Управление образования
Администрации города Магнитогорска

Муниципальное общеобразовательное учреждение
«Гимназия № 53»

(МОУ «Гимназия №53»)

СОГЛАСОВАНО
Протоколом Педагогического совета
от 21.03.2013 № 2
РАССМОТРЕНО
На заседании Родительского комитета
Протокол № 1 от 22.01.2013

УТВЕРЖДЕНО
Приказом МОУ «Гимназия № 53»
№ 96 от 01.04.2013
Директор МОУ «Гимназия № 53»
_____ Ф.Н. Уразманова
«01» апреля 2013 г.

ПОЛИТИКА

«01» апреля 2013г.

г. Магнитогорск

Информационной безопасности при обработке персональных данных в Муниципальном общеобразовательном учреждении «Гимназия № 53»

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АВС	– антивирусные средства
АРМ	– автоматизированное рабочее место
ВТСС	– вспомогательные технические средства и системы
ИСПДн	– информационная система персональных данных
КЗ	– контролируемая зона
КИМ	– контрольно-измерительный материал
ЛВС	– локальная вычислительная сеть
МЭ	– межсетевой экран
НСД	– несанкционированный доступ
ОС	– операционная система
ПДн	– персональные данные
ПМВ	– программно-математическое воздействие
ПО	– программное обеспечение
ПЭМИН	– побочные электромагнитные излучения и наводки
САЗ	– система анализа защищенности
СЗИ	– средства защиты информации
СЗПДн	– система (подсистема) защиты персональных данных
СОВ	– система обнаружения вторжений
ТКУИ	– технические каналы утечки информации
УБПДн	– угрозы безопасности персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика информационной безопасности при обработке персональных данных (далее – Политика) в Муниципальном общеобразовательном учреждении «Гимназия № 53» (далее – «Гимназия») разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных. Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и других нормативных правовых документов Российской Федерации в области защиты ПДн.

1.2. В Политике определены требования к ИСПДн Гимназии к системе защиты, статус и обязанности сотрудников Гимназии по защите ПДн, степень их ответственности.

1.3. Целью настоящей Политики является обеспечение безопасности объектов защиты Гимназии от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).

1.4. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

1.5. Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн. Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

1.6. Состав объектов защиты представлен в Перечне персональных данных, обрабатываемых в информационных системах Гимназии.

2. ОБЛАСТЬ ДЕЙСТВИЯ ПОЛИТИКИ

2.1. Требования настоящей Политики распространяются на всех сотрудников Гимназии, а также сотрудников, работающих по договору в период государственной итоговой аттестации, контролирующих органов и лиц, осуществляющих обслуживание технических средств Гимназии.

2.2. Политика информационной безопасности затрагивает все виды деятельности Гимназии, касающиеся сбора, обработки, хранения, предоставления, распространения ПДн.

2.3. Предметом настоящей Политики являются:

– персональные данные, представленные в виде документированной информации на различного рода носителях, информационных массивов и баз данных, подлежащих защите в соответствии с законодательством Российской Федерации и внутренними нормативными актами Гимназии;

– средства и системы информатизации, программные средства, автоматизированные системы управления, технологические процессы, используемые для обработки ПДн.

2.4. Выполнение положений настоящей Политики информационной безопасности является обязательным для всех сотрудников Гимназии.

2.5. Взаимоотношения по использованию положений настоящего документа применительно к защите информации, находящейся в совместном ведении с другими организациями, регулируются на основании Постановления Правительства Российской Федерации «Об утверждении правил формирования и ведения федеральной информационной системы обеспечения проведения единого государственного экзамена и приема граждан в образовательные учреждения среднего профессионального образования и образователь-

ные учреждения высшего профессионального образования и региональных информационных систем обеспечения проведения единого государственного экзамена» от 27.01.2012 № 36.

3. СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Система защиты персональных данных в Гимназии (СЗПДн), строится на основании:

– федеральных законов, Указов Президента, Постановлений Правительства РФ, приказов и положениях ФСТЭК России, ФСБ России и других нормативно-правовых актов регулирующих область защиты информации; - перечня персональных данных, подлежащих защите;

– модели угроз безопасности персональных данных;

– перечня персональных данных, обрабатываемых в информационных системах Гимназии;

– акта классификации информационной системы персональных данных.

3.2. Система защиты ПДн Гимназии основывается:

– использовании ПДн только в соответствии с целями их обработки;

– регламентации порядка доступа к информационным ресурсам;

– определении прав доступа к ПДн их владельцами;

– применении сертифицированных ФСТЭК России и ФСБ России средств защиты информации.

3.3. Для обеспечения безопасности СЗПДн необходимо использовать следующие технические средства:

– антивирусные средства для рабочих станций пользователей и серверов;

– средства межсетевого экранирования;

– средства обнаружения вторжений;

– средства анализа защищенности;

– средства идентификации и аутентификации пользователей;

– средства физического разграничения доступа в защищаемые помещения;

– охранной сигнализации Гимназии;

– средства криптографической защиты информации;

– другие средства направленные на обеспечение информационной безопасности.

3.4. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Перечень технических средств и прикладного программного обеспечения ИСПДн и утверждены руководителем Гимназии или лицом, ответственным за обеспечение защиты ПДн.

4. МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Комплекс мер по защите информации в Гимназии включает в себя следующие мероприятия:

– назначение ролей и распределение ответственности;

– разработка, реализация, внедрение и контроль исполнения планов мероприятий и других документов по обеспечению информационной безопасности;

– аудит информационной безопасности.

4.2. Политика защиты ИСПДн Гимназии реализуется путем сочетания организационных и технических мер направленных на защиту ИСПДн.

К организационным мерам защиты ИСПДн относятся:

– управление персоналом;

– физическая защита объекта;

– поддержание работоспособности серверов, АРМ с ИСПДн;

– реагирование на нарушения режима безопасности;

– планирование восстановительных работ.

4.3. Реагирование на нарушения режима безопасности должно предусматривать набор оперативных мероприятий и инструкций, направленных на обнаружение и нейтрализацию угрозы.

4.4. Общее руководство информационной безопасностью осуществляет директор Гимназии.

5. ПОЛЬЗОВАТЕЛИ ИСПДН

5.1. Описание обязанностей всех сотрудников Гимназии при получении, передаче, хранении, обработке и защите ПДн отражено в следующих документах:

– инструкция ответственного за защиту информации в ИСПДн;

– инструкция пользователя ИСПДн;

– порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;

– порядок охраны и допуска посторонних лиц в защищаемые помещения.

5.2. Сотрудники Гимназии обязаны своевременно информировать о ставших им известными фактах нарушения положений настоящей Политики и инцидентах информационной безопасности директору Гимназии и/или заместителю руководителя в незамедлительном порядке.

5.3. Пользователь – сотрудник Гимназии, осуществляющий обработку ПДн. Обработка ПДн включает:

– возможность просмотра ПДн,

– ручной ввод ПДн в систему ИСПДн,

– корректировку ПДн;

– формирование справок и отчетов по информации, полученной из ИСПД.

Пользователь не имеет полномочий для управления подсистемами обработки данных и СЗПДн. Пользователь ИСПДн обладает следующим уровнем доступа и знаний:

– обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к ПДн региональной информационной системе;

– располагает конфиденциальной информацией, содержащейся в региональной системе и контрольно-измерительных материалах.

5.4. Технический специалист по обслуживанию периферийного оборудования – сотрудник осуществляет обслуживание и настройку периферийного оборудования ИСПДн.

В случае проведения технического обслуживания оборудования Гимназии приглашенными техническими специалистами, присутствует и контролирует проведение необходимых работ. Технический специалист по обслуживанию не имеет доступа к ПДн, не имеет полномочий для управления подсистемами обработки данных и безопасности. Технический специалист по обслуживанию обладает следующим уровнем доступа и знаний:

– обладает частью информации о системном и прикладном программном обеспечении ИСПДн;

– обладает частью информации о технических средствах и конфигурации ИСПДн.

6. ТРЕБОВАНИЯ К ПЕРСОНАЛУ ГИМНАЗИИ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПДН

6.1. Все сотрудники Гимназии, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

6.2. При вступлении в должность нового сотрудника директор Гимназии и его за-

местители, обязаны организовать его ознакомление с инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

6.3. Сотрудник Гимназии (далее – сотрудник) должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

6.4. Сотрудники, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а также возможность их утери или использования третьими лицами. Данные сотрудники несут персональную ответственность за сохранность идентификаторов.

6.5. Сотрудники, не использующие технические средства аутентификации, должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей.

6.6. Сотрудники должны обеспечивать надлежащую защиту оборудования ИСПДн, не оставлять его без присмотра, исключив самостоятельный доступ в помещения посторонних лиц.

6.7. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования ИСПДн, а также свои обязанности по обеспечению такой защиты.

6.8. Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и другие носители информации, а также записывать на них защищаемую информацию. Сотрудникам запрещается разглашать конфиденциальную информацию и защищаемую информацию, которая стала им известна при работе с информационными системами Гимназии, третьим лицам.

6.9. При работе с ПДн в ИСПДн сотрудники обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ. При завершении работы с ИСПДн сотрудники обязаны защитить АРМ с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

6.10. Сотрудники должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

6.11. Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

7. ОТВЕТСТВЕННОСТЬ СОТРУДНИКОВ ИСПДН ГИМНАЗИИ

7.1. В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность. Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 УК РФ).

7.2. Администратор ИСПДн и администратор безопасности несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

7.3. При нарушениях сотрудниками Гимназии – пользователей ИСПДн правил, связанных с безопасностью ПДн, данные сотрудники несут ответственность, установленную действующим законодательством Российской Федерации. Руководитель и сотрудники Гимназии несут ответственность за разглашение конфиденциальной информации и несанкционированную модификацию (искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки предусмотренную законодательством Российской Федерации.

7.4. Приведенные выше требования нормативных документов по защите информации и ответственность сотрудников должны быть отражены в Положении о региональном центре обработке информации, осуществляющем обработку ПДн в ИСПДн, и должностных инструкциях сотрудников Гимназии.