Обеспечение информационной безопасности школы (Операция «Дельта»)

Елена Васильевна Зачёсова, *методист Московского института открытого образования*

Роман Зачёсов, *инженер технической поддержки ЗАО «Вокснет»*

В российскую школу пришёл интернет. Точнее, его провели. В рамках приоритетного нацпроекта «Образование». И теперь приходится с этим как-то жить.

Матчасть. Хард

Согласно типовым перечням учебного оборудования в каждой школе имеется компьютерный класс (а иногда и не один), где установлены десяток-другой машин различной степени новизны и крутости. Сохранность и работоспособность «железа» теоретически должен обеспечивать ответственный за кабинет — т.е. учитель информатики. Персональный компьютер обязательно имеется у директора и/или его секретаря, часто — у завучей, а если в школе наличествует собственная бухгалтерия — компьютер/компьютеры стоят и там; иногда их можно встретить и в предметных кабинетах.

Последняя тенденция — объединять разрозненные школьные машины в локальные сети.

Согласно отчётам в 2007 г. все российские школы подключены к интернету, но не уточняется, каким именно способом: через телефонный модем, ADSL, витой парой до ближайшей точки доступа, коаксиальным кабелем, оптоволоконной связью, Wi-Fi или Bluetooth.

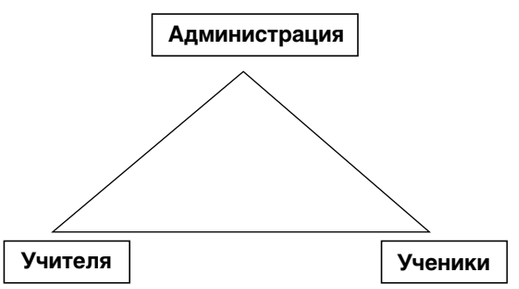
Матчасть. Софт

Предустановленное на машинах ПО может оказаться любым — от лицензионного до пиратского (интуитивно — чаще встречается последнее). Кто имеет право поставлять/покупать/дарить школе программное обеспечение, и что именно следует устанавливать, нормативными актами пока не регламентируется, поэтому нельзя исключить возможность несовместимости программных продуктов.

Признаком информатизации учебного заведения считается наличие действующего сайта. Уровень посещаемости ресурса, к сожалению, часто определяется не столько реальным качеством контента и дизайна, сколько количеством личных друзей и знакомых веб-мастера, участвующих в его раскрутке.

Оперативная схема

Для анализа ситуации с информационной безопасностью кроме матчасти в школе важно учитывать и три группы пользователей: учеников, учителей и администрацию. Расположив их на схеме, получим треугольник, напоминающий прописную греческую букву «дельта», которой в свою очередь принято обозначать разницу (или приращение) измеряемых или рассчитываемых величин. Согласно сложившейся многолетней отечественной традиции присваивать всему кодовые названия поименуем программу обеспечения информационной безопасности школы «Операция «Дельта».



Живая сила. Разведданные

Ученики в массе своей желают работать на компьютерах. Наблюдается чётко выраженное гендерное деление. Мальчики уверены, что хорошо во всём разбираются, могут назвать технические характеристики своего «dream-comp»; склонны к рискованным действиям с незнакомыми программами; дорвавшись до машины, большую часть времени играют в MMORPG и командные шутеры. Девочки «железками» практически не интересуются; довольно консервативны в пользовательских пристрастиях, предпочитают общение в чатах и на форумах; кроме MMORPG охотно играют в casual-игры. Серфинг равно характерен для мальчиков и девочек. За учебными материалами ученики обоих полов чаще всего обращаются в банки рефератов (загляните в любой TOP-100, раздел «Образование»). Старшеклассники и студенты традиционно составляют большую часть Интернет-аудитории (до $^2/_3$).

Учителя относятся к компьютеризации школы преимущественно негативно, считая технические нововведения «бантиками», отвлекающими учеников от главного — изучения предметов и подготовки к экзаменам. Интернет, по их мнению, — главный рассадник агрессии, бездуховности и бескультурья подрастающего поколения. Возможно, эта позиция связана с недостаточной осведомлённостью педагогов. По данным Центра социологических исследований (ЦСИ) МГУ им. М.В. Ломоносова дома пользуются компьютерами меньше половины учителей; доступ на работе в Москве и Санкт-Петербурге имеют примерно столько же, в других городах — около трети, а в селе — около четверти. Следует учесть, что пользователями считаются и те, кто буквы алфавита начинают перечислять с ЙЦУКЕН, и те, кто раз в год, заботливо опекаемые продвинутыми друзьями или коллегами, робко заглядывают в монитор, чтобы посмотреть на какую-нибудь диковинку, которую (по каким-то причинам) не показали по телевизору. Если к этому добавить, что средний уровень учительских доходов не позволяет оплачивать услуги провайдеров, неудивительно, что больше 70% школьных педагогов знают об интернете только понаслышке, а 40% вообще не умеют пользоваться компьютером.

Администрация понимает необходимость информатизации школ; но статистика, хоть и менее удручающая, тоже весьма нерадостна: только половина директоров школ заходила в Интернет, а около 20% из них компьютером не владеют вовсе.

Ради справедливости следует признать, что квалифицированных взрослых пользователей в школе с каждым годом становится всё больше, и всё чаще учителя, работающие в компьютерном классе, обходятся без помощи учеников.

Sed lex

В круг законов, охватывающих вопросы информационной безопасности, входят Закон РФ «О безопасности» (от 05.03.1992 №2446-I), Закон РФ «О правовой охране программ для электронных вычислительных машин и баз данных» (от 02.09.1992 № 3523-I), Закон РФ «Об авторском праве и смежных правах» (от 09.07.1993 №5351-I), Федеральный закон «Об информации, информатизации и защите информации» (от 20.02.1995 № 24-ФЗ) и Федеральный закон «Об участии в международном информационном обмене» (от 04.07.1996 №85-ФЗ). Принятая 09.09.2000 Доктрина информационной безопасности Российской Федерации служит основой для:

- формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;
- подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;
- разработки целевых программ обеспечения информационной безопасности России.

Безопасность определяется как состояние защищённости жизненно важных интересов (т.е. совокупности потребностей, удовлетворение которых надёжно обеспечивает существование и возможности прогрессивного развития) личности, общества и государства от внутренних и внешних угроз.

Основными принципами обеспечения безопасности согласно ст. 5 Закона «О безопасности» являются:

- законность;
- соблюдение баланса жизненно важных интересов личности, общества и государства;

• взаимная ответственность личности, общества и государства по обеспечению безопасности;

• интеграция с международными системами безопасности.

Понятие информационной безопасности определено как «состояние защищённости информационной среды, общества, обеспечивающее её формирование, использование и развитие в интересах граждан, организаций, государства».

Целями защиты информационной сферы являются:

• предотвращение утечки, хищения, утраты, искажения, подделки информации;

• предотвращение угроз безопасности личности, общества, государства;

• предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;

• предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объёма собственности;

• защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

• сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;

• обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Потенциальные опасности

Угрозы информационной безопасности бывают 4-х видов, и для обеспечения информационной безопасности в школе всем участникам процесса информатизации желательно хотя бы кратко ознакомиться с ними.

1. Возможные угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России:

• принятие федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;

• создание монополий на формирование, получение и распространение информации в Российской Федерации, в том числе с использованием телекоммуникационных систем;

• противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;

• нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;

• противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;

• неисполнение федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере;

• неправомерное ограничение доступа граждан к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, к открытым архивным материалам, к другой открытой социально значимой информации;

• дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;

• нарушение конституционных прав и свобод человека и гражданина в области массовой информации;

• вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рын-

ка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;

● девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе;

● снижение духовного, нравственного и творческого потенциала населения России, что существенно осложнит подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных;

● манипулирование информацией (дезинформация, сокрытие или искажение информации).

2. Угрозами информационному обеспечению государственной политики Российской Федерации могут являться:

● монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;

● блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории;

● низкая эффективность информационного обеспечения государственной политики Российской Федерации вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики.

3. Угрозами развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в её продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов могут являться:

● противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления технологической зависимости России в области современных информационных технологий;

● закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;

● вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи;

● увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.

4. Угрозами безопасности информационных и телекоммуникационных средств и систем, как уже развёрнутых, так и создаваемых на территории России, могут являться:

● противоправные сбор и использование информации;

● нарушения технологии обработки информации;

● внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;

● разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;

● уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;

● воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;

● компрометация ключей и средств криптографической защиты информации;

● утечка информации по техническим каналам;

● внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;

- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
- перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
- использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации.

Оставив в стороне внешние, обратимся к внутренним источникам опасности, перечисленным в Доктрине информационной безопасности:

- критическое состояние отечественных отраслей промышленности;
- неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищённости законных интересов граждан, общества и государства в информационной сфере;
- недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;
- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;
- неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;
- недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;
- недостаточная экономическая мощь государства;
- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;
- недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;
- отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

Список так велик, что пункте на десятом утрачивается внимание, а последние, наверное, уже просто никто не читает.

Всё же, чего на самом деле следует опасаться в школе?

Доводы «Против»

Во-первых, реальную опасность представляет недостаточная квалификация взрослых пользователей. Показательным в этом отношении является скандал, разразившийся в августе 2007 года в Австралии. Правительство потратило 84 млн. AUD на разработку проекта NetAlert — фильтров, призванных обеспечить безопасность детского и семейного доступа в Интернет и защитить несовершеннолетних пользователей Интернета от противозаконного, неэтичного и агрессивного контента, предотвращая доступ к сайтам с порнографией, насилием, расовой неприязнью и терроризмом. А 16-летний Том Вуд из Мельбурна за полчаса этот фильтр взломал, причём не просто, а с сохранением видимости его работы. Согласно показаниям компьютера контролирующие подростков

взрослые могли быть спокойны, если бы не одно обстоятельство — фильтр больше не блокирует неприличное содержимое ***(http://www.news.com.au/heraldsun/story/0,21985,22351069-11869,00.html*** — исходная новость в Herald Sun, естественно, по-английски; ***http://www.content-filtering.ru/doc.asp?ob_no=3817*** — а здесь уже по-русски). Пока существует дельта между компьютерными умениями учителей и учеников «в пользу» последних, информационную безопасность в школе обеспечить нельзя.

Во-вторых, учитель информатики — «и швец, и жнец, и на дуде игрец». Почему-то считается, что кроме своих прямых преподавательских обязанностей он должен обеспечивать работу всего компьютерного оборудования в школе: следить за хардом и софтом, бороться с вирусами, иметь ежедневные бэкапы на случай сбоев, администрировать сеть и пр., и пр., и пр. Не считая ликбеза для коллег. Пока не исчезнет дельта между объёмом работы и физическими возможностями человека, об информационной безопасности в школе можно забыть.

В-третьих, компьютеры поставляются в школы централизованно, как и подключение к интернету, а вот их дальнейшее использование целиком отнесено к компетенции образовательного учреждения, включая покупку лицензионного ПО и оплату трафика. А система финансирования образования как раз модернизируется — и вот вам «дело Поносова» ***(http://www.gazeta.ru/education/2007/01/12_a_1249587.shtml).*** Пока существует дельта между потребностью школ в деньгах на информатизацию и возможностью их получения опасность пиратского софта и ограничение доступа к общественно необходимой информации (сиречь интернету) остаётся.

Доводы «За»

Во-первых, прогресс остановить нельзя.

Во-вторых, деньги, конечно, это очень важно, но, к счастью, школа, один из немногих современных институтов, в которых не всё решается на коммерческой основе.

И, наконец, в-третьих, «Глаза боятся — руки делают». ❑