Информационная безопасность образовательного учреждения общего образования

М.И. Шубинский

Информационно-методический центр Петроградского района Санкт-Петербурга
pnmc@mail.ru

Аннотация

В настоящей статье рассмотрены потенциальные объемы работ по обеспечению информационной безопасности образовательного учреждения. Сформулированы основные направления информационной безопасности образовательных учреждений и определены те аспекты, которые заслуживают наибольшего внимания их руководителей.

Введение.

Скачкообразное насыщение компьютерами системы образования, случившееся в начале 2000-ых годов в России породило целый ряд насущных проблем, связанных с внедрением информационных технологий в образовательный процесс. В результате последние 10 лет основной задачей стало выстраивание информационной образовательной среды. Эта чрезвычайно нужная и важная проблема отодвинула все более частные проблемы на второй план. Сейчас, когда уже можно говорить, о существующей информационной среде в образовательных учреждениях (ОУ), начинают всплывать важнейшие проблемы, оставленные ранее до лучших времен.

Один из самых важных вопросов стоящих сейчас перед ОУ с точки зрения информационных технологий – это вопрос информационной безопасности образовательного учреждения. Целью данной работы является определить потенциальные объемы работ по защите информации, стоящие перед образовательным учреждением общего образования

С нашей точки зрения, информационная безопасность ОУ включает в себя три больших направления:

- информационная безопасность компьютеров, локальной сети, серверов и информационных систем;
- информационная безопасность персональных данных;
- защита детей от доступа к негативной информации.

Все направления требуют серьезной и кропотливой работы. Рассмотрим каждое из них в отдельности.

Труды XV Всероссийской объединенной конференции «Интернет и современное общество» (IMS-2012), Санкт-Петербург, Россия, 2012.

1. Информационная безопасность компьютеров, локальной сети, серверов и информационных систем

Это направление наиболее близко к привычной деятельности специалистов, занимающихся информационной безопасностью. Здесь речь идет о защите от несанкционированного доступа, разграничении прав доступа, защиты от вирусов, и компьютерных атак.

К сожалению, школа долго воспринималась как место, в котором работа по защите информации совершенно не требуется. Однако современные образовательные учреждения, например в Петербурге, имеют парк более из 100 современных компьютеров, объединенных в локальную сеть, файловые и почтовые сервера и используют от 5 до 10 автоматизированных информационных систем (АИС).

Рассмотрим модельное учреждение. За основу возьмем хорошо оснащенную школу, имеющую одно здание, собственную бухгалтерию и использующую информационные системы характерные для Санкт-Петербурга. Будем считать, что подобная школа, в настоящее время, оснащена следующим образом.

- Два компьютерных класса по 13 машин (12 ученических + 1 учительская), связанных во внутреннюю локальную сеть.
- Медиатека, в которой расположены 5–10 компьютеров, где могут работать и учителя и ученики, плюс компьютер библиотекаря.
- 20–25 учительских компьютеров в учебных кабинетах, оснащенных мультимедийными проекторами и иногда интерактивными досками, и имеющих выход в локальную сеть ОУ и через нее в Интернет.
- 2–3 компьютера в учительской. Эти компьютеры предназначены для подготовки к уроку учителей, не имеющих своих постоянных кабинетов.
- «Управленческие» компьютеры
- 2 в бухгалтерии
- 5–6 у директора, секретаря и замов
- 1 у социального педагога
- 2 сервера и 2 компьютера у инженерной службы.

Таким образом, общий парк машин может составить 60–70 компьютеров и 2 сервера. Часть компьютеров могут быть мобильными (ноутбуки), в том числе мобильным может быть и один из 2-х компьютерных классов

Подробнее разберем задачи, решающиеся на тех или иных компьютерах.

Компьютеры в компьютерных классах предназначены для обучения учащихся на уроках «основы ИКТ» или интегрированных уроках по иным предметам. Для ведения обучения на данных компьютерах требуется выход в сеть Интернет и установка, требуемых педагогических программных средств (ППС). Занятия ведутся под контролем учителя.

Компьютеры в медиатеке предназначены для самостоятельной работы педагогов и учащихся. Компьютеры должны быть подключены к сети Интернет и к школьному файловому серверу.

Компьютеры в учебных кабинетах предназначены для подготовки учителей к урокам, ведению электронного классного журнала и к работе на уроке с мультимедийным проектором и интерактивной доской.

Компьютеры в учительской предназначены для подготовки учителей к урокам, ведению электронного классного журнала.

Компьютеры в бухгалтерии работают с системой 1С-бухгалтерия и АИС «Госзаказ» (АИС ГЗ)

Компьютер директора должен быть подключен к Интернету и не нем должен быть настроен официальный электронный адрес учреждения. На компьютере должно стоять специальное ПО для работы с ЭЦП для АИС ГЗ и АИС «Электронный торги», на нем должен быть доступ к файлам с управленческими документами (приказами, письмами, тарификацией и т.п.) и ко всем основным модулям АИС «Параграф» (Кадры, движение учащихся, классный журнал, учебный план и т.п.). Компьютер должен быть связан локальной сетью с остальными управленческими компьютерами

Компьютеры секретаря и заместителей директора тоже должны быть связаны в единую локальную сеть, иметь доступ в Интернет. На них на всех должен быть настроен вход в АИС «Параграф» с соответствующими правами. На компьютере секретаря необходим доступ к БД «Метрополитен» (база учащихся, которым положен льготный проездной билет).

На компьютере социального педагога, не должно быть выхода в Интернет а должна быть настроена АИС «Профилактика правонарушений»

К файловому серверу должен быть доступ у всех компьютеров, правда с возможностью разграничить доступ логически к тем или иным разделам, а на сервере баз данных стоит серверная часть АИС «Параграф»

Компьютеры инженерной службы имеют администраторские права с полным доступом ко всем приложениям.

Все вышеперечисленное говорит о том, что в упрощенном случае локальная сеть учреждения должна быть разбита минимум на 3 сегмента (или домена).

1. Машины, на которых работают учащиеся (компьютерные классы и медиатека). С данных машин должен быть невозможен доступ к базам данных, учительским и административным компьютерам.
2. Учительские компьютеры (в учебных кабинетах и учительской). Из данного сегмента сети должен быть невозможен доступ к управленческим компьютерам, но требуется выход к АИС «Параграф»
3. Управленческие компьютеры. Наиболее закрытая часть локальной сети, доступ, к которой из остальной сети строго воспрещен.

Надо отметить, что к файловому серверу доступ должен быть возможен из всех трех сегментов сети, а к серверу баз данных из двух.

На всех компьютерах должно стоять полноценное антивирусное ПО, защищающее от вирусов, троянов, сетевых атак и т.п.

Еще одной немаловажной проблемой является одновременный доступ с компьютеров к информационной системе управления образовательным учреждением (в Санкт-Петербурге это АИС «Параграф») и к сети Интернет. В общем случае это крайне нежелательно, но в Санкт-Петербурге у образовательных учреждений выход в Интернет происходит через защищенный канал связи – единую мультисервисную телекоммуникационная сеть (ЕМТС), что нивелирует данную проблему.

Кроме серьезных технических работ, важнейшей задачей являются организационные меры по защите информации, в том числе большой объем бумажной работы. Так необходимы регламенты о работе с локальной сетью, Интернетом, каждой информационной системой. Причем в регламентах должен быть описан порядок действий, запреты и ответственные должностные лица учреждения (в регламентах указываются должности, а не конкретные люди). Администрация учреждения должна выпустить приказы, в которых назначаются ответственные за работу с информационными системами, а также приказ о назначении ответственного за информационную безопасность учреждения. В этих приказах уже указываются конкретные фамилии.

Если бы речь шла о коммерческом предприятии с таким парком машин и объемами информации, стоимость полноценных работ по защите информации исчислялась бы десятками тысяч долларов или сотнями тысяч рублей. На практике деньги на защиту информации в бюджет ОУ не закладываются вообще, и все работы проводятся силами инженеров.

Конечно, далеко не все школы могут похвастаться таким уровнем внедрения информатизации. Но необходимо иметь ввиду, что рассмотренный вариант школы не является чем-нибудь уникальным, и есть гораздо более сложные случаи:

– когда школа имеет два, а то и три здания;
– когда внедряется система электронного документооборота;

- когда существует собственная кадровая служба (что не удивительно при более чем 100 сотрудниках);
- когда школа оказывает множество дополнительных платных услуг, и в этом случае, одно из ключевых подразделений – бухгалтерия становится отделом, для которого уже необходимо выделять отдельный сегмент сети;

и т.д.

2. Информационная безопасность персональных данных

Начиная с 2006 года согласно 152 ФЗ «О защите персональных данных любое государственное образовательное учреждение является оператором персональных данных. С этим сложно спорить, поскольку любое учебное заведение хранит у себя персональные данные обучающихся и сотрудников и не только хранит, но и ведет автоматизированную обработку этих данных. В Санкт-Петербурге во всех общеобразовательных ОУ имеется АИС «Параграф» с помощью, которого и ведется данная обработка. Но на самом деле, автоматизированная обработка персональных данных ведется и в тех регионах, в которых системы управления ОУ еще не внедрены повсеместно. Поскольку с точки зрения проверяющего органа, которым в данном случае является Роскомнадзор, ввод списка персональных данных с помощью текстового редактора, тоже является автоматизированной обработкой персональных данных.

Если же разбирать ситуацию более пристально, то мы увидим, что существует еще и информация о родителях учащихся, с паспортными данными, местом проживания, местом работы, контактными телефонами, испокон веков, заполнявшаяся на последних страницах классных журналов, а сейчас без раздумий переносящаяся в автоматизированные системы.

Подводя итог вышесказанного можно посчитать, что в школе на 800 учащихся хранятся данные на 800 учеников, примерно 1200 родителей (обычное в школе соотношение – в среднем не меньше чем 1,5 родителя на 1 ребенка) и около 100 сотрудников учреждения. Итого в школе хранятся текущие персональные данные на более чем две тысячи человек.

Много это или мало? С одной стороны, видно, что такое количество данных требует работы по их защите, с другой с точки зрения 152 ФЗ и иных нормативных документов (Приказы ФСТЭК России, ФСБ России, Мининформсвязи России N 55/86/20), значения обрабатываемых персональных данных относятся к категории 3 и объем обрабатываемых персональных данных относятся к категории 2 (от 1000 до 100 000 записей). А значит информационную систему персональных данных (ИСПДн) ОУ можно отнести к 3 классу и ограничить работу по защите персональных данных организационными мерами.

Сразу оговоримся, что существуют случаи, когда нельзя говорить о 3 классе персональных данных. Например, если образовательное учреждение имеет функции районного или муниципального центра, собирающего персональные данные с разных учреждений. В этом случае, даже если число записей не велико, сам функционал сбора, повышает класс ИСПДн до 2-го. Еще один случай повышения класса, когда информационные системы могут содержать данные о заболеваниях, судимостях, политических предпочтениях и т.п. данные. В этом случае надо говорить о 1 классе ИСПДн.

Во всех вышеперечисленных случаях учреждение не может ограничиться организационными мерами, а должно заказать технические работы по защите персональных данных. Причем, именно заказать, поскольку такие работы осуществляются только при наличии соответствующих лицензий ФСБ или ФСТЭК и требуют серьезного финансирования.

В нашей работе мы рассмотрим только необходимые организационные меры и перечень необходимых документов.

Ниже приведен примерный перечень из 15 документов, которые необходимо разработать ОУ. Он не является единственно возможным. Так в рамках опытного проекта по защите персональных данных, проводимого Информационно-аналитическим центром правительства СПб (ИАЦ) совместно с Комитетом по образованию для образовательных учреждений Петроградского района Санкт-Петербурга, был разработан комплект из 19 документов. Однако в нижеперечисленные документы вошло все, что было упомянуто в методических рекомендациях министерства образования и науки от 2010 года.

- Приказ о назначении ответственных за безопасность ПДн (персональные данные).
- Приказ о назначении ответственных лиц за ПДн и список ответственных лиц.
- Приказ о введении режима обработки ПДн.
- Приказ о создании комиссии для классификации ИСПДн.
- Перечень подразделений и сотрудников, допущенных к работе с ПДн.
- Перечень ИСПДн.
- Перечень ПДн.
- Положение о разграничении прав доступа к обрабатываемым персональным данным в информационных системах.
- Частная модель угроз.
- Инструкция пользователя ИСПДн.
- Акт Классификации ИСПДн.
- СОГЛАСИЕ на обработку ПДн.
- Обязательство о неразглашении ПДн.
- Журнал учета носителей ПДн.
- Журнал учёта обращений субъектов ПДн о выполнении их законных прав.

Видно, что перечисленные документы делятся на несколько групп.

1-я группа приказы по учреждению. Самый важный из приказов – о назначении ответственных за безопасность ПДн. Одна из типичных ошибок администрации школы – назначить на эту должность

учителя информатики или инженера. Но работа по организации безопасности ПДн это работа не столько с техникой, сколько с документами и людьми, а значит разумнее, чтобы отвечал за нее заместитель руководителя. Оптимальным вариантом, нам представляется ситуация, когда над задачей в связке работают заместитель директора и технический специалист (учитель информатики). К тому же, именно заместитель директора, а то и только сам директор, владеют информацией, о том, кто из сотрудников с какими персональными данными и с какими ИСПДн работает.

После выпуска первых приказов, ответственный или, созданная рабочая группа, готовят вышеперечисленный набор документов.

2-я часть документации это набор перечней, положений и частная модель угроз. Эти документы разрабатываются один раз и надолго. Существенные изменения в них вносятся только в случае добавления ИСПДн или серьезных изменений в организационной структуре ОУ. Эти документы разрабатываются в соответствии с образцами, спускаемыми из органов управления образованием или региональных министерств, занимающихся информационными технологиями.

3-я группа документов состоит всего из двух документов, но зато требует большого объема организационной работы. Это согласие на обработку персональных данных и обязательство о неразглашении персональных данных. После того как эти документы разработаны, согласие необходимо взять у всех субъектов персональных данных – детей, педагогов и родителей. Обязательство о неразглашении подписывается всеми сотрудниками учреждения работающими с персональными данными. Все согласия и обязательства собираются и хранятся в бумажном виде в соответствующих папках и предъявляются проверяющим органам при необходимости.

4-я группа документов – Журналы, которые должны вестись круглогодично.

Грамотно проведенная работа позволит, не только подготовить необходимый комплект документов для возможной проверки, но и серьезно настроить сотрудников, работающих с персональными данными и ввести персонифицированную ответственность за эти данные.

С каждым годом все больше родителей знает требования к защите персональных данных (и ребенка и своих), а значит, школа должна быть готова работать в ситуации жесткого прессинга по поводу автоматизированной обработки персональных данных со стороны родительской общественности.

3. Защита детей от доступа к негативной информации.

С 1 сентября вступает в силу № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью развитию», подписанный 29.12.2010 г. с поправками принятыми летом 2012 года. Вступление в силу закона активизирует разговоры о необходимости контроля учебным заведением предоставляемого учащимся контента. Безусловно, школы уже давно работают в данном направлении, а первые системы контентной фильтрации были поставлены в школы вместе с пакетом лицензионного программного обеспечения «Первая помощь 1.0» еще в 2007 году. Однако, необходимо отметить, что зачастую школы относятся к защите учащихся от нежелательного контента формально, ограничиваясь минимально требуемыми процедурами.

С нашей точки зрения решение данной задачи должно идти по трем направлениям, взаимно дополняющим друг друга.

1. Разработка нормативных документов
2. Установка на компьютеры, к которым имеют доступ учащиеся, системы контентной фильтрации
3. Обучение учащихся правилам безопасной работы в сети Интернет

Если говорить о нормативной документации, то в данном направлении она немногочисленна и значительно менее регламентирована.

1. Необходимо выпустить приказ об ответственном за установку и поддержку системы контентной фильтрации.
2. В регламенте работы с сетью Интернет, обязательно должен быть раздел о правах и обязанностях учащихся.
3. Желательно создать памятку для учащихся о правилах работы в сети Интернет в образовательном учреждении и ознакомить их с ней под роспись в специальном журнале.
4. Желательно завести журнал, в котором учителя бы фиксировали использование сети Интернет на своих уроках.

Данный перечень документации не исчерпывающий, но достаточный для большинства ОУ. Стоит еще сказать, что можно издать один общий приказ об ответственных за информационную безопасность ОУ, в котором прописать ответственных по направлениям деятельности.

Системы контентной фильтрации, используемые в школах России, делятся на два типа в соответствии с подходом к фильтрации ресурсов.

1. Системы с белым списком – доступ разрешен только в сайты из белого списка

Это например, Интернет-цензор – разработан в Москве одним из лидеров на рынке интеллектуальных домов — системным интегратором «Интернет-дом» при содействии Фонда поддержки развития общества «Наши дети».

Белые списки составляются экспертами разработчика, с возможностью добавить или удалить сайт из этого списка. Проект предназначен, прежде всего, для родителей, однако сильно пропагандировался в ОУ. Из недостатков можно отметить необходимость устанавливать программу на каждый конкретный компьютер

Еще один пример, ТЫРНЕТ Прокси – разработан в Санкт-Петербурге, порталом Тырнет.

Белый список составляется компанией Тырнет с помощью приглашенных экспертов. Предназначен для родителей, но есть комплексная реализация проекта в школах Приморья. Устанавливается на сервер, через который в ОУ настроен вход в сеть Интернет.

2. Системы с черным списком – доступ разрешен только во все сайты кроме сайтов из черного списка

Основными системами являются программы разработанные московской компанией ЦАИР (Центр анализа Интернет-ресурсов)

– СКФ – система поставленная в школы с пакетом «Первая помощь 1.0»,
– NetPolice – более свежий продукт компании ЦАИР.

Вообще ЦАИР наверное единственная компания, чьей основной специализацией является как раз создание систем Интернет-фильтрации различных уровней от домашнего до регионального.

Сами продукты позволяют организовать 2-х уровневый контроль

1. На уровне региона (по черному списку ЦАИР)
2. На уровне учреждения (дополнения в список по желанию учреждения, например социальные сети)

Самый важный момент, что составляются черные списки с помощью экспертного педагогического сообщества с хорошей отлаженной системой с обратной связью.

Нет однозначного ответа, какой из подходов лучше. Черные списки не дают 100% гарантии закрытия всех вредоносных сайтов, поскольку Интернет динамическая система в котором новые сайты появляются ежесекундно, в том числе и с вредоносным содержанием. Белые списки могут гарантировать, ребенок не увидит «плохие» сайты, однако затрудняет учебную работу и существенно ограничивает ресурсы сети Интернет. Возможно, имеет смысл комбинировать подходы и использовать белые списки при работе учащихся начальной и частично средней ступеней (1-7 классы) и системы контентной фильтрации с черными списками для работы в 8-11 классах.

Необходимо отметить, что системы контентной фильтрации в том или ином виде используются практически в 100% ОУ России, что стимулируется регулярными проверками Прокуратуры РФ.

Хуже всего дело обстоит с Обучением учащихся правилам безопасной работы в сети Интернет. По данному направлению нет рекомендованной учебной программы и нет предметов, в рамках которого эту программу можно было бы преподавать. Вести ее в 8 классе в рамках предмета «Основы ИКТ» - поздно, а в предметах ОБЖ (5-6 класс) или «Окружающий мир» (3-4 класс) данные модули не предусмотрены. Стоит надеяться, что подобный модуль может быть введен в данные предметы в ближайшее время.

Альтернативой может быть введение курса с условным названием «Медиабезопасность» как факультативного или как курса из регионального или школьного компонентов. Для работы над подобным курсом можно рекомендовать материалы, разработанные компанией Майкрософт и Лабораторией Касперского. С 2006 года ведутся работы по созданию подобного курса (Основы безопасности жизнедеятельности в Интернете или ОБЖИ) в Санкт-Петербурге на базе Информационно-методического центра Петроградского района. К настоящему моменту разработаны методические рекомендации для учителей и рабочая тетрадь для учащихся 5 классов.

Конечно, некоторые изменения к лучшему есть и в этом направлении. Так 1 сентября 2011 года в большинстве школ России начались с урока Медиабезопасности, что было сделано по рекомендации П. Астахова, являющегося уполномоченным по правам ребенка в РФ. Однако кропотливой повседневной работы в данном направлении практически нигде нет.

Заключение

Нельзя сказать, что задачи информационной безопасности не решаются в образовательных учреждениях. Наоборот, по каждому из вышеперечисленных направлений проводятся работы, но в большинстве учреждений работы эти носят фрагментарный характер. Связано это с несколькими ключевыми моментами:

– не выделяется финансирование на работы по защите информации;
– нет единой политики информационной безопасности образовательных учреждений ни у региональных органов управления образованием ни у министерств (комитетов), занимающихся информационными технологиями;
– у администрации образовательных учреждений нет представления о том, что именно и как необходимо защищать.

При этом необходимо отметить, что только комплексная работа по всем вышеуказанным направлениям может привести к решению проблемы защиты информации и созданию безопасной информационной образовательной среды.

Данная работа и является попыткой объяснить необходимость единого и комплексного подхода к информационной безопасности образовательного учреждения и сформулировать положения, которые могли бы стать основой документа формирующего единую региональную или муниципальную политику в области информационной безопасности в образовании

Литература

[1] Закупень Т. Понятие и сущность информационной безопасности, и ее место в системе обеспечения национальной безопасности РФ // Информационные ресурсы России. 2009. №4.

[2] Столбов А. Обработка персональных данных в медицинских организациях// PC Week Review: ИТ в медицине. 2009. октябрь.

[3] Шубинский М.И. Информационная безопасность для работников бюджетной сферы. Учебное пособие / НИУ ИТМО. СПб., 2012.
[4] Шафеева Е.Ю. Шубинский М.И. Основы безопасности жизнедеятельности в сети Интернет (ОБЖИ). Методическое пособие / МПСС. СПб., 2010.

Information Security in Educational Institution of General Education

M. Shubinskiy

The potential amount of information security tasks in educational institutions is given in the article. The main directions of information security establishment in general education institutions are formulated. The key aspects to be concerned by the heads of educational institutions are determined in the text.