

3. [Электронный ресурс] // Режим доступа: <http://www.milandr.ru/>.

УДК 379.8+004.514

Д.А. Богданова
ИНТЕРНЕТ-БЕЗОПАСНОСТЬ ДЕТЕЙ: ЧТО НАДО ЗНАТЬ ШКОЛЕ

Богданова Диана Александровна

d.a.bogdanova@mail.ru

ФГБУН Институт проблем информатики Российской академии наук,

Россия, г. Москва

CHILDREN INTERNET-SAFETY: WHAT SCHOOLS KNOW

Bogdanova Diana Aleksandrovna

The Institute of Informatics Problems of the Russian Academy of Sciences IPI RAN,

Russia, Moscow

***Аннотация.** Предлагается структура системы безопасности в школе с определением областей ответственности.*

***Abstract.** The structure of a security system at school with definition of areas of responsibility is offered.*

***Ключевые слова:** Структура Интернет-безопасности в школе.*

***Keywords:** Structure of Internet safety at schools.*

Информационно-коммуникационные технологии активно меняют среду, в которой мы живем. Постепенно происходят изменения и в организации обучения в школе. Специалисты говорят об информационно-образовательной среде, о смешанном обучении, об Интернете на уроках. В связи с этим все более актуальной становится тема организации безопасной работы детей, а также защиты школьной сети от несанкционированного доступа. Организация системы безопасности в самой школе держится на «трех китах»: инфраструктура, технология, работа с персоналом. Рассмотрим каждую из них.

1. Инфраструктура

В наших школах пока что отсутствует, но со временем обязательно должен появиться специалист, комплексно занимающийся вопросами школьной Интернет-безопасности, который и станет строить свою работу, учитывая все существующие аспекты. Сказанное не означает, что должна появиться новая административная единица. В каждом конкретном случае этот вопрос может решаться по-разному. Просто круг обязанностей одного или нескольких сотрудников расширится, включив формирование и поддержку комплексной структуры информационной безопасности школы. Школьная сеть, как правило, находится в ведении учителя информатики. Проблема поддержки школьного сайта тоже решается по-разному. В идеальном варианте в школе должен быть сотрудник, который знает всю школьную ИТ-инфраструктуру, школьные правила безопасности, круг обязанностей участвующих сотрудников, календарь событий – и с позиций этого комплексного знания координирует работу. Иногда эти функции могут быть поручены заместителю директора по

информатике. В данном случае речь не идет о системе хранения и защиты внутренней школьной информации, касающейся внутренних управленческих вопросов, или, например, личных дел обучающихся. Ответственный специалист поддерживает отношения с Интернет-провайдером и находится в курсе происходящих изменений в плане появления нового программного обеспечения, технических параметров и т.д. В его ведении должен находиться и контроль доступа к сети. Он принимает участие в разработке школьных правил ИТ безопасности, обязательных к исполнению всеми учащимися и всеми сотрудниками. Он в курсе того, какая информация размещается на школьном сайте. Принимает участие в разборе чрезвычайных происшествий или нарушений правил работы за компьютером.

В школе должны существовать правила работы с нарушениями безопасности и информирования о них, а также журнал фиксации нарушений. Основная цель этих правил – незамедлительное реагирование и разбор происшествия с целью минимизации возможных негативных последствий для школы и учащихся. Журнал фиксации нарушений должен просматриваться как минимум раз в семестр (или в четверть). В соответствии с оценкой происшествия, должна быть просмотрена и классификация списка рисков с позиции возможной необходимости ее пополнения или переоценки. На основании журнала школа может составить возможный список происшествий, например:

- попытка обойти систему безопасности;
- доступ к ненадлежащим материалам (список должен содержаться в Правилах пользования);
- инсталляция неразрешенного программного обеспечения;
- использование чужого почтового адреса или пароля;
- нарушение авторского права;
- выгрузка школьного материала в чат или социальную сеть;
- оставление школьных мобильных устройств без присмотра;
- не выход из сети по окончании работы.

2. Технологические вопросы

Трафик

Там, где разрешен трафик в школу из внешней сети, должна быть установлена защитная система (файервол). Сотрудник несет ответственность за антивирусное сканирование и обновление антивирусных программ, отвечает за организацию фильтрации запросов, отслеживает запросы школьников на предмет ненадлежащего содержания и т.д. В середине января 2015 года в школе графства Эссекс (Великобритания) произошел случай, когда во время урока, используя школьный планшет, несовершеннолетняя девочка, в нарушение школьных правил, общалась по Skype с мужчиной, совершавшим половой акт. Она познакомилась с ним в социальной сети во время рождественских каникул, находясь в гостях у родственников [1]. Школа, в которой учится девочка, в начале учебного года купила планшеты для всех учащихся, а чуть позже успешно прошла проверку государственного комитета по стандартам в образовании. В школе придерживаются метода свободного обучения, когда учащиеся на уроке получают задание, и работают самостоятельно, разыскивая требуемую информацию в Интернете. В развернувшейся по этому случаю дискуссии обвиняют школу в недостаточности мер безопасности, учителя – в отсутствии контроля за занятиями детей, девочку – в нарушении школьных правил пользования компьютером.

Скандал пока только набирает обороты, и следствие по делу продолжается. Приведенный пример создал прецедент, который инициирует пересмотр существующих правил и введение дополнительных требований по школьной безопасности. Но, как пишет британская пресса, подобный случай, скорее всего, не единичный. Школы стараются не «выносить сор из избы», поскольку опасаются за собственную репутацию, которая серьезным образом сказывается на финансировании школы.

Пароль

Все сотрудники, имеющие доступ к сети, должны сознавать необходимость соблюдения мер безопасности при выборе и хранении пароля. Примерный перечень рекомендаций к использованию паролей включает следующие требования:

- не давать свой пароль ученикам
- использовать разные пароли для домашнего и школьного доступа
- необходимость периодической замены пароля
- заканчивая работу, отключаться от сети, или, в крайнем случае, запереть клавиатуру
- должны быть установлены ограничения по числу неудачных попыток подключения
- необходимо исключить возможность одновременного подключения (когда пользователь входит в систему с двух компьютеров одновременно).

Удаленный доступ

Доступ к школьной сети не из школы, а с мобильных устройств или домашних компьютеров сотрудников содержит в себе некоторые риски, которые необходимо минимизировать.

- Все имеющие удаленный доступ должны иметь учетное имя и пароль. В ситуациях, когда к сети требуется доступ третьей стороны, это должно происходить только с ведома и одобрения руководства
- Все неудачные попытки входа в систему должны быть заблокированы спустя 3-5 неудачных попыток.

3. Работа с персоналом

Руководство должно своевременно информировать ответственного за безопасность о нанятых и уволившихся сотрудниках. Соответственно должно быть обеспечено прекращение (или организация) доступа к школьной сети. То же должно быть сделано и в отношении новых и покинувших школу учащихся. Персонал школы и учащиеся должны проходить ежегодный инструктаж по правилам безопасной работы. Каждый пользователь школьной сети должен следовать требованиям безопасности. В каждом классе, где занятия проводятся с использованием компьютера, должны быть размещены в качестве напоминания правила поведения за компьютером, а дети должны быть с ними ознакомлены.

Учащиеся и персонал должны знать, что вся ИКТ деятельность через школьную сеть контролируется, включая частную переписку. Учащимся не следует позволять бездумного пребывания в Интернете. Они всегда должны сознавать, что именно они собираются делать, какое задание выполнять. Школа должна работать в тесном контакте с родителями, с ними должна вестись просветительская работа, и в школе должно быть некоторое количество обновляемых обучающих материалов для родителей.

В сказанном нет ничего экстраординарного. Основная задача руководства школы состоит в создании такой системы функционирования, когда все сотрудники информированы

о правилах, существуют и исполняются соответствующие регламенты, а также разработан алгоритм работы с нарушениями. Далее приводится пример школьных правил поведения за компьютером, разработанный совместно с детьми [2]. Дети ответственнее относятся к исполнению правил, если сами принимали участие в их разработке.

1. Я буду использовать школьный компьютер только для школьной и домашней работы.
2. Я буду работать только со своими файлами и не буду смотреть или менять файлы других без их согласия.
3. Я буду держать свое учетное имя и пароль в секрете.
4. Я не буду приносить в школу без разрешения посторонние материалы и не буду сгружать их на свой компьютер.
5. Я понимаю, что некоторые социальные сети имеют возрастные ограничения и я должен это уважать.
6. Я не буду пытаться посетить те сайты, которые запрещены в школе.
7. Я буду общаться по электронной почте с теми, кого я знаю лично или кто одобрен доверенными взрослыми.
8. Информация, которую я посылаю, или письма по электронной почте должны быть вежливыми.
9. Я не стану открывать приложение или сгружать на свой компьютер файл, если я не уверен в том, кто его послал. Я предварительно посоветуюсь со взрослыми.
10. Я не буду сообщать свои персональные данные – имя, фамилию, телефон, адрес – или посылать фотографию тому, кого я не знаю.
11. Если я увижу что-нибудь или получу сообщение, которое меня огорчит, я не стану на него отвечать, а покажу его учителю или доверенному взрослому.
12. Я не принимаю за истину все, что пишут в Интернете. Когда я собираю информацию в Интернете, всегда тщательно проверяю источник информации и обращаюсь за советом к родителям, библиотекаря или учителю. В Интернете можно найти много деловой и полезной информации, но, в то же время, и много неточных и даже ложных данных.

Список литературы

1. Cahalan, P. Girl groomed sex by paedophile in her classromm on school iPad paid for by YOU / P. Cahalan [Электронный ресурс] // Daily mail. — 2015. — January 17. — Режим доступа: <http://www.dailymail.co.uk/news/article-2914989/Girl-groomed-sex-paedophile-classroom-school-ipad-paid-YOU.html> (дата обращения: 02.02.2015)
2. Богданова, Д.А. В Интернет - с широко закрытыми глазами [Текст] / Д.А. Богданова, А.А. Лисицына // Дистанционное и виртуальное обучение. — 2011. — №2. — С. 117-125.