УПРАВЛЕНИЕ ОБРАЗОВАНИЯ АДМИНИСТРАЦИИ ВЕЙДЕЛЕВСКОГО РАЙОНА

ПРИКАЗ

от 3 июня 2013 года № 325

О политике информационной безопасности
управления образования администрации Вейделевского района

В целях обеспечения безопасности информации в соответствии с Федеральным законом от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации» **п р и к а з ы в а ю :**

1. Утвердить политику информационной безопасности управления образования администрации Вейделевского района (далее-Политика) (приложение №1).

2. Утвердить Инструкцию ответственного за обеспечение информационной безопасности персональных данных в управлении образования администрации Вейделевского района (приложение №2).

3. Утвердить Инструкцию администратора безопасности информации в автоматизированных системах объектов информатизации управления образования администрации Вейделевского района (приложение №3).

4. Утвердить Инструкцию пользователя локальной вычислительной сети управления образования администрации Вейделевского района (приложение №4).

5. Утвердить Порядок использования (подключения) внешних USB-совместимых устройств (приложение №5).

6. Утвердить Порядок резервного копирования информации и данных автоматизированных систем управления образования администрации Вейделевского района (приложение №6).

7. Рекомендовать МОУ ДОД «Вейделевская ДЮСШ» (Вдовенко А.В.), МОУ ДОД Вейделевская РСЮН (Данченко Ю.В.), МОУ «ДДТ»

(Звычайная Г.А.), МУ «МЦОКО» (Лазебная О.П.), руководителям общеобразовательных учреждений разработать Политику информационной безопасности в соответствии с данным приказом.

8. Контроль за исполнением приказа оставляю за собой.

Начальник
управления образования

Решетникова В.С.

Приложение №1
Утверждена
приказом управления
образования администрации
Вейделевского района
«3» июня 2013 года № 325

Политика информационной безопасности управления образования администрации Вейделевского района

1. Общие положения

1.1.Политика информационной безопасности управления образования администрации Вейделевского района (далее – управления) определяет цели и задачи системы обеспечения информационной безопасности) и устанавливает совокупность правил, процедур, практических приемов, требований и руководящих принципов в области информационной безопасности (далее-ИБ), которыми руководствуются работники управления при осуществлении своей деятельности.

1.2.Основной целью Политики информационной безопасности управления является защита информации управления при осуществлении уставной деятельности, которая предусматривает принятие необходимых мер в целях защиты информации от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных в управлении.

1.3.Политика информационной безопасности разработана в соответствии с: Федеральным законом от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации», Федеральным закон от 27 июля 2006г. № 152-ФЗ «О персональных данных», Федеральным закон от 10 января 2002г. № 1-ФЗ «Об электронной цифровой подписи», Указом Президента Российской Федерации от 6 марта 1997г. № 188 «Об утверждении Перечня сведений конфиденциального характера», Постановлением Правительства РФ №781 от 17.11.07г. «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Постановление Правительства РФ №687 от 15.09.08г. «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» а также рядом иных нормативных правовых актов в сфере защиты информации.

1.4.Выполнение требований Политики ИБ является обязательным для всех структурных подразделений управления.

1.5.Ответственность за соблюдение информационной безопасности несет каждый сотрудник управления. На лиц, работающих в управлении по

договорам гражданско-правового характера, положения настоящей политики распространяются в случае, если это обусловлено в таком договоре.

2. Цель и задачи политики информационной безопасности

2.1.Основными целями политики ИБ являются:

-сохранение конфиденциальности критичных информационных ресурсов;

-обеспечение непрерывности доступа к информационным ресурсам управления;

-защита целостности информации с целью поддержания возможности управления по оказанию услуг высокого качества и принятию эффективных управленческих решений;

-повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами управления;

-определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности в управлении.

-повышение уровня эффективности, непрерывности, контролируемости мер по защите от реальных угроз ИБ;

-предотвращение и/или снижение ущерба от инцидентов ИБ.

2.2.Основными задачами политики ИБ являются:

-разработка требований по обеспечению ИБ;

-контроль выполнения установленных требований по обеспечению ИБ;

-повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению и поддержанию ИБ;

-разработка нормативных документов для обеспечения ИБ управления;

-выявление, оценка, прогнозирование и предотвращение реализации угроз ИБ управления;

-организация антивирусной защиты информационных ресурсов управления;

-защита информации управления от несанкционированного доступа (далее-НСД) и утечки по техническим каналам связи;

- организация периодической проверки соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки начальнику управления.

3. Концептуальная схема обеспечения информационной безопасности

3.1.Политика ИБ управления направлена на защиту информационных ресурсов (активов) от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий сотрудников управления, технических сбоев автоматизированных систем, неправильных технологических и организационных решений в процессах поиска, сбора

хранения, обработки, предоставления и распространения информации и обеспечение эффективного и бесперебойного процесса деятельности.

3.2.Наибольшими возможностями для нанесения ущерба обладает собственный персонал управления. Риск аварий и технических сбоев в автоматизированных системах определяется состоянием аппаратного обеспечения, надежностью систем энергоснабжения и телекоммуникаций, квалификацией сотрудников и их способностью к адекватным и незамедлительным действиям в нештатной ситуации.

3.3.Стратегия обеспечения ИБ управления заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий сотрудников управления.

4. Основные принципы обеспечения информационной безопасности

4.1.Основными принципами обеспечения ИБ :

-постоянный и всесторонний анализ автоматизированных систем и трудового процесса с целью выявления уязвимости информационных активов управления;

-своевременное обнаружение проблем, потенциально способных повлиять на ИБ управления, корректировка моделей угроз и нарушителя;

-разработка и внедрение защитных мер;

-контроль эффективности принимаемых защитных мер;

-персонификация и разделение ролей и ответственности между сотрудниками управления за обеспечение ИБ управления исходит из принципа персональной и единоличной ответственности за совершаемые операции.

5.Объекты защиты

5.1.Объектами защиты с точки зрения ИБ в управлении являются:

-информационный процесс профессиональной деятельности;

-информационные активы управления.

5.2.Защищаемая информация делится на следующие виды:

- информация по финансово-экономической деятельности управления;

- персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное,

имущественное положение, образование, профессия, доходы, другая информация;

- другая информация, не относящаяся ни к одному из указанных выше видов, которая отмечена грифом «Для служебного пользования» или «Конфиденциально».

6. Требования по информационной безопасности

6.1.В отношении всех собственных информационных активов управления, активов, находящихся под контролем управления, а также активов, используемых для получения доступа к инфраструктуре управления, должна быть определена ответственность соответствующего сотрудника управления.

Информация о смене владельцев активов, их распределении, изменениях в конфигурации и использовании за пределами управления должна доводиться до сведения начальника управления.

6.2. Все работы в пределах управления должны выполняться в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию в управлении.

6.3.Вынос в здание и помещения управления личных портативных компьютеров и внешних носителей информации (диски, дискеты, флэш-карты и т.п.), а также вынос их за пределы управления производится только при согласовании с администратором ЛВС.

6.4.Все данные (конфиденциальные или строго конфиденциальные), составляющие тайну управления и хранящиеся на жестких дисках портативных компьютеров, должны быть зашифрованы.

6.5.Руководители подразделений должны периодически пересматривать права доступа своих сотрудников и других пользователей к соответствующим информационным ресурсам.

6.6.В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в систему должен осуществляться с использованием уникального имени пользователя и пароля.

6.7.Пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким.

6.8.В процессе своей работы сотрудники обязаны постоянно использовать режим "Экранной заставки" с парольной защитой. Рекомендуется устанавливать максимальное время "простоя" компьютера до появления экранной заставки не дольше 15 минут.

6.9.Каждый сотрудник обязан немедленно уведомить администратора ЛВС обо всех случаях предоставления доступа третьим лицам к ресурсам корпоративной сети.

Доступ третьих лиц к информационным системам управления должен быть обусловлен производственной необходимостью. В связи с этим, порядок доступа к информационным ресурсам управления должен быть четко определен, контролируем и защищен.

6.10.Сотрудникам, использующим в работе портативные компьютеры управления, может быть предоставлен удаленный доступ к сетевым ресурсам управления в соответствии с правами в корпоративной информационной системе.

6.11.Сотрудникам, работающим за пределами управления с использованием компьютера, не принадлежащего управлению, запрещено копирование данных на компьютер, с которого осуществляется удаленный доступ.

6.12.Сотрудники, имеющие право удаленного доступа к информационным ресурсам управления, должны соблюдать требование, исключающее одновременное подключение их компьютера к сети управления и к каким-либо другим сетям, не принадлежащим управления.

6.13.Все компьютеры, подключаемые посредством удаленного доступа к информационной сети управления, должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления.

6.14. Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.

Рекомендованные правила:

- сотрудникам управления разрешается использовать сеть Интернет только в служебных целях;

- запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию сексуального характера, пропаганду расовой ненависти, комментарии по поводу различия/превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности;

- сотрудники управления не должны использовать сеть Интернет для хранения корпоративных данных;

- работа сотрудников управления с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации управления в сеть Интернет;

- сотрудникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем управлению;

- сотрудники управления перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;

- запрещен доступ в Интернет через сеть управления для всех лиц, не являющихся сотрудниками управления, включая членов семьи сотрудников управления.

6.15.Администратор ЛВС имеет право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

6.16. Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация управления.

6.17.Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит администратор ЛВС.

6.18.Все компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (например, принтеры и сканеры), аксессуары (манипуляторы типа "мышь", шаровые манипуляторы, дисководы для CD-дисков), коммуникационное оборудование (например, факс-модемы, сетевые адаптеры и концентраторы), для целей настоящей политики вместе именуются "компьютерное оборудование". Компьютерное оборудование, предоставленное управлением, является ее собственностью и предназначено для использования исключительно в производственных целях.

6.19.Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности.

6.20.Все компьютеры должны защищаться паролем при загрузке системы, активации по горячей клавиши и после выхода из режима "Экранной заставки". Для установки режимов защиты пользователь должен обратиться к администратору ЛВС. Данные не должны быть скомпрометированы в случае халатности или небрежности приведшей к потере оборудования. Перед утилизацией все компоненты оборудования, в состав которых входят носители данных (включая жесткие диски), необходимо проверять, чтобы убедиться в отсутствии на них конфиденциальных данных и лицензионных продуктов. Должна выполняться процедура форматирования носителей информации, исключающая возможность восстановления данных.

6.20.При записи какой-либо информации на носитель для передачи субъектам, участвующим в информационном обмене, необходимо убедиться в том, что носитель чист, то есть не содержит никаких иных данных. Простое переформатирование носителя не дает гарантии полного удаления записанной на нем информации.

6.21.Порты передачи данных, в том числе FDD и CD дисководы в стационарных компьютерах сотрудников управления блокируются, за исключением тех случаев, когда сотрудником получено разрешение на запись администратора ЛВС.

6.22.Все программное обеспечение, установленное на предоставленном управлением компьютерном оборудовании, является собственностью управления и должно использоваться исключительно в производственных целях.

6.23.Сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности. Если в ходе выполнения технического обслуживания будет обнаружено не разрешенное к установке программное обеспечение, оно будет удалено, а сообщение о нарушении будет направлено непосредственному руководителю сотрудника и начальнику управления.

6.24.На всех портативных компьютерах должны быть установлены программы, необходимые для обеспечения защиты информации:

- персональный межсетевой экран;
- антивирусное программное обеспечение;
- программное обеспечение шифрования жестких дисков;
- программное обеспечение шифрования почтовых сообщений.

6.25.Все компьютеры, подключенные к корпоративной сети, должны быть оснащены системой антивирусной защиты, утвержденной администратором ЛВС.

6.26.Сотрудники управления не должны:

- блокировать антивирусное программное обеспечение;
- устанавливать другое антивирусное программное обеспечение;
- изменять настройки и конфигурацию антивирусного программного обеспечения.

6.27.Электронные сообщения должны строго соответствовать стандартам в области деловой этики. Использование электронной почты в личных целях не допускается. Сотрудникам запрещается направлять конфиденциальную информацию управления по электронной почте без использования систем шифрования. Строго конфиденциальная информация управления, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

6.28.Использование сотрудниками управления публичных почтовых ящиков электронной почты осуществляется только при согласовании с ответственным за обеспечение безопасности информации ЛВС при условии применения механизмов шифрования.

6.29.Сотрудники управления для обмена документами должны использовать только свой официальный адрес электронной почты.

6.30.Сообщения, пересылаемые по электронной почте, представляют собой постоянно используемый инструмент для электронных коммуникаций, имеющих тот же статус, что и письма и факсимильные сообщения. Электронные сообщения подлежат такому же утверждению и хранению, что и прочие средства письменных коммуникаций.

В целях предотвращения ошибок при отправке сообщений пользователи перед отправкой должны внимательно проверить правильность написания имен и адресов получателей. В случае получения сообщения лицом, вниманию которого это сообщение не предназначается, такое сообщение необходимо переправить непосредственному получателю. Если полученная таким образом информация носит конфиденциальный характер, об этом следует незамедлительно проинформировать администратора ЛВС. Отправитель электронного сообщения, документа или лицо, которое его переадресовывает, должен указать свое имя и фамилию, служебный адрес и тему сообщения.

6.31.Не допускается при использования электронной почты:

- рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;

- рассылка рекламных материалов;

- подписка на рассылку, участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;

- поиск и чтение сообщений, направленных другим лицам (независимо от способа их хранения);

- пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным или способствует поведению, которое может рассматриваться как уголовное преступление или административный проступок либо приводит к возникновению гражданско-правовой ответственности, беспорядков или противоречит стандартам в области этики.

6.32. Объем пересылаемого сообщения по электронной почте не должен превышать 2 Мбайт.

6.33.Все пользователи должны быть осведомлены о своей обязанности сообщать об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

6.34.В случае кражи переносного компьютера следует незамедлительно сообщить администратору ЛВС.

6.35.Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан:

-проинформировать администратора ЛВС;

- не пользоваться и не выключать зараженный компьютер;

-не подсоединять этот компьютер к компьютерной сети управления до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование администратором ЛВС.

6.35.Конфиденциальные встречи (заседания) должны проходить только в защищенных техническими средствами информационной безопасности помещениях.

6.36.Перечень помещений с техническими средствами информационной безопасности утверждается начальником управления.

6.37.Участникам заседаний запрещается входить в помещения с записывающей аудио/видео аппаратурой, фотоаппаратами, радиотелефонами и мобильными телефонами без предварительного согласования с администратором ЛВС.

6.38.Аудио/видео запись, фотографирование во время конфиденциальных заседаний может вести только сотрудник управления, который отвечает за подготовку заседания, после получения письменного разрешения руководителя группы организации встречи.

6.39.Доступ участников конфиденциального заседания в помещение для его проведения осуществляется на основании утвержденного перечня, контроль за которым ведет лицо, отвечающее за организацию встречи.

6.40.Сотрудникам управления запрещается:

- нарушать информационную безопасность и работу сети управления;
- сканировать порты или систему безопасности;
- контролировать работу сети с перехватом данных;
- получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;
- использовать любые программы, скрипты, команды или передавать сообщения с целью вмешаться в работу или отключить пользователя оконечного устройства;
- передавать информацию о сотрудниках или списки сотрудников управления посторонним лицам;
- создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

6.41.Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях.

6.42.Необходимо регулярно делать резервные копии всех основных служебных данных и программного обеспечения.

6.43.Только администратор ЛВС на основании заявок руководителей подразделений может создавать и удалять совместно используемые сетевые ресурсы и папки общего пользования, а также управлять полномочиями доступа к ним.

6.44.Сотрудники имеют право создавать, модифицировать и удалять файлы и директории в совместно используемых сетевых ресурсах только на тех участках, которые выделены лично для них, для их рабочих групп или к которым они имеют санкционированный доступ.

6.45.Все заявки на проведение технического обслуживания компьютеров должны направляться администратору ЛВС.

6.47.Все операционные процедуры и процедуры внесения изменений в информационные системы и сервисы должны быть документированы, и согласованны с администратором ЛВС.

7.Управление информационной безопасностью

7.1.Управление ИБ управления включает в себя:

-разработку и поддержание в актуальном состоянии Политики информационной безопасности;

-разработку и поддержание в актуальном состоянии нормативно-методических документов по обеспечению ИБ ;

-обеспечение бесперебойного функционирования комплекса средств ИБ;

-осуществление контроля (мониторинга) функционирования системы ИБ;

-оценку рисков, связанных с нарушениями ИБ.

8. Реализация политики информационной безопасности

8.1. Реализация Политики ИБ управления осуществляется на основании документов, регламентирующих отдельные процедуры и процессы профессиональной деятельности в управлении.

9.Порядок внесения изменений и дополнений в политику информационной безопасности

9.1.Внесение изменений и дополнений в Политику информационной безопасности производится не реже одного раза в три года с целью приведения в соответствие определенных Политикой защитных мер реальным жизненным условиям и текущим требованиям к защите информации.

10.Контроль за соблюдением политики информационной безопасности

10.1.Текущий контроль за соблюдением выполнения требований Политики информационной безопасности управления возлагается на сотрудника, назначенного приказом управления образования.

10.2.Начальник управления образования на регулярной основе рассматривает реализацию и соблюдение отдельных положений Политики информационной безопасности, а также осуществляет последующий контроль за соблюдением ее требований.

Приложение №2
Утверждена
приказом управления
образования администрации
Вейделевского района
«3» июня 2013 г.
№ 325

ИНСТРУКЦИЯ

ответственного за обеспечение безопасности персональных данных в управлении образования администрации Вейделевского района Белгородской области

1. Общие положения

1.1. Сотрудник, ответственный за обеспечение безопасности персональных данных в управлении образования администрации Вейделевского района Белгородской области (далее – управление образования) назначается приказом управления образования из числа сотрудников управления образования.

1.2. Настоящая должностная инструкция определяет функции, обязанности, права, ответственность сотрудника, ответственного за обеспечение безопасности персональных данных в управлении образования.

2.Функции сотрудника, ответственного за обеспечение безопасности персональных данных в управлении образования

2.1.Контроль соблюдения сотрудниками, обрабатывающими персональные данные, правил обеспечения безопасности персональных данных;

2.2.Подготовка документов по защите персональных данных.

3.Обязанности сотрудника, ответственного за обеспечение безопасности персональных данных в управлении образования

Сотрудник, ответственный за обеспечение безопасности персональных данных в управлении образования, обязан:

3.1. обеспечивать выполнение режимных и организационных мероприятий на месте эксплуатации автоматизированных систем, а также следить за выполнением требований по условиям размещения средств вычислительной техники и их сохранность;

3.2. проводить инструктаж и консультации пользователей ПВЭМ по соблюдению режима конфиденциальности;

3.3. организовывать периодический контроль пользователей по соблюдению ими режима конфиденциальности, правил работы со съемными машинными носителями информации, выполнению организационных мер по защите информации, а также принимать участие в проведении проверок уполномоченными структурами;

3.4. взаимодействовать с администратором безопасности по вопросам обеспечения и выполнения требований обработки персональных данных;

3.5. организовывать работы по плановому контролю работоспособности технических средств защиты персональных данных, охраны объекта, средств защиты информации от несанкционированного доступа;

3.6. знать перечень установленных технических средств, входящих в состав информационных систем, и перечень задач, решаемых с их использованием.

3.7. контролировать целостность печатей (логотипов) на устройствах защищенных (допущенных к обработке персональных данных) компьютеров и серверов;

3.8. обеспечивать соблюдение сотрудниками утвержденного порядка проведения работ по установке и модернизации аппаратных и программных средств компьютеров и серверов из состава информационных систем.

3.9. хранить технические паспорта защищенных компьютеров и серверов, контролировать их соответствие реальным конфигурациям и вести учет изменений их аппаратно-программной конфигурации (заявки, на основании которых были произведены данные изменения);

3.10. осуществлять контроль за порядком учета, создания, хранения и использования резервных копий и машинных (выходных) документов, содержащих персональные данные;

3.11. контролировать порядок использования и обеспечения сохранности персональных устройств идентификации пользователей;

3.12. при выявлении возможных каналов неправомерного вмешательства в процесс функционирования информационных систем и осуществления несанкционированного доступа к персональным данным и техническим средствам из состава информационных систем, сообщать о них начальнику управлении образования;

3.13. инструктировать сотрудников по вопросам обеспечения информационной безопасности и правилам работы, с применяемыми средствами защиты информации.

4. Права сотрудника, ответственного за обеспечение безопасности персональных данных в управлении образования

Сотрудник, ответственный за обеспечение безопасности персональных данных в управлении образования, имеет право:

4.1. требовать от всех пользователей информационных систем персональных данных выполнения установленной технологии обработки

персональных данных, инструкций и других нормативных правовых документов по обеспечению безопасности персональных данных;

4.2. участвовать в разработке мероприятий по совершенствованию безопасности персональных данных;

4.3. инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемых персональных данных и технических средств из состава информационных систем;

4.4. обращаться к начальнику управления образования с предложением о приостановке процесса обработки персональных данных или отстранению от работы пользователя в случаях нарушения установленной технологии обработки персональных данных или нарушения режима конфиденциальности.

4.5. подавать свои предложения по совершенствованию организационных, технологических и технических мер защиты персональных данных.

5. Ответственность

Сотрудник, ответственный за обеспечение безопасности персональных данных в управлении образования, несет ответственность в соответствии с законодательством РФ за:

5.1. несоблюдение требований нормативных документов и инструкций, определяющих порядок обработки персональных данных;

5.2. разглашение персональных данных, ставших ему известными в связи с исполнением должностных обязанностей;

5.3. сохранность персональных данных.

Приложение №3
Утверждена
приказом управления
образования администрации
Вейделевского района
«3» июня 2013года
№ 325

ИНСТРУКЦИЯ
администратора безопасности информации в автоматизированных системах объектов информатизации управления образования администрации Вейделевского района Белгородской области

1. Общие положения

1.1.Администратор безопасности информации в автоматизированных системах объектов информатизации (далее - администратор безопасности информации) в управлении образования администрации Вейделевского района (далее – управление образования) назначается приказом управления образования из числа сотрудников управления образования.

1.2.Настоящая должностная инструкция определяет функции, обязанности, права, ответственность администратора безопасности информации в управлении образования.

2. Функции администратора безопасности информации

2.1.Контроль за выполнением требований действующих нормативных документов по вопросам обеспечения режима конфиденциальности, при проведении работ в автоматизированных системах (АС) информационных систем персональных данных (ИСПДн) управления (далее «АС ИСПДн»);

2.2.Настройка и сопровождение в процессе эксплуатации подсистемы управления доступом в «АС ИСПДн»;

2.3.Контроль доступа лиц в помещение «АС ИСПДн»;

2.4.Контроль за проведением периодической смены паролей для доступа пользователей в «АС ИСПДн»;

2.5.Настройка и сопровождение подсистемы регистрации и учета действий пользователей при работе в «АС ИСПДн»;

2.6.Сопровождение подсистемы обеспечения целостности информации в «АС ИСПДн»;

2.7.Анализ данных журналов аудита «АС ИСПДн» с целью выявления возможных нарушений требований защиты;

2.8.Оценка возможности и последствия внесения изменений в состав «АС ИСПДн» с учетом требований по защите, подготовка своих предложения;

2.9.Контроль физической сохранности средств и оборудования «АС ИСПДн»;

2.10.Своевременный анализ журналов учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений;

2.11.В период профилактических работ на рабочих станциях «АС ИСПДн» снятие при необходимости средства защиты информации с эксплуатации с обязательным обеспечением сохранности информации;

2.12.Периодически предоставлять сотруднику, ответственному за обеспечение безопасности персональных данных отчет о состоянии защиты «АС ИСПДн» и о нештатных ситуациях и допущенных пользователями нарушений установленных требований по защите информации.

3. Обязанности администратора безопасности информации

3.1.Администратор безопасности информации в управлении образования обязан:

-знать в совершенстве применяемые информационные технологии;

-знать права доступа пользователей по обработке, хранению и передаче защищаемой информации;

-обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в пределах возложенных функций;

-проводить инструктаж пользователей по правилам работы в «АС ИСПДн»;

-в случае отказа средств и систем защиты информации принимать меры по их восстановлению;

-докладывать сотруднику, ответственному за обеспечение безопасности персональных данных, о неправомерных действиях пользователя, приводящих к нарушению требований по защите информации;

-вести документацию в «АС ИСПДн» в соответствии с требованиями нормативных документов;

-настраивать только те параметры системы, которые определяют права доступа пользователей к информации;

-производить периодическое тестирование всех реализованных программно-техническими средствами функций и требований по обеспечению информационной безопасности;

-в соответствии с приказом управления образования и разрешительной системой доступа осуществлять добавление, блокирование, удаление и назначение прав доступа пользователям в системе;

-определить начальное значение паролей пользователя;

-восстанавливать настройки средств защиты информации при сбоях;

-хранить журналы аудита средств защиты информации на весь срок исковой давности действий и 5 лет после его окончания.

3.2.При выявлении факта несанкционированного доступа администратор безопасности информации в управлении образования обязан:

-блокировать доступ к конфиденциальной информации;

-проанализировать характер несанкционированного доступа;

-доложить ответственному за обеспечение безопасности персональных данных служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

-принять меры к защите от несанкционированного доступа;

-по решению ответственного за обеспечение безопасности персональных данных возобновить работу.

4.Права администратора безопасности информации

4.1.Администратор безопасности информации в управлении образования имеет право:

-участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа;

-требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;

-блокировать учетные записи пользователей, осуществивших несанкционированный доступ к защищаемым ресурсам;

-участвовать в любых проверках в «АС ИСПДн»;

-запрещать устанавливать на серверах и рабочих станциях нештатное программное и аппаратное обеспечение;

-вести контроль за процессом резервирования и дублирования важных ресурсов «АС ИСПДн»;

-участвовать в приемке новых программных средств;

-уточнять в установленном порядке обязанности пользователей «АС ИСПДн» по поддержанию уровня защиты;

-вносить предложения по совершенствованию уровня защиты «АС ИСПДн»;

-запрещать и немедленно блокировать попытки изменения программно-аппаратной среды «АС ИСПДн» без согласования порядка ввода новых (отремонтированных) технических и программных средств и средств защиты информации;

-запрещать и немедленно блокировать применение пользователям «АС ИСПДн» программ, с помощью которых возможны факты несанкционированного доступа к ресурсам «АС ИСПДн»;

-незамедлительно докладывать ответственному за обеспечение безопасности персональных данных обо всех попытках нарушения защиты «АС ИСПДн»;

-анализировать состояние защиты «АС ИСПДн» и ее отдельных подсистем;

-контролировать состояние средств и систем защиты информации и их параметры и критерии;

-контролировать правильность применения пользователями средств защиты информации;

-оказывать помощь пользователям в части применения средств защиты;

-не допускать установку, использование, хранение и размножение в «АС ИСПДн» программных средств, не связанных с выполнением функциональных задач;

-осуществлять контроль за соблюдением установленных правил и параметров регистрации и учета бумажных носителей информации;

-контролировать установленный порядок и правила антивирусной защиты информации;

-контролировать отсутствие на машинных носителях остаточной информации по окончании работы;

-не допускать к работе на рабочих станциях «АС ИСПДн» посторонних лиц.

5. Ответственность

5.1.Ответственность за сохранность конфиденциальной информации несет администратор безопасности информации, действия которого фиксируются в протоколах аудита.

5.2.Администратор безопасности информации несет ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования этих учетных записей.

5.3.При нарушениях администратором безопасности информации правил, связанных с информационной безопасностью, он несет ответственность, установленную действующим законодательством Российской Федерации.

Приложение №4
Утверждена
приказом управления
образования администрации
Вейделевского района
«3» июня 2013года
№ 325

ИНСТРУКЦИЯ
пользователя локальной вычислительной сети управления образования администрации Вейделевского района Белгородской области

1.Локальная вычислительная сеть (далее - ЛВС) управления образования администрации Вейделевского района Белгородской области (далее-управление) объединяет в единую информационную систему вычислительные ресурсы всех компьютеров и рабочих станций, использующихся в управлении.

2.С целью оперативного обеспечения сотрудников управления вычислительными и информационными ресурсами регламентом работ определен круглосуточный режим работы ЛВС, включая выходные и праздничные дни. В случае проведения плановых или профилактических работ администратор ЛВС своевременно оповещает заинтересованных об этом лиц.

3.Каждый сотрудник управления, допущенный к работе в информационной системе, является пользователем ЛВС. Все действия пользователей в ЛВС фиксируется многоуровневой системой аудита.

4.Пользователь получает от администратора безопасности ЛВС индивидуальную учетную запись и соответствующий ему уникальный пароль доступа к ЛВС.

Пароли входа в систему меняются администратором ЛВС с определенной периодичностью, о чём предварительно оповещаются пользователи.

Внеочередная смена пароля может произойти при потере информационного листа пароля, при переопределении прав доступа в сети в случае смены занимаемой должности (по ходатайству начальника отдела) и при несанкционированном доступе, отраженном в журнале аудита, в целях отключения данного пользователя от сети до выяснения обстоятельств. Для внеочередной смены пароля следует обратиться к администратору безопасности ЛВС. Если пользователь забыл свой пароль, необходимо получить его у администратора безопасности ЛВС.

Пароль доступа в ЛВС является конфиденциальной информацией, дающей возможность получения закрытой информации из ЛВС и должен сохраняться пользователем в полном секрете от остальных пользователей. Знать пароль не имеет прав никто, кроме его владельца и администратора

безопасности ЛВС. В случае если в результате утечки информации постороннее лицо получит несанкционированный доступ к информации, сведения о чём незамедлительно будут зафиксированы в протоколе сетевого аудита, полную ответственность за это будет нести владелец пароля, допустивший разглашения или утечку конфиденциальной информации. В случае непреднамеренного разглашения пароля пользователь обязан немедленно обратиться к администратору безопасности ЛВС с целью блокировки пароля, его аннулирования и получения нового.

Каждому паролю доступа к сети соответствует строго определенный список полномочий доступа владельца пароля к информации, ограниченные прав работы с информацией и пакетами прикладных программ. Изменение полномочий или расширение прав доступа пользователя к информации осуществляется по мотивированному письменному ходатайству начальника отдела, в котором работает пользователь, к ответственному за обеспечение безопасности. С целью предотвращения утечки информации каждый пользователь информационной системы управления обязан:

не допускать прямого или косвенного разглашения пароля доступа к информационной системе управления;

препятствовать попыткам посторонних лиц считать какую-либо информацию с экрана монитора;

не оставлять посторонних лиц без присмотра в помещении, где установлена вычислительная техника;

в случае длительного отсутствия в помещении предварительно выйти из пакета прикладных программ;

принять меры к неразглашению за пределами управления сведений о специфике используемых пакетов прикладных программ, информационной системе, топологии сети и т.д

Категорически запрещено считывание информации, копирование или запуск программ с носителей, посторонних лиц без предварительной проверки этой информации средствами антивирусной защиты.

6. С целью предотвращения отказов, сбоев и поломок оборудования каждый пользователь информационной системы управления при эксплуатации вычислительной техники обязан:

не допускать попадания влаги на поверхность компьютера, принтера, монитора или клавиатуры;

своевременно протирать экран монитора от загрязнения мягкой ветошью;

соблюдать правила техники безопасности;

с целью предотвращения падения оборудования следить за надёжной, устойчивой установкой на рабочем месте монитора и системного блока.

В случае выхода оборудования из строя или нестабильной работы следует немедленно обратиться к администратору безопасности ЛВС.

В управлении развернута система приема-передачи электронной почты.

По всем вопросам эксплуатации электронной почты следует обращаться к администратору безопасности ЛВС.

7. Пользователь ЛВС, совершивший действия, повлекшие нарушения работы информационной системы, несёт служебную, либо уголовную ответственность в соответствии со ст.ст. 272-274 Уголовного Кодекса Российской Федерации.

Приложение №5
Утвержден
приказом управления
образования администрации
Вейделевского района
«3» июня 2013 года
№325

Порядок
использования (подключения) внешних USB – совместимых устройств

Внешние USB-накопители, используемые в управлении образования администрации Вейделевского района должны быть идентифицированы и выданы под роспись пользователю информационной системы.

Запрещено подключение каких-либо неучтенных USB-совместимых устройств к автоматизированным рабочим местам, на которых осуществляется обработка персональных данных, либо сведения составляющие государственную тайну.

Подключение съемных носителей следует производить при включенном компьютере и загруженной операционной системой.

Если USB-накопитель в текущей сессии пользователя персонального компьютера будет использован только в «режиме чтения», то настоятельно рекомендуется, перед подключением USB-накопителя включить блокировку записи (если она предусмотрена конструкцией Вашего USB-устройства).

Запрещено извлекать USB-накопитель из персонального компьютера в момент обращения к нему, это может привести к потере данных и повреждению устройства. Если при попытке извлечь USB-накопитель через значок "Безопасное извлечение устройства" появляется диалоговое окно "Проблема при извлечении "Запоминающее устройство для USB": Устройство Универсальный том не может быть остановлено прямо сейчас. Попробуйте остановить его позже", значит открыты какие-то файлы с USB-накопителя. Закройте их и повторите попытку.

Для сохранности и целостности данных не рекомендуется открывать файлы с данными со сменных носителей.

Перед копированием файлов данных с внешних носителей настоятельно рекомендуется проверить носитель с помощью антивирусного сканера, установленного на персональном компьютере. Запрещается запускать или копировать с внешних носителей любые исполняемые файлы (приложения или командные файлы с расширениями exe, bat, com, cmd, inf, dll, scr) без согласования с администратором безопасности.

Запрещено подключение к персональным компьютерам, находящимся в информационной системе управления образования USB совместимых устройств, таких как: переносные жесткие диски, цифровые фотоаппараты,

телефоны и т.д. Подключение данных носителей возможно лишь под контролем администратора безопасности.

Приложение №6
Утвержден
приказом управления
образования администрации
Вейделевского района
«3» июня 2013 года
№ 325

Порядок
резервного копирования информации и данных автоматизированных систем управления образования администрации Вейделевского района Белгородской области

Резервное копирование информации автоматизированных систем управления образования администрации Вейделевского района Белгородской области (далее - управление) производится на основании следующих данных:

- состава и объема копируемых данных, необходимой периодичности проведения резервного копирования;
- максимального срока хранения резервных копий -1 месяц;
- хранения 3-х следующих архивов:

архив на 1-е число текущего месяца;
архив среда-четверг, либо пятница-суббота текущей недели;
архив сделанный в текущую ночь.

Для снижения совокупной нагрузки на информационную систему все операции по резервированию информации необходимо проводить в не рабочее время (с 0 часов до 5 часов). Существуют три набора резервных копий:

Месячный набор. Записывается информация на первое число текущего месяца. Срок хранения – месяц. Хранится на сервере резервного копирования.

Недельная копия. Записывается в ночь на среду и в ночь на субботу. Срок хранения – субботняя копия – до следующей среды, вторничная копия – до субботы. Хранится на сервере резервного копирования.

Ежедневная копия. Записывается ежесуточно, кроме ночи на среду и ночи на субботу. Срок хранения – сутки. Записывается на съёмный жёсткий диск. Съемный диск хранится в сейфе у администратора безопасности.

На основе анализа данных автоматизированных систем управления, возникает необходимость создания резервных копий следующей информации:

Информации, хранимой на файловом сервере управления:

Информации, хранимой непосредственно на персональных компьютерах в файловой системе - MS Windows.

Базы данных информационных систем 1С «Бухгалтерия» и Парус.

Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации. Для организации системы резервного копирования в управлении используется программное обеспечение «Мастер архивации и восстановления» (ntbackup.exe), которое является штатным средством резервного копирования для семейства операционных систем Microsoft Windows, а также обычное копирование данных на сервер резервного копирования. С целью оптимизации расходов на развёртывание системы резервного копирования, запись резервной копии осуществляется на жёсткий диск сервера резервного копирования.

С помощью указанного программного обеспечения выполняются такие действия, как задание режимов и составление расписания резервного копирования клиентов, осуществляются операции по загрузке и выгрузке носителей информации, проводится контроль за состоянием выполнения заданий, запускаются процедуры восстановления информации.

Резервное копирование баз данных информационных систем 1С «Бухгалтерия» и Парус, осуществляется средствами самой системы, с возможностью указания директории назначения на сервер резервного копирования управления. При этом указывается срок хранения информации и периодичность выполнения резервного копирования.

Любое восстановление информации, не вызванное необходимостью экстренного восстановления, связанной с потерей работоспособности информационной системы или ее компонентов, выполняется на основании заявки администратору ЛВС.