Утверждаю

Директор МОУ ИТЛ № 24

_____ С.М. Жилин

«31» августа 2016 года

Положение об информационной безопасности
МОУ – Информационно-технологический лицей №24 г.Нерюнгри

г.Нерюнгри

2016г.

I. Общие положения

1.1 Настоящее Положение об информационной безопасности МОУ ИТЛ №24 (далее - Положение) разработано в соответствии с нормативными правовыми документами:

- Федеральным законом от 29.12.2012 г. №273 - ФЗ «Закон об образовании в российской Федерации» (п.21 ч.3 ст.28, ч.1 ст. 29, ст. 30);

- Федеральным законом от 27.07.2006 г. 152 -ФЗ «О защите персональных данных» с изменениями;

- Законом РФ «О безопасности» (от 05.03.1992 №2446-1) Закон РФ «О правовой охране программ для электронных вычислительных машин и баз данных» (от 2.09.1992 № 3523-1);

- Законом РФ «Об авторском праве и смежных правах» (от 9.07.1993 5351-1);

- Федеральным законом «Об информации, информатизации и защите информации» (от 20.02.1995 № 24-ФЗ);

- Федеральным законом «Об участии в международном информационном обмене» (от 04.07.1996 №85-ФЗ);

- Постановлением Правительства РФ от 18.04.2012 г. №343 «Правила размещения в сети Интернет и обновления информации об образовательном учреждении».

1.2 Настоящее Положение определяет порядок обеспечения информационной безопасности в МОУ ИТЛ №24 (далее - Лицей).

1.3 Под информационной безопасностью лицея понимается защищенность информации от случайного или преднамеренного вмешательства в нормальный процесс функционирования, а также от попыток хищения, модификации или разрушения ее компонентов. В МОУ ИТЛ №24 создана локальная сеть с выходом в интернет, подлежащая информационной защите.

Под безопасностью локальной сети Лицея понимается ее защищенность от случайного или преднамеренного вмешательства в нормальный процесс функционирования, а также от попыток хищения, модификации или разрушения ее компонентов. Безопасность системы достигается обеспечением конфиденциальности обрабатываемой ею информации, а также целостности и доступности компонентов и ресурсов системы.

Безопасность системы обеспечивается комплексом технологических и административных мер, применяемых в отношении аппаратных средств, программ, данных и служб с целью обеспечения доступности, целостности и конфиденциальности связанных с компьютерами ресурсов; сюда же относятся и процедуры проверки выполнения системой определенных функций в строгом соответствии с их запланированным порядком работы.

II. Обеспечение информационной безопасности

2.1 Систему обеспечения безопасности можно разбить на следующие подсистемы:

- компьютерную безопасность;

- безопасность данных;

- безопасное программное обеспечение;

- безопасность коммуникаций.

2.2 Компьютерная безопасность обеспечивается комплексом технологических и административных мер, применяемых в отношении аппаратных средств компьютера с целью обеспечения доступности, целостности и конфиденциальности связанных с ним ресурсов.

2.3 Безопасность данных достигается защитой данных от неавторизованных, случайных, умышленных или возникших по халатности модификаций, разрушений или разглашения.

2.3 Безопасное программное обеспечение представляет собой общесцелевые и прикладные программы и средства, осуществляющие безопасную обработку данных н системе и безопасно использующие ресурсы системы.

2.4 Безопасность коммуникаций обеспечивается посредством аутентификации телекоммуникаций за счет принятия мер по предотвращению предоставления неавторизованным лицам критичной информации, которая может быть выдана системой в ответ на телекоммуникационный запрос.

2.5 К объектам информационной безопасности лицея относятся:

- информационные ресурсы, содержащие сведения, отнесенные к коммерческой тайне, к конфиденциальной информации, представленную в виде документированных информационных массивов и баз данных;

- средства и системы информатизации — средства вычислительной и организационной техники, локальной сети, общесистемное и прикладное программное обеспечение, автоматизированные системы управления рабочими местами, системы связи и передачи данных, технические средства сбора, регистрации, передачи, обработки и отображения информации.

III. Задачи системного администратора но обеспечению информационной безопасности

3.1 Задачи связанные с информационной безопасностью являются прерогативой системного администратора.

3.2 Для обеспечения информационной безопасности системный администратор должен:

3.2.1 Обеспечивать функционирование программно-аппартного комплекса защиты по внешним цифровым линиям связи;

3.2.2 Следить за соблюдением требований по парольной защите, в том числе осуществлять изменение паролей по мере необходимости (утрата пароля, появление новых пользователей в связи с изменением кадрового состава и пр.);

3.2.3 Обеспечивать мероприятия по антивирусной защите как на уровне серверов, так и на уровне пользователей;

3.2.4 Обеспечивать нормальнос функционирование системы резервного копирования.

IV. Базы данных

4.1. Все процедуры по использованию и обслуживанию базы данных осуществляет Ответственный за ведение базы данных. В том числе:

- резервное копирование;
- периодический контроль исправности резервных копий;
- подключение и отключение пользователей;

- внесение изменений в структуру базы, при необходимости (изменение степени конфиденциальности, места расположения и т.д.);
- прочие виды работ связанных с данной базой.

V. Система аутентификации

5.1 На всех клиентских персональных компьютерах Лицея необходимо использовать лицензированные операционные системы WINDOWS не ниже версии XP.

5.2. Для использования локальной сети в учебном процессе используются групповая идентификация: пользователь-ученик, пользователь учитель, администратор с разграничением прав доступа к папкам файлового сервера.

5.3. Для всех пользователей баз данных устанавливаются уникальные пароли.

5.4. Обязать пользователей осуществлять выход из базы данных, если планируется отсутствие на рабочем месте более 1,5 часов.

5.5. Обязать пользователей не разглашать сетевые реквизиты (имена и пароли) для доступа к информационным ресурсам, а также хранить их в недоступном месте.

5.6. Обслуживание системы аутентификации осуществляют ответственные за базы данных и системный администратор.

VI. Обеспечение информационной безопасности по внешним цифровым линиям связи.

6.1 В целях уменьшения риска повреждения программного обеспечения и утери информации, доступ из внутренней сети во внешнюю (Интернет, электронная почта) осуществляется через одну точку (компьютер/сервер), защищенную от несанкционированного доступа извне брандмауэром, контент фильтром и антивирусом.

6.2 Запрещается несанкционированное использование модемов или иных средств доступа с персонального компьютера, подключенных к внутренней сети, во внешние сети.

VII. Защита от несанкционированного подключения к ЛС и размещение активного сетевого оборудования

7.1 Для размещения серверов оборудуются специальная серверная комната, имеющая источник бесперебойного питания, систему кондиционирования и оборудованная пожарной и охранной сигнализацией.

7.2 В серверной комнате не допускается оборудование постоянных рабочих мест для персонала.

7.3 В случае необходимости выполнения каких-либо работ в серверной комнате посторонним персоналом (электрики, сантехники, уборщики и т.д.) обязательно присутствие системного администратора.

7.4. Коммутаторы, концентраторы и прочее активное сетевое оборудование должно располагаться в местах по возможности, исключающих свободный доступ.

VIII. Договор с пользователями о неразглашении информации

8.1 При заключении трудового договора с сотрудниками специально оговаривается и письменно оформляется ответственность сотрудника на случай разглашения им информации, связанной защищенностью информации от случайного или преднамеренного вмешательства в нормальный процесс функционирования, а также от попыток хищения,

модификации или разрушения ее компонентов, К такой информации относятся имена пользователей, пароли, архитектура сети, виды применяемых методов защиты и т.д.

IX. Процедура увольнении сотрудников имеющих доступ к сети

9.1 В случае увольнения системного администратора после подписания заявления об увольнении немедленно назначается исполняющий обязанности увольняемого сотрудника, который меняет все пароли доступа к ресурсам, подконтрольным увольняемому сотруднику. На учетную запись увольняемого администратора устанавливается ограничение по дате с учетом даты фактического прекращения работы увольняемого.

9.2 В случае увольнения рядового пользователя, после подписания заявления об увольнении, руководитель структурного подразделения уведомляет служебной запиской системного администратора о дате фактического прекращения работы увольняемого пользователя. Системный администратор устанавливает ограничения по дате на учетную запись увольняемого сотрудника, по истечении которой учетная запись будет заблокирована, а в дальнейшем уничтожена.

9.3 Новый сотрудник, принимаемый впоследствии на данное рабочее место должен получать новую учетную запись, с новым именем и паролем.

X. Обеспечение информационной безопасности при пользовании внешними сетевыми ресурсами.

10.1. Работа с внешними сетевыми ресурсами (Интернет, электронная почта и т.п.) не допускается без организации антивирусной защиты.

10.2 Антивирусная зашита организуется двухуровнево.

10.2.1 Верхний уровень антивирусной защиты располагается на сервере Лицея, через который осуществляется выход во внешние сети. Нижний уровень располагается на каждом персональном компьютере.

10.3 Тип применяемого антивирусного программного обеспечения (как серверного, так и пользовательского) определяется системным администратором и является общим для всего Лицея.

10.4 Обновление базы используемого антивирусного программного обеспечения осуществляется автоматически не реже 1 раза в неделю.

10.5 Своевременность обновления антивирусного программного обеспечения обеспечивает системный администратор.