Государственное бюджетное общеобразовательное учреждение
средняя общеобразовательная школа №113
с углубленным изучением информационно-технологического профиля
Приморского района Санкт-Петербурга

Принята

решением общего собрания работников
ГБОУ школы №113, протоқол № 2 от 24.01.2014

Утверждена

Директор
_____ Е.А. Касавцова
приказ от 28.01.2014 №74

ПОЛИТИКА

ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Санкт-Петербург
2014

1. Общие положения

1.1. Политика информационной безопасности Государственного бюджетного общеобразовательного учреждения средней общеобразовательной образовательного учреждения №113 с углубленным изучением информационно-технологического профиля Приморского района Санкт-Петербурга (далее – образовательное учреждение) определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, процедур, практических приемов, требований и руководящих принципов в области информационной безопасности, которыми руководствуются работники образовательного учреждения при осуществлении своей деятельности.

1.2. В целях настоящего документа используются следующие основные понятия:

1) персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2) оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

3) обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

4) автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

5) распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

7) блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

8) уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

9) обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.3. Основной целью Политики информационной безопасности образовательного учреждения является защита информации образовательного учреждения 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.

1.4. Политика информационной безопасности разработана в соответствии с:

- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите и информации»;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

- Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»,
- Постановлением Правительства РФ от 01.11.2012. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановлением Правительства от 15.09.2008 РФ №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- приказом ФСТЭК от 18.02.2013 № 21 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- иными нормативными правовыми актами в сфере защиты информации.

1.5. Выполнение требований Политики информационной безопасности является обязательным для всех структурных подразделений образовательного учреждения.

1.6. Ответственность за соблюдение информационной безопасности несет каждый сотрудник образовательного учреждения. На лиц, работающих 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 информационной безопасности являются:
-сохранение конфиденциальности критичных информационных ресурсов;
-обеспечение непрерывности доступа к информационным ресурсам образовательного учреждения;
-защита целостности информации с целью поддержания возможности образовательного учреждения по оказанию услуг высокого качества и принятию эффективных управленческих решений;
-повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами образовательного учреждения;
-определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности;
-повышение уровня эффективности, непрерывности, контролируемости мер по защите от реальных угроз информационной безопасности;
-предотвращение и/или снижение ущерба от инцидентов информационной безопасности.

2.2. Основными задачами политики информационной безопасности являются:
- разработка требований по обеспечению информационной безопасности;
- контроль выполнения установленных требований по обеспечению информационной безопасности;
- повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению и поддержанию информационной безопасности;
- разработка нормативных документов для обеспечения информационной безопасности образовательного учреждения;
-выявление, оценка, прогнозирование и предотвращение реализации угроз информационной безопасности образовательного учреждения;
- организация антивирусной защиты информационных ресурсов образовательного учреждения;
- защита информации образовательного учреждения от несанкционированного доступа и утечки по техническим каналам связи;
- организация периодической проверки соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки директору образовательного учреждения.

3. Концептуальная схема обеспечения информационной безопасности

3.1. Политика информационной безопасности образовательного учреждения 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 образовательного учреждения, 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.

Наибольшими возможностями для нанесения ущерба обладает собственный персонал образовательного учреждения.

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.

Стратегия обеспечения информационной безопасности образовательного учреждения 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 образовательного учреждения.

4. Основные принципы обеспечения информационной безопасности

4.1. Основными принципами обеспечения информационной безопасности:

- постоянный и всесторонний анализ автоматизированных систем и трудового процесса с целью выявления уязвимости информационных активов образовательного учреждения;
- своевременное обнаружение проблем, потенциально способных повлиять на информационной безопасности образовательного учреждения, корректировка моделей угроз и нарушителя;
-разработка и внедрение защитных мер;
-контроль эффективности принимаемых защитных мер;
-персонификация и разделение ролей и ответственности между сотрудниками образовательного учреждения за обеспечение информационной безопасности образовательного учреждения исходит из принципа персональной и единоличной ответственности за совершаемые операции.

5.Объекты защиты

5.1. Объектами защиты с точки зрения информационной безопасности являются:

- информационный процесс профессиональной деятельности;
- информационные активы образовательного учреждения.

5.2. Защищаемая информация делится на следующие виды:

- информация по финансово-экономической деятельности образовательного учреждения;
- 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 образовательного учреждения, активов, находящихся под контролем образовательного учреждения, а также активов, используемых для получения доступа к инфраструктуре образовательного учреждения, должна быть определена ответственность соответствующего сотрудника образовательного учреждения.

6.2. Информация о смене владельцев активов, их распределении, изменениях в конфигурации и использовании за пределами образовательного учреждения должна доводиться до сведения директора образовательного учреждения.

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

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

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

6.6. Ответственные лица должны периодически пересматривать права доступа сотрудников и других пользователей к соответствующим информационным ресурсам.

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

6.8. 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.

6.9. 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.

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

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

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

6.12. Сотрудникам, работающим за пределами образовательного учреждения с использованием компьютера, не принадлежащего образовательному учреждению, запрещено копирование данных на компьютер, с которого осуществляется удаленный доступ.

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

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

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

Рекомендованные правила:

- сотрудникам образовательного учреждения 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 образовательного учреждения не должны использовать сеть Интернет для хранения корпоративных данных;

- работа сотрудников образовательного учреждения с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации образовательного учреждения в сеть Интернет;
- сотрудникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем образовательному учреждению;
- сотрудники образовательного учреждения перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;
- запрещен доступ в Интернет через сеть образовательного учреждения для всех лиц, не являющихся сотрудниками образовательного учреждения, включая членов семьи сотрудников образовательного учреждения.

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

6.17. Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация образовательного учреждения.

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

6.19. 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 образовательным учреждением, является ее собственностью и предназначено для использования исключительно в производственных целях.

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.

6.21. 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.

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

6.22. Все программное обеспечение, установленное на предоставленном образовательным учреждением компьютерном оборудовании, является собственностью образовательного учреждения 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 директору образовательного учреждения.

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.

Сотрудники образовательного учреждения не должны:
- блокировать антивирусное программное обеспечение;
- устанавливать другое антивирусное программное обеспечение;
- изменять настройки и конфигурацию антивирусного программного обеспечения.

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

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

Сотрудники образовательного учреждения для обмена документами должны использовать только свой официальный адрес электронной почты.

6.28. 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.

6.29. 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.

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

6.30. 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.

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

6.32. 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 образовательного учреждения до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование администратором ЛВС.

Сотрудникам образовательного учреждения запрещается:

- нарушать информационную безопасность и работу сети образовательного учреждения;
- 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 образовательного учреждения посторонним лицам;
- создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

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

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

6.35. 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.

6.36. 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.

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

6.38. 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 образовательного учреждения включает в себя:

- разработку и поддержание в актуальном состоянии Политики информационной безопасности;
- разработку и поддержание в актуальном состоянии нормативно-методических документов по обеспечению информационной безопасности;
- обеспечение бесперебойного функционирования комплекса средств информационной безопасности;
- осуществление контроля (мониторинга) функционирования системы информационной безопасности;
- оценку рисков, связанных с нарушениями информационной безопасности

8. Реализация политики информационной безопасности

8.1. Реализация Политики информационной безопасности образовательного учреждения осуществляется на основании документов, регламентирующих отдельные процедуры и процессы профессиональной деятельности в образовательном учреждении.

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 образовательного учреждения возлагается на сотрудника, назначенного приказом образовательного учреждения.

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