова М.В. _____
«____»_____2013г

Утверждаю:
И.о. заведующего МАДОУ
Унгурова Е.А._____
«____»_____2013г

**ПОЛОЖЕНИЕ**

**о порядке обработки и защите персональных данных**

**в муниципальном автономном**

**дошкольном образовательном учреждении**

**«Детский сад № 14 «Вишенка»**

г. Прокопьевск, 2013г.

Согласованно:
Председатель ПК
Назарова М.В. _____
«____»_____2013г.

Утверждаю:
Заведующая МДОУ
Федорова Н.Г. _____
«____»_____2013 г.

Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные

**1. Общие положения**

1.1. Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные (далее – Инструкция), является обязательной для муниципального автономного дошкольного образовательного учреждения «Детский сад №14 «Вишенка» (далее – МАДОУ).

1.2. Под персональными данными понимается любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в т. ч. его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное и имущественное положение, образование, профессия, доходы и др.

1.3. Обеспечение конфиденциальности персональных данных не требуется в случае обезличивания персональных данных, а также в отношении общедоступных персональных данных.

В общедоступные источники персональных данных (в т. ч. справочники, адресные книги) в целях информационного обеспечения с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес и другие сведения.

1.4. Конфиденциальность персональных данных предусматривает обязательное получение согласия субъекта персональных данных (наличие иного законного основания) на их обработку.

Согласие не требуется на обработку данных:

- необходимых для доставки почтовых отправлений организациями почтовой связи;
- включающих в себя только фамилию, имя и отчество субъекта;
- данных, работа с которыми проводится в целях исполнения обращения (запроса) субъекта персональных данных, трудового или иного договора с ним, однократного пропуска в здание или в иных аналогичных целях;
- обработка которых осуществляется без средств автоматизации.

1.5. Порядок ведения перечней персональных данных в МАДОУ утверждается локальным актом. Осуществлять обработку и хранение конфиденциальных данных, не внесенных в перечень, запрещается.

1.6. Все работники, постоянно работающие в помещениях, в которых ведется обработка персональных данных, должны иметь допуск (разрешение) к работе с соответствующими видами персональных данных.

1.7. Работникам, осуществляющим обработку персональных данных, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью, а также оставлять материальные носители с персональными данными без присмотра в незапертом помещении. После подготовки и передачи документа в соответствии с резолюцией файлы черновиков и вариантов документа должны переноситься подготовившим их работником на маркированные носители, предназначенные для хранения персональных данных. Без согласования с руководителем структурного подразделения формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих конфиденциальные данные, запрещается.

1.8. Передача персональных данных допускается только в случаях, установленных Федеральными законами от 27.07.2006 № 152-ФЗ "О персональных данных" и от 02.05.2006 № 59-ФЗ "О порядке рассмотрения обращений граждан Российской Федерации", действующими инструкциями по работе со служебными документами и обращениями граждан, а также по письменному поручению (резолюции) вышестоящих должностных лиц.

1.9. Запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством РФ и действующими инструкциями по работе со служебными документами и обращениями граждан. Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать конфиденциальные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

1.10. Ответственность за защиту обрабатываемых персональных данных возлагается на заведующего и на лицо имеющее доступ( согласно приказу) . Лица, виновные в нарушении норм, регулирующих обработку и хранение конфиденциальных данных, несут дисциплинарную, административную и уголовную ответственность в соответствии с законодательством и ведомственными нормативными актами.

**2. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемых без использования средств автоматизации**

2.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна быть организована таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения материальных носителей персональных данных и установить перечень лиц, осуществляющих обработку.

2.2. При хранении материальных носителей необходимо соблюдать условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах выполнения такой обработки.

2.3. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. При фиксации персональных данных на материальных носителях не допускается на одном материальном носителе размещать персональные данные, цели обработки которых заведомо не совместимы. Для обработки персональных данных каждой категории должен использоваться отдельный материальный носитель.

2.4. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, и невозможности обработки одних персональных данных

отдельно от других, зафиксированных на том же носителе, должны быть приняты меры по обеспечению раздельной обработки персональных данных, исключающие одновременное копирование иных персональных данных, не подлежащих распространению и использованию.

2.5. Уничтожение или обезличивание всех или части персональных данных (если это допускается материальным носителем) производится способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание). Уточнение персональных данных производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

**3. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемых с использованием средств автоматизации**

3.1. Безопасность персональных данных при их обработке в информационных системах, хранении и пересылке обеспечивается с помощью системы защиты персональных данных, включающей специальные средства защиты информации, а также используемые в информационной системе информационные технологии.

3.2. Допуск лиц к обработке персональных данных в информационных системах осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа.

3.3. Работа с информационными системами должна быть организована таким образом, чтобы обеспечить сохранность носителей персональных данных и средств защиты информации, а также исключить возможность неконтролируемого пребывания в помещениях, где они находятся, посторонних лиц.

3.4. Электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из шести и более символов.

3.5. Работа на компьютерах с персональными данными без паролей доступа или под чужими или общими (одинаковыми) паролями, а также пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в т. ч. сети Интернет, запрещается.

3.6. При обработке персональных данных в информационных системах пользователями должно быть обеспечено:

- использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;
- недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- недопущение несанкционированного выноса из помещений, установки и подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

3.7. При обработке персональных данных в информационных системах разработчики и администраторы систем должны обеспечивать:

- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
- учет лиц, допущенных к работе с персональными данными в информационных системах, прав и паролей доступа;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;
- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- описание системы защиты персональных данных.

3.8. Специфические требования к защите персональных данных в отдельных автоматизированных системах устанавливаются инструкциями по их использованию и эксплуатации.

3.9. Работники подразделений  МАДОУ и лица, выполняющие работы по договорам и контрактам, имеющие отношение к обработке персональных данных, должны быть ознакомлены с Инструкцией под расписку.

**Дата размещения: 06.05.2011**

# Инструкция пользователя, осуществляющего обработку персональных данных на объектах вычислительной техники

## 1. Общие положения

1.1. Инструкция пользователя, осуществляющего обработку персональных данных на объектах вычислительной техники (далее – Инструкция), регламентирует основные обязанности, права и ответственность пользователя, допущенного к автоматизированной обработке персональных данных и иной конфиденциальной информации на объектах вычислительной техники (ПЭВМ) дошкольного образовательного учреждения (далее – ДОУ).

1.2. Инструкция регламентирует деятельность пользователя, который имеет допуск к обработке соответствующих категорий персональных данных и обладает необходимыми навыками работы на ПЭВМ.

## 2. Обязанности пользователя

2.1. При выполнении работ в пределах своих функциональных обязанностей пользователь несет персональную ответственность за соблюдение требований нормативных документов по защите информации.

2.2. Пользователь обязан:

- выполнять требования Инструкции по обеспечению режима конфиденциальности проводимых работ;
- при работе с персональными данными исключать присутствие в помещении, где расположены средства вычислительной техники, не допущенных к обрабатываемой информации лиц, а также располагать во время работы экран видеомонитора так, чтобы отображаемая на нем информации была недоступна для просмотра посторонними лицами;
- соблюдать правила работы со средствами защиты информации, а также установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с персональными данными при ее обработке;
- после окончания обработки персональных данных в рамках выполнения одного задания, а также по окончании рабочего дня стирать остаточную информацию с жесткого диска ПЭВМ;
- оповещать обслуживающий ПЭВМ персонал, а также непосредственного руководителя обо всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в ПЭВМ;
- не допускать "загрязнения" ПЭВМ посторонними программными средствами;
- знать способы выявления нештатного поведения используемых операционных систем и пользовательских приложений, меры предотвращения ухудшения ситуации;
- знать и соблюдать правила поведения в экстренных ситуациях, порядок действий при ликвидации последствий аварий;
- помнить личные пароли и персональные идентификаторы;
- знать штатные режимы работы программного обеспечения, пути проникновения и распространения компьютерных вирусов;
- при применении внешних носителей информации перед началом работы проводить их проверку на наличие компьютерных вирусов.

2.3. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках
и т. п.) пользователь должен провести внеочередной антивирусный контроль своей рабочей станции. В случае обнаружения зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного руководителя, администратора системы, а также смежные подразделения, использующие эти файлы в работе;
- оценить необходимость дальнейшего использования файлов, зараженных вирусом;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта следует привлечь администратора системы).

2.4. Пользователю ПЭВМ запрещается:

- записывать и хранить персональные данные на неучтенных в установленном порядке машинных носителях информации;
- удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности;
- самостоятельно подключать к ПЭВМ какие-либо устройства, а также вносить изменения в состав, конфигурацию и размещение ПЭВМ;

- самостоятельно устанавливать и/или запускать на ПЭВМ любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей;
- осуществлять обработку персональных данных в условиях, позволяющих просматривать их лицам, не имеющим к ним допуска, а также нарушающих требования к эксплуатации ПЭВМ;
- сообщать кому-либо устно или письменно личные атрибуты доступа к ресурсам ПЭВМ;
- отключать (блокировать) средства защиты информации;
- производить какие-либо изменения в подключении и размещении технических средств;
- производить иные действия, ограничения на исполнение которых предусмотрены утвержденными регламентами и инструкциями;
- бесконтрольно оставлять ПЭВМ с загруженными персональными данными, установленными маркированными носителями, электронными ключами и выведенными на печать документами, содержащими персональные данные.

**3. Права пользователя**

Пользователь ПЭВМ имеет право:

- обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленных ему полномочий;
- обращаться к обслуживающему ПЭВМ персоналу с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, установленным в ПЭВМ, а также со средствами защиты информации.

**4. Заключительные положения**

4.1. Особенности обработки персональных данных пользователями отдельных автоматизированных систем могут регулироваться дополнительными инструкциями.

4.2. Работники подразделений ДОУ и лица, выполняющие работы по договорам и контрактам и имеющие отношение к обработке персональных данных на объектах вычислительной техники, должны быть ознакомлены с Инструкцией под расписку.

**Дата размещения: 06.05.2011**

Инструкция по проведению мониторинга информационной безопасности и антивирусного контроля

1. Инструкция по проведению мониторинга информационной безопасности и антивирусного контроля (далее – Инструкция) регламентирует порядок планирования и проведения мероприятий, направленных на обеспечение безопасности автоматизированных систем, обрабатывающих персональные данные, от несанкционированного доступа, распространения, искажения и утраты информации, необходимой в работе дошкольного образовательного учреждения (далее – ДОУ).

2. Мониторинг работоспособности аппаратных компонентов автоматизированных систем, обрабатывающих персональные данные, осуществляется в процессе их администрирования и при проведении работ по техническому обслуживанию оборудования. Наиболее существенные компоненты системы, имеющие встроенные средства контроля работоспособности (серверы, активное сетевое оборудование), должны постоянно контролироваться в рамках работы администраторов соответствующих систем.

3. Мониторинг парольной защиты предусматривает:

- контроль соблюдения сроков действия паролей (не более трех месяцев);
- периодическую (не реже одного раза в месяц) проверку пользовательских паролей на количество символов и очевидность с целью выявления слабых паролей, которые легко угадать или дешифровать с помощью специализированных программных средств ("взломщиков" паролей).

4. Мониторинг целостности программного обеспечения включает:

- проверку контрольных сумм и цифровых подписей каталогов и файлов сертифицированных программных средств при загрузке операционной системы;
- сверку дубликатов идентификаторов пользователей;
- проверку и восстановление системных файлов администраторами систем с резервных копий при несовпадении контрольных сумм.

5. Мероприятия, направленные на предупреждение и своевременное выявление попыток несанкционированного доступа, в т. ч. выявление фактов сканирования определенного диапазона сетевых портов в короткие промежутки

времени с целью обнаружения сетевых анализаторов, изучающих систему и определяющих места ее уязвимости, осуществляются с использованием средств операционной системы и специальных программных средств. Они должны сопровождаться фиксацией неудачных попыток входа в систему в системном журнале и протоколированием работы сетевых сервисов.

6. Мониторинг производительности автоматизированных систем, обрабатывающих персональные данные, осуществляется по обращениям пользователей в ходе администрирования систем и проведения профилактических работ для выявления попыток несанкционированного доступа, повлекших существенное уменьшение производительности.

7. Системный аудит производится ежеквартально и в особых ситуациях. Он включает в себя проведение обзоров безопасности, тестирование системы и контроль внесения изменений в системное программное обеспечение.

8. Обзоры безопасности проводятся с целью проверки соответствия текущего состояния систем, обрабатывающих персональные данные, уровню безопасности, удовлетворяющему требованиям политики безопасности, и включают:

- составление отчетов о безопасности пользовательских ресурсов (в т. ч. о наличии повторяющихся пользовательских имен и идентификаторов, неправильных форматах регистрационных записей, пользователях без пароля, неправильной установке домашних каталогов пользователей и уязвимостях пользовательских окружений);
- проверку содержимого файлов конфигурации на соответствие списку для проверки;
- анализ данных об обнаружении изменений системных файлов со времени проведения последней проверки (контроль целостности системных файлов);
- проверку прав доступа и других атрибутов системных файлов (команд, утилит и таблиц);
- оценку правильности настройки механизмов аутентификации и авторизации сетевых сервисов;
- проверку корректности конфигурации системных и активных сетевых устройств (мостов, маршрутизаторов, концентраторов и сетевых экранов).

9. Активное тестирование надежности механизмов контроля доступа производится путем осуществления попыток проникновения в информационную систему с помощью автоматического инструментария или вручную.

10. Пассивное тестирование механизмов контроля доступа осуществляется путем анализа конфигурационных файлов системы. Сначала информация об известных уязвимостях извлекается из документации и внешних источников, затем осуществляется проверка конфигурации системы с целью выявления опасных состояний системы, т. е. таких состояний, в которых могут проявлять себя известные уязвимости. Если система находится в опасном состоянии, то с целью нейтрализации уязвимостей необходимо выполнить одно из следующих действий:

- изменить конфигурацию системы (для ликвидации условий проявления уязвимости);
- установить программные коррекции либо другие версии программ, в которых данная уязвимость отсутствует;
- отказаться от использования системного сервиса, содержащего данную уязвимость.

11. Внесение изменений в системное программное обеспечение осуществляется администраторами систем, обрабатывающих персональные данные, с обязательным соблюдением следующих условий:

- документирование изменений в соответствующем журнале;
- уведомление работника, которого касается изменение;
- анализ претензий, в случае если это изменение причинило кому-нибудь вред;
- разработка планов действий в аварийных ситуациях для восстановления работоспособности системы, если внесенное в нее изменение вывело ее из строя.

12. Для защиты от вредоносных программ и вирусов необходимо использовать только лицензионные или сертифицированные свободно распространяемые антивирусные средства.

13. Для защиты серверов и рабочих станций используются:

- резидентные антивирусные мониторы, контролирующие подозрительные действия программ;
- утилиты для обнаружения и анализа новых вирусов.

14. При подозрении на наличие не выявленных установленными средствами защиты заражений следует использовать Live CD с другими антивирусными средствами.

15. Установка и настройка средств защиты от вредоносных программ и вирусов на рабочих станциях и серверах автоматизированных систем, обрабатывающих персональные данные, осуществляется администраторами соответствующих систем в соответствии с руководствами по установке приобретенных средств защиты.

16. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено администратором системы на отсутствие вредоносных программ и компьютерных вирусов. После установки (изменения) программного обеспечения рабочей станции необходимо провести антивирусную проверку.

17. Запуск антивирусных программ осуществляется автоматически по заданию, созданному с использованием планировщика задач, входящего в поставку операционной системы либо поставляемого вместе с антивирусными программами.

18. Антивирусный контроль рабочих станций проводится ежедневно в автоматическом режиме. Если проверка всех файлов на дисках рабочих станций занимает неприемлемо большое время, то допускается проводить выборочную проверку загрузочных областей дисков, оперативной памяти, критически важных инсталлированных файлов операционной системы и загружаемых файлов по сети или с внешних носителей. В этом случае полная проверка осуществляется не реже одного раза в неделю в период неактивности пользователя. Пользователям рекомендуется проводить полную проверку во время перерыва на обед путем перевода рабочей станции в соответствующий автоматический режим функционирования
в запертом помещении.

19. Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, текстовые файлы любых форматов, файлы данных), получаемая пользователем по сети или загружаемая со съемных носителей (магнитных дисков, оптических дисков, флэш-накопителей и т. п.). Контроль информации проводится антивирусными средствами в процессе или сразу после ее загрузки на рабочую станцию пользователя. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

20. Устанавливаемое на серверы программное обеспечение предварительно проверяется администратором системы на отсутствие компьютерных вирусов и вредоносных программ. Непосредственно после установки (изменения) программного обеспечения сервера должна быть выполнена антивирусная проверка.

21. На серверах систем, обрабатывающих персональные данные, необходимо применять специальное антивирусное программное обеспечение, позволяющее:

- осуществлять антивирусную проверку файлов в момент попытки записи файла на сервер;
- проверять каталоги и файлы по расписанию с учетом нагрузки на сервер.

22. На серверах электронной почты необходимо применять антивирусное программное обеспечение, позволяющее осуществлять проверку всех входящих сообщений. В случае если проверка входящего сообщения на почтовом сервере показала наличие в нем вируса или вредоносного кода, отправка данного сообщения блокируется. При этом должно осуществляться автоматическое оповещение администратора почтового сервера, отправителя сообщения и адресата.

23. Антивирусные базы на всех рабочих станциях и серверах необходимо регулярно обновлять.

24. Администратор системы должен проводить регулярные проверки протоколов работы антивирусных программ с целью выявления пользователей и каналов, через которых распространяются вирусы. При обнаружении зараженных вирусом файлов администратору необходимо выполнить следующие действия:

- отключить от компьютерной сети рабочие станции, представляющие вирусную опасность, до полного выяснения каналов проникновения вирусов и их уничтожения;
- немедленно сообщить о факте обнаружения вирусов непосредственному начальнику, в т. ч. указать предположительный источник (отправитель, владелец и т. д.) зараженного файла, тип зараженного файла, тип вируса, а также рассказать о характере содержащейся в файле информации и выполненных антивирусных мероприятиях.

25. Если администратор системы, обрабатывающей персональные данные, подозревает или получил сообщение о том, что его система подвергается атаке или уже была скомпрометирована, он должен определить системные ресурсы, безопасность которых была нарушена, и установить:

- была ли попытка несанкционированного доступа (далее – НСД);
- когда, как и при каких обстоятельствах была предпринята попытка НСД;
- продолжается ли НСД в настоящий момент;
- кто является источником НСД;
- что является объектом НСД;
- какова была мотивация нарушителя;
- точку входа нарушителя в систему;
- была ли попытка НСД успешной.

26. Для выявления попытки НСД необходимо:

- установить, какие пользователи в настоящее время работают в системе и на каких рабочих станциях;
- выявить подозрительную активность пользователей, проверить, все ли пользователи вошли в систему со своих рабочих мест и не работает ли кто из них в системе необычно долго;
- убедиться, что никто из пользователей не использует подозрительные программы или программы, не относящиеся к его области деятельности.

27. При анализе системных журналов администратор должен:

проверить наличие подозрительных записей в системных журналах, сделанных в период предполагаемой попытки НСД, включая вход в систему пользователей, которые должны были отсутствовать в этот период времени, а также входы в систему из неожиданных мест, в необычное время и на короткий период времени;

- убедиться в том, что системный журнал не уничтожен и в нем отсутствуют пробелы;
- просмотреть списки команд, выполненных пользователями в рассматриваемый период времени;
- проверить наличие исходящих сообщений электронной почты, адресованных подозрительным хостам;
- проверить журналы на наличие мест, которые выглядят необычно;
- выявить неудачные попытки входа в систему.

28. В ходе анализа журналов активного сетевого оборудования (мостов, переключателей, маршрутизаторов, шлюзов) следует проверить:

- нет ли в них подозрительных записей, сделанных в период предполагаемой попытки НСД;
- есть ли в них пробелы, а также места, которые выглядят необычно;
- были ли попытки изменения таблиц маршрутизации и адресных таблиц.

Кроме того, необходимо проверить конфигурацию сетевых устройств с целью определения возможности нахождения в системе программы, просматривающей весь сетевой трафик.

29. Для обнаружения в системе следов, оставленных злоумышленником в виде файлов, вирусов, троянских программ, изменения системной конфигурации следует:

- составить базовую схему того, как обычно выглядит система;
- провести поиск подозрительных файлов, скрытых файлов, имен файлов и каталогов, которые обычно используются злоумышленниками;
- проверить содержимое системных файлов, которые обычно изменяются злоумышленниками;
- оценить целостность системных программ;
- проверить систему аутентификации и авторизации.

30. Особенности мониторинга информационной безопасности персональных данных в отдельных автоматизированных системах могут регулироваться дополнительными инструкциями.

31. Работники подразделений ДОУ и лица, выполняющие работы по договорам и контрактам, имеющие отношение к проведению мониторинга информационной безопасности и антивирусного контроля при обработке персональных данных, должны быть ознакомлены с Инструкцией под расписку.

**Дата размещения: 06.05.2011**