

ОБЩЕОБРАЗОВАТЕЛЬНОЕ ЧАСТНОЕ УЧРЕЖДЕНИЕ
СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА «ПОТЕНЦИАЛ» Г. МОСКВЫ

Приказ

от 07.06.2016 г.

№ 47

***О выполнении работ по защите конфиденциальной информации
в ОЧУ СОШ «Потенциал»***

В соответствии с Федеральным законом № 149-ФЗ от 27 июля 2006 года «Об информации, информационных технологиях и о защите информации», Федеральным законом № 152-ФЗ от 27 июля 2006 года «О персональных данных», Постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и другими нормативными правовыми актами, в целях определения перечня персональных данных и общего порядка обращения с информацией, содержащей персональные данные, в ЧУ СОШ «Потенциал» ПРИКАЗЫВАЮ:

1. Утвердить «Положение о защите, хранении, обработке и передаче персональных данных работников ОЧУ СОШ «Потенциал» г. Москвы» (Приложение № 1).
2. Утвердить «Положение о защите, хранении, обработке и передаче персональных данных обучающихся ОЧУ СОШ «Потенциал» г. Москвы» (Приложение № 2).

3. Утвердить «Инструкция по организации парольной защиты в ОЧУ СОШ «Потенциал» г. Москвы» (Приложение № 3).
4. Утвердить «Инструкция по организации антивирусной защиты в ОЧУ СОШ «Потенциал» г. Москвы» (Приложение № 4).
5. Ввести положения и инструкции для работы в школе со дня подписания.
6. Контроль за исполнением приказа осуществляет директор ОЧУ СОШ «Потенциал» Гущина Г.В.

Директор школы

Гущина Г. В.

УТВЕРЖДЕНО
Приказом директора
ОЧУ СОШ «Потенциал»
г. Москвы
от 07.06.2016 г. № 47

_____ Г.В. Гущина

**Положение о защите, хранении, обработке и передаче
персональных данных работников
ОЧУ СОШ «Потенциал» г. Москвы.**

Настоящее Положение разработано на основании Конституции Российской Федерации, Федерального закона от 19.12.2005 №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных», Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», Трудового кодекса Российской Федерации, Федерального закона от 27.07.2006 №149-ФЗ "Об информации, информационных технологиях и о защите информации», постановления Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и призвано обеспечить права и свободу участников образовательного процесса при обработке их персональных данных.

1. Общие положения

1.1. Персональные данные Работника - сведения о фактах, событиях и

обстоятельствах жизни Работника, позволяющие идентифицировать его личность, необходимые администрации в связи с трудовыми отношениями с Работником и касающиеся Работника.

К персональным данным Работника относятся:

- сведения, содержащиеся в паспорте или ином документе, удостоверяющем личность;
- информация, содержащаяся в трудовой книжке Работника;
- информация, содержащаяся в страховом свидетельстве государственного пенсионного страхования;
- сведения, содержащиеся в документах воинского учета (при их наличии);
- информация об образовании, квалификации или наличии специальных знаний или подготовки;
- информация о состоянии здоровья Работника (сведения об инвалидности и т.п.);
- ИНН;
- СНИЛС;
- справка об отсутствии судимости;
- документы, содержащие сведения, необходимые для предоставления Работнику гарантий и компенсаций, установленных действующим законодательством (о составе семьи; о состоянии здоровья детей; документы, подтверждающие дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством; донорстве; нахождении в зоне воздействия радиации в связи с аварией на Чернобыльской АЭС и т. п.; о возрасте малолетних детей).

1.2. Все персональные данные о Работнике администрация может получить только от него самого. Работник принимает решение о

предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе. Согласие оформляется в письменной форме в двух экземплярах, один из которых предоставляется субъекту персональных данных, второй хранится у оператора персональных данных в течение срока, указанного в Согласии. В случаях, когда администрация может получить необходимые персональные данные Работника только у третьего лица, она должна уведомить об этом Работника заранее и получить от него письменное согласие.

Администрация обязана сообщить Работнику о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа Работника дать письменное согласие на их получение.

Персональные данные Работника являются конфиденциальной информацией и не могут быть использованы администрацией или любым иным лицом в личных целях.

При определении объема и содержания персональных данных Работника администрация руководствуется Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, иными федеральными законами и настоящим Положением.

2. Хранение, обработка и передача персональных данных Работника

2.1. Обработка персональных данных Работника осуществляется для обеспечения соблюдения законов и иных нормативных правовых актов в целях содействия Работнику в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности Работника,

контроля качества и количества выполняемой работы, оплаты труда, обеспечения сохранности имущества, пользования льготами, предусмотренными законодательством Российской Федерации и актами администрации.

Право доступа к персональным данным Работника имеют:

- работники Департамента (Комитета, отдела) образования при наличии соответствующих полномочий, установленных приказа Департамента (Комитета, отдела) образования;
- директор, заместитель директора по учебно - воспитательной работе образовательного учреждения;
- документовед руководителя образовательного учреждения;
- экономист;
- врач/медработник (по согласованию).

2.2. Директор, заместитель директора, документовед образовательного учреждения могут передавать персональные данные Работника третьим лицам, только если это необходимо в целях предупреждения угрозы жизни и здоровья Работника, а также в случаях, установленных федеральными законами.

Документовед руководителя оформляет прием на работу работников, заполняет трудовые договоры, выдает информацию о персональных данных Работника по письменному запросу работника или его представителя на основании нотариально заверенной доверенности на получение таких сведений о профессиональной деятельности работника (справки, выписки из приказов, копии трудовых книжек и т. д.). Запрос должен содержать номер основного документа, удостоверяющего личность Работника или его законного

представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись Работника или его законного представителя.

Экономист имеет право доступа к персональным данным Работника в случае, когда исполнение им своих трудовых обязанностей или трудовых обязанностей работников бухгалтерии по отношению к Работнику (начисление заработной платы, предоставление льгот, установленных законодательством) зависит от знания персональных данных Работника.

При передаче персональных данных Работника директор, делопроизводитель, экономист образовательного учреждения обязаны предупредить лиц, получающих данную информацию, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, а также потребовать от этих лиц письменное подтверждение соблюдения этого условия.

Иные права, обязанности, действия работников, в трудовые обязанности которых входит обработка персональных данных Работника, определяются трудовыми договорами и должностными инструкциями.

Директор образовательного учреждения обязан предоставлять персональную информацию в соответствующее территориальное управление Пенсионного фонда Российской Федерации по форме, в порядке и объеме, установленным законодательством Российской Федерации.

2.3. Родственники и члены семьи Работника не имеют права доступа к его персональным данным.

3. Обязанности работников, имеющих доступ к персональным данным Работника, по их хранению и защите

3.1. Работники, имеющие доступ к персональным данным Работника, обязаны:

- не сообщать персональные данные Работника третьей стороне без его письменного согласия, кроме случаев, когда в соответствии с федеральными законами такого согласия не требуется;
- использовать персональные данные Работника, полученные только от него лично или с его письменного согласия;
- обеспечить защиту персональных данных Работника от неправомерного их использования или утраты, в порядке, установленном законодательством Российской Федерации;
- ознакомить Работника и его представителей с настоящим Положением и их правами, и обязанностями в области защиты персональных данных под роспись;
- соблюдать требование конфиденциальности персональных данных Работника;
- исключать или исправлять по письменному требованию Работника недостоверные или неполные персональные данные Работника, а также данные, обработанные с нарушением требований законодательства;
- ограничивать персональные данные Работника при передаче представителю Работника только той информацией, которая необходима для выполнения указанным представителем своих полномочий;
- не запрашивать информацию о состоянии здоровья Работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

- обеспечить Работнику свободный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные Работника;

- предоставить по требованию Работника полную информацию о его персональных данных и обработке этих данных.

3.2. Лица, имеющие доступ к персональным данным Работника, не вправе:

- получать и обрабатывать персональные данные Работника о его политических, религиозных и иных убеждениях, интимной жизни, членстве в общественных объединениях или профсоюзной деятельности;

- предоставлять персональные данные Работника в коммерческих целях без письменного согласия Работника.

3.3. При принятии решений, затрагивающих интересы Работника, администрации запрещается основываться на персональных данных Работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

4. Права и обязанности Работника

4.1. В целях обеспечения защиты персональных данных, хранящихся у работодателя, Работник имеет право на:

- определение своих представителей для защиты своих персональных данных;

- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса Российской Федерации или иного федерального закона. При отказе администрации исключить или исправить персональные данные Работника последний имеет право

заявить в письменной форме администрации о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера Работник имеет право дополнить заявлением, выражающим его собственную точку зрения; требование об извещении администрацией всех лиц, которым ранее были сообщены неверные или неполные персональные данные Работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

- обжалование в суд любых неправомерных действий или бездействия администрации при обработке и защите персональных данных Работника;

- возмещение убытков и/или компенсацию морального вреда в судебном порядке.

4.2. Работник обязан сообщать администрации сведения, которые могут повлиять на принимаемые в отношении него решения, касающиеся его трудовой деятельности.

5. Хранение персональных данных Работника

Документы, поступившие от Работника, сведения о Работнике, поступившие от третьих лиц с письменного согласия Работника, иная информация, которая касается трудовой деятельности Работника, хранятся в сейфе на бумажных носителях (трудовая книжка, личная карточка, личное дело) и на электронных носителях с ограниченным доступом.

Личные карточки уволенных работников хранятся в архиве образовательного учреждения в алфавитном порядке в течение 75 лет (ст. 339 Перечня типовых управленческих документов, образующихся

в деятельности организаций, с указанием сроков хранения, утвержденного руководителем Федеральной архивной службы России 06.10.2000).

6. Ответственность администрации и ее сотрудников

Защита прав Работника, установленных законодательством Российской Федерации и настоящим Положением, осуществляется судом в целях пресечения неправомерного использования персональных данных Работника, восстановления нарушенных прав и возмещения причиненного ущерба, в том числе морального вреда.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной и материальной ответственности, а также привлекаются к гражданско-правовой, административной ответственности в порядке, установленном федеральными законами.

УТВЕРЖДЕНО
Приказом директора
ОЧУ СОШ «Потенциал»
г. Москвы
от 7.06.2016 г. № 47

_____ Г.В. Гущина

**Положение о защите, хранении, обработке и передаче персональных
данных обучающихся**

ОЧУ СОШ «Потенциал» г. Москвы.

Настоящее Положение разработано на основании Конституции Российской Федерации, Федерального закона от 19.12.2005 №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных», Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» и постановления Правительства Российской Федерации от 17.11.2007 № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» с целью обеспечения уважения прав и основных свобод каждого обучающегося при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1. Общие положения

Персональные данные обучающегося - сведения о фактах, событиях и обстоятельствах жизни обучающегося, позволяющие идентифицировать его личность, необходимые администрации образовательного учреждения

(далее - администрация) в связи с отношениями обучения и воспитания обучающегося и касающиеся обучающегося.

К персональным данным обучающегося относятся:

- сведения, содержащиеся в свидетельстве о рождении, паспорте или ином документе, удостоверяющем личность;
- информация, содержащаяся в личном деле обучающегося;
- информация, содержащаяся в личном деле обучающегося, лишенного родительского попечения;
- сведения, содержащиеся в документах воинского учета (при их наличии);
- информация об успеваемости;
- информация о состоянии здоровья;
- документ о месте проживания;
- СНИЛС;
- иные сведения, необходимые для определения отношений обучения и воспитания.

1.2. Администрация может получить от самого обучающегося данные о:

- фамилии, имени, отчестве, дате рождения, месте жительства, обучающегося;
- фамилии, имени, отчестве родителей (законных представителей) обучающегося.

Иные персональные данные обучающегося, необходимые в связи с отношениями обучения и воспитания, администрация может получить только с письменного согласия одного из родителей (законного представителя). К таким данным относятся документы, содержащие сведения, необходимые для предоставления обучающемуся гарантий и компенсаций, установленных действующим законодательством:

- документы о составе семьи;

- документы о состоянии здоровья (сведения об инвалидности, о наличии хронических заболеваний и т. п.);
- документы, подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством (родители-инвалиды, неполная семья, ребенок-сирота и т. п.).

В случаях, когда администрация может получить необходимые персональные данные обучающегося только у третьего лица, она должна уведомить об этом одного из родителей (законного представителя) заранее и получить от него письменное согласие.

Администрация обязана сообщить одному из родителей (законному представителю) о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа одного из родителей (законного представителя) дать письменное согласие на их получение. Персональные данные обучающегося являются конфиденциальной информацией и не могут быть использованы администрацией или любым иным лицом в личных целях. При определении объема и содержания персональных данных обучающегося администрация руководствуется Конституцией Российской Федерации, федеральными законами и настоящим Положением.

2. Хранение, обработка и передача персональных данных обучающегося

2.1. Обработка персональных данных обучающегося осуществляется для обеспечения соблюдения законов и иных нормативных правовых актов в целях воспитания и обучения обучающегося, обеспечения его личной безопасности, контроля качества образования, пользования льготами, предусмотренными законодательством Российской Федерации и

локальными актами администрации.

2.2. Право доступа к персональным данным обучающегося имеют:

- работники комитета по образованию (при наличии соответствующих полномочий, установленных приказом департамента (управления) образования);
- директор образовательного учреждения;
- документовед образовательного учреждения;
- экономист образовательного учреждения;
- заместители директора по УВР, ВР, ШИС, АХЧ;
- классные руководители (только к персональным данным обучающихся своего класса);
- заведующий библиотекой;
- врач/медработник;
- ответственный за организацию питания обучающихся.

2.3. Директор образовательного учреждения осуществляет прием обучающегося в образовательное учреждение. Директор образовательного учреждения может передавать персональные данные обучающегося третьим лицам, только если это необходимо в целях предупреждения угрозы жизни и здоровья обучающегося, а также в случаях, установленных федеральными законами.

2.4. Классный руководитель принимает или оформляет вновь личное дело обучающегося и вносит в него необходимые данные. Заместитель директора по ШИС предоставляет свободный доступ родителям (законным представителям) к сервису «Электронный дневник» на портале ГАОУ ДПО «ТемоЦентр » на основании письменного заявления. Не имеет права получать информацию об обучающемся родитель, лишенный или ограниченный в родительских правах на основании вступившего в законную силу постановления суда.

Экономист имеет право доступа к персональным данным

обучающегося в случае, когда исполнение им своих трудовых обязанностей или трудовых обязанностей работников бухгалтерии по отношению к обучающемуся (предоставление льгот, установленных законодательством) зависит от знания персональных данных обучающегося.

При передаче персональных данных обучающегося директор, делопроизводитель, экономист, заместители директора по УВР, ВР, АХЧ, классные руководители, ответственный за организацию питания обучающихся обязаны:

- предупредить лиц, получающих данную информацию, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены:
- потребовать от этих лиц письменное подтверждение соблюдения этого условия.

Иные права, обязанности, действия работников, в трудовые обязанности которых входит обработка персональных данных обучающегося, определяются трудовыми договорами и должностными инструкциями.

Все сведения о передаче персональных данных обучающихся регистрируются в Журнале учета передачи персональных данных обучающихся образовательного учреждения в целях контроля правомерности использования данной информации лицами, ее получившими.

3. Обязанности работников администрации, имеющих доступ к персональным данным обучающегося

3.1. Работники администрации, имеющие доступ к персональным данным обучающегося, обязаны:

- не сообщать персональные данные обучающегося третьей стороне без письменного согласия одного из родителей (законного представителя), кроме случаев, когда в соответствии с федеральными законами такого

согласия не требуется;

- использовать персональные данные обучающегося, полученные только от него лично или с письменного согласия одного из родителей (законного представителя);

- обеспечить защиту персональных данных обучающегося от их неправомерного использования или утраты, в порядке, установленном законодательством Российской Федерации;

- ознакомить родителя (родителей) или законного представителя с настоящим Положением и их правами, и обязанностями в области защиты персональных данных;

- соблюдать требование конфиденциальности персональных данных обучающегося;

- исключать или исправлять по письменному требованию одного из родителей (законного представителя) обучающегося его недостоверные или неполные персональные данные, а также данные, обработанные с нарушением требований законодательства;

- ограничивать персональные данные обучающегося при передаче уполномоченным работникам правоохранительных органов или работникам департамента (управления) образования только той информацией, которая необходима для выполнения указанными лицами их функций;

- запрашивать информацию о состоянии здоровья обучающегося только у родителей (законных представителей);

- обеспечить обучающемуся или его родителям (законным представителям) свободный доступ к персональным данным обучающегося, включая право на

получение копий любой записи, содержащей его персональные данные;

- предоставить по требованию одного из родителей (законного представителя) обучающегося полную информацию о его персональных

данных и обработке этих данных.

3.2. Лица, имеющие доступ к персональным данным обучающегося, не вправе:

- получать и обрабатывать персональные данные обучающегося о его религиозных и иных убеждениях, семейной и личной жизни;
- предоставлять персональные данные обучающегося в коммерческих целях.

3.3. При принятии решений, затрагивающих интересы обучающегося, администрации запрещается основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

4. Права и обязанности обучающегося, родителя (законного представителя)

4.1. В целях обеспечения защиты персональных данных, хранящихся у администрации, обучающийся, родитель (законный представитель) имеют право на:

- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований законодательства. При отказе администрации исключить или исправить персональные данные обучающегося родитель (законный представитель) имеет право заявить в письменной форме администрации о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера родитель (законный представитель) имеет право дополнить заявлением, выражающим его собственную точку зрения;
- требование об извещении администрацией всех лиц, которым ранее были сообщены неверные или неполные персональные данные обучающегося, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжалование в суд любых неправомерных действий или бездействия

администрации при обработке и защите персональных данных обучающегося;

- возмещение убытков и/или компенсацию морального вреда в судебном порядке.

4.2. Родитель (законный представитель) обязан сообщать администрации сведения, которые могут повлиять на принимаемые администрацией решения в отношении обучающегося.

5. Хранение персональных данных обучающегося

Должны храниться в сейфе на бумажных носителях и на электронных носителях с ограниченным доступом:

- документы, поступившие от родителя (законного представителя);
- сведения об обучающемся, поступившие от третьих лиц с письменного согласия родителя (законного представителя);
- иная информация, которая касается отношений обучения и воспитания обучающегося.

6. Ответственность администрации и ее сотрудников

Защита прав обучающегося, установленных законодательством Российской Федерации и настоящим Положением, осуществляется судом в целях пресечения неправомерного использования персональных данных обучающегося, восстановления нарушенных прав и возмещения причиненного ущерба, в том числе морального вреда.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных обучающегося, привлекаются к дисциплинарной и материальной ответственности, а также привлекаются к гражданско-правовой, административной ответственности в порядке, установленном федеральными законами.

УТВЕРЖДЕНО
Приказом директора
ОЧУ СОШ «Потенциал»
г. Москвы
от 7.06.2016г. № 47

_____ Г.В. Гущина

Инструкция по организации парольной защиты в ОЧУ СОШ «Потенциал» г. Москвы.

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в ОЧУ СОШ «Потенциал» г. Москвы.

1. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 6 символов;
- в числе символов пароля могут присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, \$, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
- личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

2. При наличии в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п. технологической необходимости использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей их новые значения.
3. Полная плановая смена паролей пользователей должна проводиться по мере необходимости, не реже одного раза в год сотрудниками – администраторами соответствующих средств защиты немедленно после окончания последнего сеанса работы данного пользователя с системой.
4. Внеплановая смена личного пароля или удаление учетной записи пользователя ПК в случае прекращения его полномочий (увольнение, переход на другую работу) должна производиться уполномоченными.
5. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу, другие обстоятельства) администраторов средств защиты и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ПК в ОУ.
6. В случае компрометации личного пароля пользователя ПК должны быть немедленно предприняты меры в соответствии с п.4 или п.5 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.
7. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственного за соблюдение норм парольной защиты.

УТВЕРЖДЕНО
Приказом директора
ОЧУ СОШ «Потенциал»
г. Москвы
от 7.06.2016 г. № 47

_____ Г.В. Гущина

Инструкция по организации антивирусной защиты в ОЧУ СОШ «Потенциал» г. Москвы

Настоящая Инструкция определяет требования к организации защиты в ОЧУ СОШ «Потенциал» г. Москвы (далее Организация) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников Организации за их выполнение.

К использованию в Организации допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

Установка средств антивирусного контроля на компьютерах осуществляется уполномоченным сотрудником Организации. Настройка параметров средств антивирусного контроля в соответствии с руководствами по применению конкретных антивирусных средств.

Применение средств антивирусного контроля еженедельно в начале работы при загрузке компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, CD-ROM и т.п.).

Контроль входящей и исходящей информации на защищаемых серверах и персональных компьютерах (далее ПК) осуществляется непрерывно посредством постоянно работающего компонента антивирусного программного обеспечения («монитора»).

Полная проверка информации, хранящейся на серверах и ПК должна осуществляться не реже одного раза в месяц.

Обновление баз вирусов антивирусного программного обеспечения, установленного на ПК и серверах, должно осуществляться ежедневно. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), должна быть выполнена антивирусная проверка:

- на защищаемом автоматизированном рабочем месте (АРМ) - ответственным за обеспечение информационной безопасности.

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.) сотрудник Организации самостоятельно или вместе с ответственным за антивирусную защиту Организации должен провести внеочередной антивирусный контроль своей рабочей станции.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и ответственного за антивирусную защиту Организации, владельца зараженных файлов, а также сотрудников,

использующих эти файлы в работе;

- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

Ответственность за организацию антивирусного контроля в Организации, в соответствии с требованиями настоящей Инструкции возлагается на руководителя Организации.

Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящей Инструкции возлагается на ответственного за антивирусную защиту Организации и всех сотрудников, являющихся пользователями ПК Организации.

Периодический контроль за состоянием антивирусной защиты в Организации, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками подразделений Организации осуществляется ответственным за антивирусную защиту Организации.

