Государственное бюджетное специальное (коррекционное) образовательное учреждение для обучающихся, воспитанников с ограниченными возможностями здоровья общеобразовательная школа-интернат № 7 VIII вида станицы Казанской Краснодарского края

« 01 » сентября 2015 г. **ПРИКАЗ** № 242

О проведении работ по защите персональных данных в ГБС(К)ОУ школе – интернате № 7 станицы Казанской

В целях исполнения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и в соответствии с постановлением Правительства РФ от 21 марта 2012 г. № 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», ПРИКАЗЫВАЮ:

1. Ввести в ГБС(К)ОУ школе – интернате № 7 станицы Казанской режим защиты персональных данных.
2. Осуществлять режим защиты персональных данных в отношении данных, указанных в Перечне персональных данных, обрабатываемых в ГБС(К)ОУ школе – интернат № 7 станицы Казанской.
3. Утвердить:
3.1. Правила обработки персональных данных (Приложение № 1);
3.2. Правила рассмотрения запросов субъектов персональных данных или их представителей (Приложение № 2);
3.3. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (Приложение № 3);
3.4. Перечень должностей сотрудников ГБС(К)ОУ школы – интернат № 7 станицы Казанской, замещение которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным (Приложение №4);
3.5. Инструкция пользователя ИСПДн ГБС(К)ОУ школы – интернат № 7 станицы Казанской по работе с ПДн (Приложение №5).

3.6. Инструкцию по обеспечению безопасности персональных данных в АИС ГБС(К)ОУ школе – интернате № 7 станицы Казанской (Приложение № 6);

3.7. Инструкцию по организации парольной защиты в АИС ГБС(К)ОУ школе – интернате № 7 станицы Казанской (Приложение № 7);

3.8. Инструкцию по организации антивирусной защиты в ГБС(К)ОУ школе – интернате № 7 станицы Казанской (Приложение № 8);

3.10. Инструкция по резервированию и восстановлению работоспособности технических средств и программного обеспечения, баз данных, средств защиты информации и средств криптографической защиты информации в АИС в ГБС(К)ОУ школе – интернате № 7 станицы Казанской (Приложение № 9).

4. Ответственному за организацию обработки Загуменной А.А., довести приказ до сотрудников ГБС(К)ОУ школы – интернат № 7 станицы Казанской по роспись.

5. В случае неисполнения настоящего приказа лицо, ответственное за организацию обработки персональных данных, может быть привлечено к ответственности в соответствии с действующим законодательством Российской Федерации

6. Настоящий приказ вступает в силу с момента его подписания.

7. Контроль за выполнением настоящего приказа оставляю за собой.

Директор ГБС(К)ОУ
школы – интернат № 7
станицы Казанской Д.Н. Агафонов

ПРИНЯТО

На заседании
Педагогического совета
31.08.2015 г
Протокол №1

УТВЕРЖДАЮ
Директор ГБС(К)ОУ
школы – интернат № 7
станицы Казанской
_____ Д.Н. Агафонов
от «01» сентября 2015 года

Приложение № 1
к приказу № 271 от 01.09.2015г.

ПРАВИЛА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

7. Меры, направленные на выявление и предотвращение нарушений, предусмотренных законодательством.

1) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону от 25 июля 2011г. №261-ФЗ (далее - Федеральный закон) и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

2) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом;

3) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

8. Обеспечение безопасности персональных данных достигается, в частности:

1. определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2. применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3. применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4. оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных.

9. Целями обработки персональных данных работников являются:

1) обеспечение соблюдения законов и иных нормативных правовых актов;

2. соблюдение порядка и правил приема на государственную гражданскую службу;

4. использование в уставной деятельности с применением средств автоматизации или без таких средств, включая хранение этих данных в

архивах и размещение в информационно-телекоммуникационных сетях с целью предоставления доступа к ним;

5. заполнение базы данных автоматизированной информационной системы в целях повышения эффективности и быстрого поиска, проведения мониторинговых исследований, формирования статистических и аналитических отчётов в вышестоящие органы;

6) обеспечение личной безопасности работников.

10. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

11. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий 3 (трех) рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора, В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий 10 (десяти) рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

12. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий 30 (тридцати) дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе

осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

13. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом персональных данных. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

14. В случае отсутствия возможности уничтожения персональных данных в течение сроков, указанных выше, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем 6 (шесть) месяцев, если иной срок не установлен федеральными законами.

ПРИНЯТО

На заседании
Педагогического совета
31.08.2015 г
Протокол №1

УТВЕРЖДАЮ
Директор ГБС(К)ОУ
школы – интернат № 7
станицы Казанской
_____ Д.Н. Агафонов
от «01» сентября 2015 года

Приложение № 2
к приказу № 172 от 01.09.2015г.

Правила
рассмотрения запросов субъектов персональных данных или их представителей в ГБС(К)ОУ школе – интернате № 7 станицы Казанской

1. Настоящими Правилами рассмотрения запросов субъектов персональных данных или их представителей в ГБС(К)ОУ школе – интернате № 7 станицы Казанской (далее – Правила) определяются порядок учета (регистрации), рассмотрения запросов субъектов персональных данных или их представителей (далее – запросы).

2. Настоящие Правила разработаны в соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 г. № 152 - ФЗ «О персональных данных» (далее – Федеральный закон), Федеральным законом от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Федеральным законом от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации», Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21 марта 2012 г. № 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», приказом Минэкономразвития РФ от 14.05.2010г. № 180 «Об установлении порядка предоставления сведений, содержащихся в Едином государственном реестре прав на недвижимое имущество и сделок с ним» и другими нормативными правовыми актами.

3. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных (часть 7 статьи 14 Федерального закона), в том числе содержащей:

- подтверждение факта обработки персональных данных в ГБС(К)ОУ школе – интернат № 7 станицы Казанской (далее – школа);
- правовые основания и цели обработки персональных данных;
- цели и применяемые в школе способы обработки персональных данных;
- наименование и место нахождения школы, сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора со школой или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению школы, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом или другими федеральными законами.

4. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с частью 8 статьи 14 Федерального закона.

5. Субъект персональных данных вправе требовать от школы уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

6. Сведения, указанные в части 7 статьи 14 Федерального закона, должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

7. Сведения, указанные в части 7 статьи 14 Федерального закона, предоставляются субъекту персональных данных или его представителю школы при обращении либо при получении запроса субъекта персональных данных или его представителя.

8. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Управлением (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных школой, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

9. Рассмотрение запросов является служебной обязанностью должностных лиц, в чьи обязанности входит обработка персональных данных (далее – должностные лица Управления).

10. Должностные лица школы обеспечивают:

- объективное, всестороннее и своевременное рассмотрения запроса;
- принятие мер, направленных на восстановление или защиту нарушенных прав, свобод и законных интересов субъектов персональных данных;
- направление письменных ответов по существу запроса.

11. Ведение делопроизводства по запросам осуществляется сотрудником школы.

12. Все поступившие запросы регистрируются в день их поступления. На запросе проставляется штамп, в котором указывается входящий номер и дата регистрации.

13. Запрос прочитывается, проверяется на повторность, при необходимости сверяется с находящейся в архиве предыдущей перепиской. В случае, если сведения, указанные в части 7 статьи 14 Федерального закона, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в школу или направить повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона, и ознакомления с такими персональными данными не ранее чем через 30 дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

Субъект персональных данных вправе обратиться повторно в школу или направить повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в настоящем пункте, в случае, если такие сведения и (или) обрабатываемые

персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду с необходимыми сведениями должен содержать обоснование направления повторного запроса.

14. Школа вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона. Такой отказ должен быть мотивированным.

15. Прошедшие регистрацию запросы представляются директору школы либо лицу, его заменяющему, который определяет порядок и сроки их рассмотрения, дает по каждому из них письменное указание исполнителям.

16. Директор школы, заместители директора и другие должностные лица школы при рассмотрении и разрешении запроса обязаны:

- внимательно разобраться в их существе, в случае необходимости истребовать дополнительные материалы или направить сотрудников на места для проверки фактов, изложенных в запросах, принять другие меры для объективного разрешения поставленных заявителями вопросов, выявления и устранения причин и условий, порождающих факты нарушения законодательства о персональных данных;
- принимать по ним законные, обоснованные и мотивированные решения и обеспечивать своевременное и качественное их исполнение;
- сообщать в письменной форме субъекту персональных данных о решениях, принятых по их запросам, со ссылками на законодательство Российской Федерации, а в случае отклонения запроса - разъяснять также порядок обжалования принятого решения.

17. Школа обязана сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя в течение 30 дней с даты получения запроса субъекта персональных данных или его представителя, если иное не предусмотрено другими нормативными актами.

18. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении, либо при получении запроса субъекта персональных данных или его представителя должностные лица школы обязаны дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 30 дней со дня обращения субъекта персональных данных или его представителя, либо с даты получения запроса субъекта персональных данных или его представителя, если иное не предусмотрено другими нормативными актами.

19. Школа обязана предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных, если иное не предусмотрено другими нормативными актами.

20. В срок, не превышающий 7 рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, должностные лица школы обязаны внести в них необходимые изменения.

21. В срок, не превышающий 7 рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, должностные лица школы обязаны уничтожить такие персональные данные.

22. Школа обязана уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

23. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных должностные лица школы обязаны осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных с момента такого обращения или получения указанного запроса на период проверки.

24. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных должностные лицашколы обязаны осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

25. В случае подтверждения факта неточности персональных данных должностные лица школы на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязаны уточнить персональные данные в течение 7 рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

26. В случае выявления неправомерной обработки персональных данных должностные лица школы в срок, не превышающий 3 рабочих дней с даты этого выявления, обязаны прекратить неправомерную обработку персональных данных. В случае, если обеспечить правомерность обработки персональных данных невозможно, должностные лица в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки персональных данных, обязаны уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных школа обязана уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

27. Для проверки фактов, изложенных в запросах при необходимости организуются служебные проверки в соответствии с законодательством Российской Федерации.

28. По результатам служебной проверки составляется мотивированное заключение, которое должно содержать объективный анализ собранных материалов. Если при проверке выявлены факты совершения сотрудниками школы действия (бездействия), содержащего признаки административного правонарушения или состава преступления информация передается незамедлительно в правоохранительные органы. Результаты служебной проверки представляются директору школы.

29. Запрос считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и даны исчерпывающие ответы субъекту персональных данных или его представителю.

30. Ответы на запросы оформляются на бланке школы установленной формы.

31. Должностные лица, виновные в нарушении установленного порядка рассмотрения запросов подлежат привлечению к ответственности в соответствии с законодательством Российской Федерации.

ПРИНЯТО

На заседании
Педагогического совета
31.08.2015 г
Протокол №1

УТВЕРЖДАЮ
Директор ГБС(К)ОУ
школы – интернат № 7
станицы Казанской
_____ Д.Н. Агафонов
от «01» сентября 2015 года

Приложение № 3
к приказу № 222 от 01.09.2015г.

Правила
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных ГБС(К)ОУ школы – интернат № 7 станицы Казанской

I. Общие положения.

1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных ГБС(К)ОУ школы – интернат № 7 станицы Казаснкой (далее Школа) разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 21.03.2012 № 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».

2. Настоящие Правила определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных и действуют постоянно.

II. Тематика внутреннего контроля

1. Тематика проверок обработки персональных данных с использованием средств автоматизации:

1.1. соответствие полномочий пользователя матрице доступа;
1.2. соблюдение пользователями информационных систем персональных данных Школы парольной политики;
1.3. соблюдение пользователями информационных систем персональных данных Школы антивирусной политики;

1.4. соблюдение пользователями информационных систем персональных данных Школы правил работы со съемными носителями персональных данных;
1.5. соблюдение ответственными за криптографические средства защиты информации правил работы с ними;
1.6. соблюдение порядка доступа в помещения Школы, где расположены элементы информационных систем персональных данных;
1.7. соблюдение порядка резервирования баз данных и хранения резервных копий;
1.8. соблюдение порядка работы со средствами защиты информации;
1.9. знание пользователей информационных систем персональных данных о своих действиях во внештатных ситуациях.

2. Тематика проверок обработки персональных данных без использования средств автоматизации:
2.1. хранение бумажных носителей с персональными данными;
2.2. доступ к бумажным носителям с персональными данными;
2.3. доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными.

III. Порядок проведения внутренних проверок.

1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям Школа организует проведение периодических проверок условий обработки персональных данных.
2. Проверки осуществляются ответственным за организацию обработки персональных данных (далее Ответственный) либо комиссией, образуемой директором Школы.
3. Внутренние проверки проводятся по необходимости в соответствии с поручением директора Школы.
4. Проверки осуществляются Ответственным либо комиссией непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных.
5. Для каждой проверки составляется Протокол проведения внутренней проверки.
6. При выявлении в ходе проверки нарушений, Ответственным либо Председателем комиссии в Протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.
7. Протоколы хранятся у Ответственного либо Председателя комиссии в течение текущего года. Уничтожение Протоколов проводится Ответственным либо комиссией самостоятельно в январе следующего за проверочным годом.

8. О результатах проверки и мерах, необходимых для устранения нарушений, директору Школы докладывает Ответственный либо Председатель комиссии.

ПРИНЯТО

На заседании
Педагогического совета
31.08.2015 г
Протокол №1

УТВЕРЖДАЮ
Директор ГБС(К)ОУ
школы – интернат № 7
станицы Казанской
_____ Д.Н. Агафонов
от «01» сентября 2015 года

Приложение № 4
к приказу № 272 от 01.09.2015г.

ПЕРЕЧЕНЬ

должностей в ГБС(К)ОУ школы – интернат № 7 станицы Казанской, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

№	Наименование должности	Замещение должности предусматривает	Категория персональных данных
1.	Директор	осуществление доступа к персональным данным	персональные данные, обрабатываемые в связи с реализацией трудовых отношений, а также в связи с оказанием государственных услуг и осуществлением государственных функций
2.	Главный бухгалтер		
3.	Заместители директора		
4.	Делопроизводитель	осуществление доступа к персональным данным	персональные данные гражданских служащих и работников возглавляемых отделов; персональные данные граждан, содержащиеся в обращениях граждан, персональные данные граждан, обрабатываемые в целях оказания государственных услуг и исполнения государственных функций
5.	Главный бухгалтер, бухгалтер		персональные данные гражданских служащих возглавляемых отделов; персональные данные граждан, содержащиеся в обращениях граждан персональные данные гражданских

№	Наименование должности	Замещение должности предусматривает	Категория персональных данных
			служащих возглавляемых отделов; персональные данные граждан, содержащиеся в обращениях граждан персональные данные гражданских служащих возглавляемых отделов; персональные данные граждан, содержащиеся в обращениях граждан.
6.	Делопроизводитель	осуществление обработки персональных данных осуществление обработки персональных данных	персональные данные гражданских служащих и, содержащиеся в кадровых документах, персональные данные граждан, включенных в кадровый резерв; персональные данные граждан, не допущенных к участию в конкурсах, и граждан, участвовавших в конкурсах, но не прошедших конкурсный отбор; персональные данные граждан, содержащиеся в обращениях граждан
7.	Главный бухгалтер		
8.	бухгалтер		
9.	Главный бухгалтер		персональные данные гражданских служащих и работников; персональные данные граждан, представленные в целях заключения договоров с независимыми экспертами, подлежащие оплате, в целях заключения договоров и ведения расчетов с физическими лицами, персональные данные граждан, содержащиеся в обращениях граждан
10.	Классные руководители, воспитатели, педагог - психолог, медицинский работник	осуществление доступа к персональным данным	персональные данные граждан, содержащиеся в обращениях граждан

ПРИНЯТО

На заседании
Педагогического совета
31.08.2015 г
Протокол №1

УТВЕРЖДАЮ
Директор ГБС(К)ОУ
школы – интернат № 7
станицы Казанской
_____ Д.Н. Агафонов
от «01» сентября 2015 года

Приложение № 5
к приказу № 272 от 01.09.2015г.

Инструкция пользователя ИСПДн
ГБС(К)ОУ школы – интернат № 7 станицы Казанской по работе с ПДн

1 Общие положения

1.1. Пользователь информационных систем персональных данных (ИСПДн) (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.
1.2. Пользователем является каждый сотрудник ГБС(К)ОУ школы – интернат № 7 станицы Казанской, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.
1.3. Пользователь несет персональную ответственность за свои действия.
1.4. Пользователь в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России и регламентирующими документами ГБС(К)ОУ школы – интернат № 7 станицы Казанской.
1.5. Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных.

2 Должностные обязанности

Пользователь обязан:
2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в Положении о разграничении прав доступа к обрабатываемым персональным данным.
2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.
2.4. Соблюдать требования парольной политики.
2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других.
2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).
2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью, а так же для получений консультаций по вопросам информационной безопасности, необходимо обратиться к ответственному за обеспечение защиты ПД Хлыстовой Т.В зам. директора по УВР
2.8. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИСПДн.
2.9. Пользователям запрещается:
- разглашать защищаемую информацию третьим лицам;
- копировать защищаемую информацию на внешние носители без разрешения своего руководителя;
- самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- несанкционированно открывать общий доступ к папкам на своей рабочей станции;
- запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;
- отключать (блокировать) средства защиты информации;
- обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн;
- сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;
- привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.
2.10. При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>.

2.11. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах возложенных на него функций.

3 Организация парольной защиты

3.1 Личные пароли доступа к элементам ИСПДн выдаются пользователям Администратором информационной безопасности, Администратором ИСПДн или создаются самостоятельно.

3.2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

3.3. Правила формирования пароля:

- пароль не может содержать имя учетной записи пользователя или какую-либо его часть.
- пароль должен состоять не менее чем из 8 символов.
- в пароле должны присутствовать символы трех категорий из числа следующих четырех:

- прописные буквы английского алфавита от A до Z;
- строчные буквы английского алфавита от a до z;
- десятичные цифры (от 0 до 9);
- символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).

- запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;
- запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
- запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);
- запрещается выбирать пароли, которые уже использовались ранее.

3.4. Правила ввода пароля:

- ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;
- во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.5. Правила хранение пароля:

- запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;
- запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

3.6. Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию;
- своевременно сообщать Администратору информационной безопасности об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

4 Правила работы в сетях общего доступа и (или) международного обмена

4.1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее – Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

4.2. При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирус и других);
- передавать по Сети защищаемую информацию без использования средств шифрования;
- запрещается скачивать из Сети программное обеспечение и другие файлы;
- запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты, содержащие нелегально распространяемое ПО и другие);
- запрещается нецелевое использование подключения к Сети.

5 Права и ответственность пользователей ИСПДн

5.1 Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн.

5.2 Пользователи, виновные в несоблюдении Настоящей инструкции расцениваются как нарушители Федерального закона РФ 27.07.2006 г. N 152-ФЗ "О персональных данных" и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

ПРИНЯТО

На заседании
Педагогического совета
31.08.2015 г
Протокол №1

УТВЕРЖДАЮ
Директор ГБС(К)ОУ
школы – интернат № 7
станицы Казанской
_____ Д.Н. Агафонов
от «01» сентября 2015 года

Приложение № 6
к приказу № 242 от 01.09.2015г.

ПОЛОЖЕНИЕ
об обеспечении безопасности автоматизированной информационной системы ГБС(К)ОУ школы – интернат № 7 станицы Казанской

1. Общие положения

Настоящее Положение определяет требования по обеспечению безопасности автоматизированной информационной системы (далее по тексту - АИС) образовательного учреждения (далее по тексту – Оператор).

АИС представляет собой IT-систему, предназначенную для автоматизации процессов формирования, обработки и анализа информации по основным направлениям деятельности Оператора.

Основными функциональными возможностями АИС Оператора являются:

- формирование, хранение и обновление сведений о структуре учебных подразделений Оператора;
- формирование, хранение и обновление сведений о преподавательском составе и сотрудниках учебных подразделений Оператора;
- формирование, хранение и обновление сведений об индивидуальных планах работы преподавательского состава;
- формирование, хранение и обновление сведений об учебном (учебно-производственном) плане Оператора;
- формирование, хранение и обновление сведений об учебной нагрузке преподавательского состава;
- формирование, хранение и обновление сведений о научной и учебно-методической продукции (методические рекомендации, учебные пособия, монографии, публикации) преподавательского состава;
- формирование, хранение и обновление сведений об обучающихся, проходящих обучение у Оператора;
- формирование, хранение и обновление сведений о результатах учебного процесса (итоги тестирования, экзаменов);

- аналитическая обработка информации о проведении учебного процесса как за отчётный период, так и о текущей деятельности учебных подразделений Оператора.

В качестве информации, подлежащей защите в АИС Оператора, рассматриваются:

- персональные данные преподавательского состава и сотрудников учебных подразделений;
- персональные данные обучающихся, проходящих и прошедших обучение;
- персональные данные административно-хозяйственных подразделений.

При обеспечении безопасности персональных данных в информационной системе Оператор руководствуется следующим: выбор средств защиты информации для системы защиты персональных данных; определение типа угроз безопасности персональных данных, актуальных для информационной системы; установление и обеспечение уровня защищённости персональных в информационной системе производится Оператором в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утверждённых постановлением Правительства РФ от 1 ноября 2012 г. N 1119. Основными группами угроз, на противостояние которым направлены цели и требования безопасности, являются:

- угрозы, связанные с осуществлением несанкционированного доступа (ознакомления) с информацией, содержащей сведения о персональных данных работников и обучающихся, при ее обработке и хранении;
- угрозы, связанные с несанкционированным копированием (хищением) информации, содержащей сведения о персональных данных работников и обучающихся;
- угрозы, связанные с осуществлением доступа к информации, содержащей сведения о персональных данных работников и обучающихся, без разрешения на то ее владельца (субъекта персональных данных);
- угрозы, связанные с нарушением порядка доступа к информации, содержащей сведения о персональных данных работников и обучающихся, передаваемой заинтересованным лицам;
- угрозы, связанные с перехватом информации, содержащей сведения о персональных данных работников и обучающихся, из каналов передачи данных с использованием специализированных программно-технических средств;
- угрозы, связанные с потерей (утратой) информации, содержащей сведения о персональных данных работников и обучающихся, вследствие сбоев (отказов) программного и аппаратного обеспечения;
- угрозы, связанные с внедрением компьютерных вирусов и другого вредоносного программного обеспечения;
- угрозы, связанные с осуществлением несанкционированных информационных воздействий (направленных на «отказ в обслуживании»

для сервисов, модификацию конфигурационных данных программно-аппаратных средств, подбор аутентификационной информации и т.п.).

Функциональные требования безопасности охватывают:

- требования к осуществлению аудита безопасности;
- требования к обеспечению подлинности субъектов обмена информацией;
- требования к криптографической поддержке;
- требования к защите информации, содержащей сведения о персональных данных работников и обучающихся;
- требования к идентификации и аутентификации пользователей АИС;
- требования к управлению безопасностью;
- требования к защите системы безопасности.

2. *Основные функциональные возможности АИС, связанные с обеспечением безопасности (защитой информации)*

2.1. Защита данных пользователя

АИС должна осуществлять функции и политику избирательного (дискреционного) управления доступом. Избирательное управление доступом должно предоставлять возможность ограничивать и контролировать доступ к системе и к информации, содержащей сведения о персональных данных.

Каждый Пользователь, пытающийся получить доступ к АИС, сначала должен проходить процедуру идентификации и аутентификации, а затем, при попытках получения доступа к активам, – авторизацию, т.е. проверку разрешений Пользователя по отношению к какому-либо защищаемому активу.

В АИС доступ к информации должен быть разрешен только уполномоченным на это Пользователям. Модель защиты АИС должна включать компоненты, которые реализуют контроль субъектов доступа, действий, предпринимаемых конкретной сущностью по отношению к объекту доступа.

Каждый объект доступа, представленный в АИС, должен быть однозначно ассоциирован с набором атрибутов безопасности, определяющих безопасность защищаемого объекта. Данный набор атрибутов должен формироваться при создании объекта и впоследствии может меняться. Изменение их значений должно быть обеспечено только Пользователям, имеющим статус владельца объекта, а также субъектам, которым предоставлены соответствующие полномочия.

Права доступа субъектов к объекту должны определяться посредством списка управления доступом. Список управления доступом должен включать перечень пользователей, которым разрешен доступ к объекту, а также набор допустимых над объектом действий.

2.2. Аудит событий безопасности

АИС должна обеспечивать набор средств аудита, предназначенных для мониторинга и обнаружения нежелательных условий, которые могут возникнуть, а также событий, которые могут произойти в системе. Мониторинг относящихся к безопасности событий должен позволять обнаруживать нарушителей безопасности, а также выявлять попытки несанкционированного доступа к АИС или доступа к защищаемой информации. В частности, определяя политику аудита, уполномоченный администратор АИС должен иметь возможность осуществлять аудит только необходимых типов событий безопасности, таких как неудачные попытки подключения пользователей к АИС. Запись результатов аудита событий безопасности должна осуществляться в журналы регистрации событий аудита, доступ к которому должен быть разрешен только уполномоченному администратору АИС. Просмотр журналов регистрации событий аудита должен выполняется с использованием средств АИС (специализированных инструментальных средств). Данные средства должны предоставлять возможность мониторинга и регистрации только тех событий аудита, которые удовлетворяют заданным критериям, что позволит ограничить объем данных, собираемых о событиях безопасности.

2.3. Идентификация и аутентификация

АИС должна требовать, чтобы все субъекты доступа уникально идентифицировались и аутентифицировались при доступе к АИС с помощью ввода идентификатора и пароля. Идентификация и аутентификация должны осуществляться до выполнения субъектом доступа каких-либо действий. АИС должна поддерживать аутентификацию Пользователей вместе с их авторизацией. Предусматривается, что авторизация Пользователей представляет начальный уровень для разрешения доступа к локальным и сетевым ресурсам.

АИС должна обеспечивать хранение паролей в преобразованном формате. АИС должна предоставлять средства усиления безопасности паролей через использование механизмов, позволяющих определить минимальную длину, время действия (минимальное и максимальное), задать требование уникальности (неповторяемости) и время смены пароля.

АИС должна предоставлять механизм блокирования учетной записи пользователя после определенного количества попыток ввода неправильного имени и/или пароля пользователя до ее разблокирования администратором АИС или по истечении времени действия, заданного для счетчика блокировки.

2.4. Защита системы безопасности

АИС должна предоставлять ряд возможностей для обеспечения защиты системы безопасности. Изоляция процессов и поддержания домена

безопасности должны обеспечивать безопасное выполнение функций системы безопасности АИС. Возможность осуществления периодического тестирования среды функционирования АИС (аппаратной части) и собственно самих функций системы безопасности АИС должно обеспечивать поддержание уверенности администратора АИС в целостности и корректности функционирования функций системы безопасности.

3. Основные функциональные возможности повышения надежности

АИС должна обеспечивать надежную защиту данных от непредвиденных сбоев или отказов системы, обеспечивая следующие возможности по повышению надежности.

3.1. Резервное копирование данных

В АИС должны входить стандартные средства предотвращения потери данных и их восстановления в случае возможных сбоев. Имеющиеся средства резервного копирования должны предоставлять Пользователям возможность выбора различных стратегий резервного копирования, обеспечивающих необходимый уровень защиты данных в случае возникновения сбоев в работе системы, при этом Пользователям должна предоставляться возможность выполнения резервного копирования данных на несъемные и съемные устройства хранения.

3.2. Восстановление системы

Функциональные возможности восстановления системы должны позволять возвращать АИС в состояние, предшествующее сбою. При этом в АИС не должно происходить потери (либо потери должны быть минимальны) и искажения данных.

3.3. Средства администрирования, управления и поддержки

В состав АИС должны быть интегрированы графические средства администрирования и/или утилиты командной строки, обеспечивающие эффективное полномасштабное и гибкое управление (в том числе мониторинг).

4. Среда безопасности АИС

4.1. Модели угроз, характерные для АИС

4.1.1. Осуществление несанкционированного ознакомления с персональными данными работников и обучающихся.

Источники угрозы – внешний злоумышленник.

Способ (метод) реализации угрозы – перехват информации из каналов передачи данных с использованием специализированных программно-технических средств.

Используемые уязвимости – возможные недостатки механизмов защиты информации при ее передаче по каналам передачи данных, связанные с возможностью несанкционированного ознакомления с передаваемой информацией третьих лиц.
Вид информации, потенциально подверженной угрозе – персональные данные работников и обучающихся.
Нарушаемое свойство безопасности – конфиденциальность.
Возможные последствия реализации угрозы – нанесения морального и/или материального ущерба лицу, фигурирующему в перехваченной информации. Нанесение косвенного материального ущерба образовательному учреждению.

4.1.2. Осуществление несанкционированного ознакомления с персональными данными работников и обучающихся и их модификация (в том числе подмена).
Источники угрозы – внешний злоумышленник.
Способ (метод) реализации угрозы – перехват информации из каналов передачи данных с использованием специализированных программно-технических средств; модификация (в том числе подмена) перехваченной информации и навязывание ложной информации.
Используемые уязвимости – недостатки механизмов защиты информации при ее передаче по каналам передачи данных, связанные с возможностью несанкционированного ознакомления и модификации (в том числе подмены) передаваемой информации.
Вид информации, потенциально подверженной угрозе – персональные данные работников и обучающихся.
Нарушаемые свойства безопасности – конфиденциальность, целостность.
Возможные последствия реализации угрозы – нанесения морального и/или материального ущерба лицу, фигурирующему в перехваченной информации из-за несанкционированного раскрытия конфиденциальной информации или распространения раскрытых данных. Нанесение косвенного материального ущерба образовательному учреждению.

4.1.3. Нарушение доступности, утрата или искажение предоставляемых персональных данных работников и обучающихся вследствие сбоев (отказов) программного и аппаратного обеспечения.
Источники угрозы – программное и аппаратное обеспечение.
Способ (метод) реализации угрозы – сбои (отказы) программного и аппаратного обеспечения.
Используемые уязвимости – недостатки механизмов обеспечения доступности требуемой информации, связанные с возможностью блокирования предоставления информации на недопустимое время.
Вид информации, потенциально подверженной угрозе – персональные данные работников и обучаемых.

Нарушаемое свойство безопасности – доступность, достоверность.
Возможные последствия реализации угрозы – нарушение со стороны образовательного учреждения взятых на себя обязательств по обработке персональных данных работников и обучающихся и может привести к прямому или косвенному материальному ущербу образовательному учреждению.

4.1.4. Нарушение согласованности данных в персональных данных работников и обучающихся вследствие сбоев (отказов) программного и аппаратного обеспечения, а также ошибок персонала образовательного учреждения.
Источники угрозы – программное и аппаратное обеспечение, персонал образовательного учреждения.
Способ (метод) реализации угрозы – сбои (отказы) программного обеспечения и ошибки персонала образовательного учреждения.
Используемые уязвимости – недостатки механизмов обеспечения согласованности данных в БД АИС, связанные с возможностью нарушения согласованности.
Вид информации, потенциально подверженной угрозе – персональные данные работников и обучающихся.
Нарушаемые свойства безопасности активов – достоверность, целостность.
Возможные последствия реализации угрозы – рассогласование в персональных данных работников и обучаемых, хранимых в БД АИС, что, в свою очередь, приведет к возможному нанесения морального и/или материального ущерба образовательному учреждению.

4.1.5. Осуществление доступа (ознакомления) с персональными данными обучающегося, хранимыми и обрабатываемыми в АИС, без согласия субъекта персональных данных или окончания срока действия такого согласия.
Источники угрозы – уполномоченные на доступ к персональным данным внутренние и внешние пользователи.
Способ (метод) реализации угрозы – осуществление доступа к персональным данным обучающихся с использованием штатных средств, предоставляемых программно-аппаратным обеспечением АИС.
Используемые уязвимости – недостатки механизмов защиты персональных данных обучающегося, связанные с возможностью доступа к ним без письменного согласия субъекта персональных данных или после окончания срока его действия.
Вид информации, потенциально подверженной угрозе – персональные данные обучающихся.
Нарушаемые свойства безопасности – конфиденциальность.

Возможные последствия реализации угрозы – несанкционированное ознакомление с персональными данными ведет к нанесению морального и/или материального ущерба обучающемуся из-за несанкционированного раскрытия конфиденциальной информации.

4.1.6. Внедрение в информационную систему образовательного учреждения вирусов и другого вредоносного программного обеспечения при взаимодействии с внешними системами, а также пользователями с носителей информации, используемых на автоматизированных рабочих местах.

Источники угрозы – внутренние пользователи и персонал образовательного учреждения, внешние системы.

Способ (метод) реализации угрозы – внедрение вирусов и другого вредоносного программного обеспечения при взаимодействии с внешними системами (файловый обмен, электронная почта и т.п.), а также при использовании съемных носителей информации на автоматизированных рабочих местах.

Используемые уязвимости – недостатки механизмов защиты информационной системы образовательного учреждения от внедрения вирусов и другого вредоносного программного обеспечения, связанные с возможностью внедрения вирусов и другого вредоносного программного обеспечения.

Вид информации, потенциально подверженной угрозе – программное обеспечение информационной системы образовательного учреждения.

Нарушаемое свойство безопасности активов – целостность.

Возможные последствия реализации угрозы – нарушение режимов функционирования информационной системы образовательного учреждения, потеря (утрата) и искажение информации, снижение уровня защищенности информационной системы образовательного учреждения. Ведет к возможному материальному ущербу образовательному учреждению.

4.1.7. Осуществление несанкционированных информационных воздействий (модификация конфигурационных данных программно-аппаратных средств, подбор аутентификационной информации и т.п.) на информационную систему образовательного учреждения, осуществляемых из внешних систем.

Источники угрозы – внешние злоумышленники, внешние системы.

Способ (метод) реализации угрозы – несанкционированные информационные воздействия с использованием специализированного программно-аппаратного обеспечения.

Используемые уязвимости – недостатки механизмов защиты информационной системы образовательного учреждения от несанкционированных внешних воздействий.

Вид информации, потенциально подверженной угрозе – программно-аппаратное обеспечение информационной системы образовательного учреждения.

Нарушаемые свойства безопасности активов – конфиденциальность, целостность.

Возможные последствия реализации угрозы – нарушение режимов функционирования информационной системы образовательного учреждения, снижение уровня защищенности информационной системы образовательного учреждения. Ведет к возможному материальному ущербу образовательному учреждению.

4.2. Политика и цели безопасности для АИС

АИС должна обеспечить следование приведенным ниже правилам безопасности:

1. Должна быть обеспечена регистрация и учет получения (включая указание срока действия) согласия обучающегося на обработку предоставленных им в образовательное учреждение своих персональных данных.
2. Должна быть обеспечена возможность надежного хранения персональных данных работников и обучающихся (в течение действия срока трудового договора и разрешения на обработку персональных данных соответственно).
3. Должна быть обеспечена возможность безопасного восстановления АИС после сбоев и отказов программного обеспечения и оборудования.
4. Должна быть обеспечена защита информации, составляющей персональные данные работников и обучающихся, при ее обработке, хранении и передаче специализированными средствами защиты.
5. Должно быть обеспечено наличие надлежащих, защищенных от несанкционированного использования, механизмов регистрации и предупреждения администратора АИС о любых событиях, относящихся к безопасности АИС.
6. Должно быть обеспечено наличие надлежащих и корректно функционирующих средств администрирования безопасности информационной системы образовательного учреждения, доступных только уполномоченным администраторам.
7. Должны быть предоставлены механизмы аутентификации, обеспечивающие адекватную защиту от прямого или умышленного нарушения безопасности нарушителями с низким потенциалом нападения.
8. Должны быть обеспечены механизмы генерации, надлежащего и защищенного распределения, уничтожения ключевой информации, а также механизмы шифрования, и формирования электронной цифровой подписи. Данные механизмы должны функционировать в соответствии с сертифицированными алгоритмами.

4.3. Политика и цели безопасности для среды функционирования АИС

Среда функционирования АИС должна обеспечить следование приведенным ниже правилам безопасности:

1. Должна быть обеспечена инженерно-техническая укреплённость объектов размещения системы обработки, хранения и передачи информации, содержащей сведения о персональных данных.

2. Объекты размещения системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, должны быть оборудованы системой охранной сигнализации.
3. Должна быть исключена возможность несанкционированного физического доступа к программно-аппаратным элементам системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, со стороны посторонних лиц.
4. На объектах системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, должно быть обеспечено наличие и надлежащее использование средств антивирусной защиты, сертифицированных по требованиям безопасности. Должно быть обеспечено регулярное обновление антивирусных баз.
5. Объекты системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, должно быть подключены к внешним вычислительным сетям общего пользования с использованием надлежащих средств межсетевого экранирования, сертифицированных по требованиям безопасности.
6. На объектах системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, должно быть обеспечено отсутствие нештатных программных средств, не имеющих отношение к процессу функционирования образовательного учреждения.
7. Должны быть обеспечены установка, конфигурирование и управление программно-аппаратными средствами АИС в соответствии с руководствами и согласно оцененным конфигурациям.
8. Персонал, ответственный за администрирование АИС, должен быть благонадежным и компетентным, и руководствоваться в своей деятельности соответствующей документацией.
9. Уполномоченные на работу с АИС операторы должны быть благонадежными, руководствоваться в своей работе эксплуатационной документацией на АИС, а их совместные действия должны быть направлены исключительно на выполнение своих функциональных обязанностей.

ПРИНЯТО

На заседании
Педагогического совета
31.08.2015 г
Протокол №1

УТВЕРЖДАЮ
Директор ГБС(К)ОУ
школы – интернат № 7
станицы Казанской
_____ Д.Н. Агафонов
от «01» сентября 2015 года

Приложение № 7
к приказу №272 от 01.09.2015г.

Инструкция по организации парольной защиты
в АИС ГБС(К)ОУ школе – интернат № 7 станицы Казанской

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационной системе персональных данных (ИСПДн) ГБС(К)ОУ школы – интернат № 7 станицы Казанской (далее – Учреждение), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с идентификаторами и с личными паролями. Инструкция регламентирует организационно-техническое обеспечение генерации, смены и прекращения действия паролей в информационной системы персональных данных, а также контроль за действиями пользователей системы при работе с паролями. Настоящая инструкция оперирует следующими основными понятиями:

- **Идентификация** - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.
- **ИСПДн –** информационная система персональных данных.
- **Компрометация**- факт доступа постороннего лица к защищаемой информации, а также подозрение на него.
- **Объект доступа** - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.
- **Пароль** – уникальный признак субъекта доступа, который является его (субъекта) секретом.

- **Правила доступа** - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.
- **Субъект доступа** - лицо или процесс, действия которого регламентируются правилами разграничения доступа.
- **Несанкционированный доступ** - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или АС.

1. Правила генерации паролей

1.1 Персональные пароли должны генерироваться специальными программными средствами административной службы.

1.2 Длина пароля должна быть не менее 8 символов.

1.3 В составе пароля должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы.

1.4 Пароль не должен включать в себя:

- легко вычисляемые сочетания символов;
- клавиатурные последовательности символов и знаков;
- общепринятые сокращения;
- аббревиатуры;
- номера телефонов, автомобилей;
- прочие сочетания букв и знаков, ассоциируемые с пользователем;
- при смене пароля новое сочетание символов должно отличаться от предыдущего не менее чем на 2 символа.

1.5 Допускается использование единого пароля для доступа субъекта доступа к различным информационным ресурсам одной ИСПДн объекта образования.

2. Порядок смены паролей

2.1 Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одно раза в месяц.

2.2 Полная внеплановая смена паролей всех пользователей должна производиться случае прекращения полномочий администраторов средств защиты или других сотрудников, которым по роду службы были предоставлены полномочия по управлению парольной зашитой.

2.3 Полная внеплановая смена паролей должна производиться в случае компрометации личного пароля одного из администраторов ИСПДн.

2.4 В случае компрометации личного пароля пользователя надлежит немедленно ограничить доступ к информации с данной учетной записи, до момента вступления в силу новой учетной записи пользователя или пароля.

3. Обязанности пользователей при работе с парольной защитой

3.1 При работе с парольной защитой пользователям запрещается:

- разглашать кому-либо персональный пароль и прочие идентифицирующие сведения;
- предоставлять доступ от своей учетной записи к информации, хранящейся в ИСПДн посторонним лицам;
- записывать пароли на бумаге, файле, электронных и прочих

носителях информации, в том числе и на предметах.

3.2 Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе.

3.3 При вводе пароля пользователь обязан исключить возможность его перехвата сторонними лицами и техническими средствами.

4. Случаи компрометации паролей

4.1 Под компрометацией следует понимать:

- физическая утеря носителя с информацией;
- передача идентификационной информации по открытым каналам связи;
- проникновение постороннего лица в помещение физического хранения носителя парольной информации или алгоритма или подозрение на него (срабатывание сигнализации, повреждение устройств контроля НСД (слепков печатей), повреждение замков и т. п.);
- визуальный осмотр носителя идентификационной информации посторонним лицом;
- перехват пароля при распределении идентификаторов;
- сознательная передача информации постороннему лицу.

4.2 Действия при компрометации пароля:

- скомпрометированный пароль сразу же выводится из действия, взамен его вводятся запасной или новый пароль;
- о компрометации немедленно оповещаются все участники обмена информацией. Пароль вносится в специальные списки, содержащие скомпрометированные пароли и учетные записи.

5. Ответственность пользователей при работе с парольной защитой

5.1 Повседневный контроль за действиями сотрудников Учреждения при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на ответственного за систему защиты информации в информационной системе персональных данных.

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

5.3 Ответственность за организацию парольной защиты возлагается на ответственного за систему защиты информации в информационной системе персональных данных.

5.4 Ответственность в случае несвоевременного уведомлении ответственного за систему защиты информации в информационной системе персональных данных о случаях утери, кражи, взлома или компрометации паролей возлагается на владельца взломанной учетной записи.

ПРИНЯТО

На заседании
Педагогического совета
31.08.2015 г
Протокол №1

УТВЕРЖДАЮ
Директор ГБС(К)ОУ
школы – интернат № 7
станицы Казанской
_____ Д.Н. Агафонов
от «01» сентября 2015 года

Приложение № 8
к приказу №172 от 01.09.2015г.

Инструкция
по организации антивирусной защиты в школе

1. Общее положение.

1.1. Директор Школы назначает лицо, ответственное за антивирусную защиту. В противном случае ответственность за обеспечение антивирусной защиты несет заместитель директора школы.
1.2. В школе может использоваться только лицензионное антивирусное программное обеспечение.
1.3. 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 исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).
1.4. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.
1.5. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.
1.6. Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения должен регистрироваться в специальном журнале за подписью лица, ответственного за антивирусную защиту.

2. Требования к проведению мероприятий по антивирусной защите.

2.1 . Ежедневно в начале работы при загрузке компьютера (для серверов ЛВС – при перезапуске) в автоматическом режиме должно выполняться обновление антивирусных баз и проводиться антивирусный контроль всех дисков и файлов персонального компьютера.

2.2 . Периодические проверки электронных архивов должны проводиться не реже одного раза в неделю.

2.3 . Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

- Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), должна быть выполнена антивирусная проверка: на серверах и персональных компьютерах образовательного учреждения. Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения должен регистрироваться в специальном журнале за подписью лица, установившего (изменившего) программное обеспечение, и лица, его контролировавшего.
- 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.).

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

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение информационной безопасности в школе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов;

3. Ответственность

Ответственность за организацию антивирусной защиты возлагается на заместителя директора по АХЧ или лицо, назначенное директором школы.

Ответственность за проведение мероприятий антивирусного контроля в школе и соблюдение требований настоящей Инструкции возлагается на ответственного за обеспечение антивирусной защиты.

Периодический контроль за состоянием антивирусной защиты в школе осуществляется заместителем директора по АХЧ.

ПРИНЯТО

На заседании
Педагогического совета
31.08.2015 г
Протокол №1

УТВЕРЖДАЮ
Директор ГБС(К)ОУ
школы – интернат № 7
станицы Казанской
_____ Д.Н. Агафонов
от «01» сентября 2015 года

Приложение № 9
к приказу № 272 от 01.09.2015г.

ИНСТРУКЦИЯ № ____

по резервированию и восстановлению работоспособности технических средств и программного обеспечения, баз данных, средств защиты информации и средств криптографической защиты информации информационной системе персональных данных в ГБС(К)ОУ школе - интернате № 7 станицы Казанской

1. Общие положения

1.1. Настоящая инструкция (далее – Инструкция) по резервирования и восстановления работоспособности технических средств (далее – ТС), программного обеспечения (далее – ПО), баз данных (далее – БД), средств защиты информации (далее – СЗИ)и средств криптографической защиты информации (далее – СКЗИ) информационной системы персональных данных (далее – АИС) в ГБС(К)ОУ школе – интернате № 7 станицы Казанской (далее – Школа) определяет действия, связанные с функционированием технических и программных средств АИС и системы защиты персональных данных (далее – СЗПДн).

1.2. Настоящая инструкция разработана в соответствии с руководящими и нормативными документами регуляторов Российской Федерации в области защиты персональных данных.

1.3. Целью данной инструкции является превентивная защита элементов АИС и СЗПДн от предотвращения потери защищаемой информации.

1.4. Задачами данной инструкции являются:

- определение мер защиты от потери информации;
- определение действий восстановления технических и программных средств АИС и СЗПДн в случае потери информации.

1.5. Действие настоящей инструкции распространяется на всех пользователей, имеющих доступ к ресурсам АИС, в том числе на ответственного за обеспечение безопасности персональных данных

информационных систем персональных данных Школы и администратора АИС (далее – администратор системы), имеющих доступ к техническим и программным средствам СЗПДн в рамках своих полномочий, при возникновении аварийных ситуаций, в том числе:
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

1.6. Пользователем АИС (далее – Пользователь) является сотрудник Хлыстова Т.В., участвующий в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки персональных данных (далее – ПДн) и имеющий доступ к аппаратным средствам, программному обеспечению, данным и СЗИ АИС.

1.7. Под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов АИС или СЗПДн, предоставляемых пользователям, а также потерей защищаемой информации.

2. Порядок реагирования на инцидент

2.1. Происшествие, вызывающее инцидент, может произойти:
- в результате непреднамеренных действий пользователей;
- в результате преднамеренных действий пользователей и третьих лиц;
- в результате нарушения правил эксплуатации технических средств АИС и СЗПДн;
- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.2. Все действия в процессе реагирования на Инцидент должны документироваться ответственным за обеспечение безопасности персональных данных информационных систем персональных данных Школы и администратором системы в «Журнал учета событий информационной безопасности».

2.3. В кратчайшие сроки, не превышающие одного рабочего дня ответственный за обеспечение безопасности персональных данных информационных систем персональных данных _____ и администратор системы предпринимают меры по восстановлению работоспособности.

2.4. Предпринимаемые меры, по возможности, согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена с целью получения высококвалифицированной консультации в кратчайшие сроки.

3. Технические меры

3.1. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства

и системы, используемые для предотвращения возникновения Инцидентов, такие как:
- системы жизнеобеспечения АИС ;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

3.2. Системы жизнеобеспечения АИС включают:
- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

3.3. Все критичные помещения Школы (помещения, в которых размещаются элементы АИС и СЗПДн) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

3.4. Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств АИС в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

3.5. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы АИС и СЗПДн, сетевое и коммуникационное оборудование, а также наиболее критичные АРМ должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:
- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- дублированные системы электропитания в устройствах (серверы, активное сетевое оборудование и т. д.);
- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы.

3.6. Системы обеспечения отказоустойчивости:
- кластеризация;
- технология RAID.

3.7. Для обеспечения отказоустойчивости критичных компонентов АИС при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации.

3.8. Для наиболее критичных компонентов АИС должны использоваться территориально удаленные системы кластеров.

3.9. Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

3.10. Система резервного копирования и хранения данных должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

4. Организационные меры

4.1. Резервное копирование и хранение данных должно осуществлять на периодической основе:
- для обрабатываемых ПДн – согласно инструкции по обеспечению безопасности ПДн;
- для технологической информации – не реже раза в месяц;
- эталонные копии программного обеспечения (ОС, штатное и специальное ПО, программные СЗИ), с которых осуществляется их установка на элементы АИС – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

4.2. Данные о проведении процедуры резервного копирования должны отражаться в специально созданном журнале учета.

4.3. Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

4.4. Носители должны храниться в несгораемом шкафу или помещении оборудованном системой пожаротушения.

4.5. Носители должны храниться не менее года для возможности восстановления данных.