Повышение квалификации в области ИКТ

Информационная безопасность ОУ

Баданов Александр Геннадьевич (badanov1@yandex.ru)

ГОУ ДПО(ПК) С «Марийский институт образования», г. Йошкар-Ола

Аннотация

В статье рассматриваются вопросы об основных проблемах организации обеспечения информационной безопасности в образовательных учреждениях РМЭ. Обзор информационных ресурсов по вопросам информационной безопасности и рекомендации по информированию и обучению большей части учителей основным правилам и технологиям обеспечения информационной безопасности как в ОУ, так и на личных персональных компьютерах.

Свойства информации, связанные с ее безопасностью

- Конфиденциальность.
- Целостность (некий набор фактов, не подлежащий изменению).
- Доступность (информация может быть доступна только определенному кругу людей).

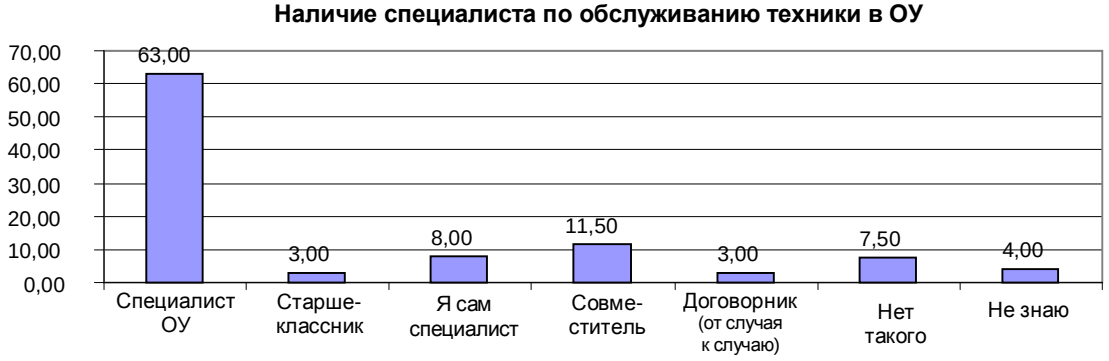
Организация защиты информации

- Технические средства. Это программные, аппаратные и программно-аппаратные комплексы, обеспечивающие выполнение различных функций защиты информации.
- Криптографические средства, обеспечивающие шифрование информации и механизмы проверки подлинности (цифровая подпись и сертификаты).
- Антивирусные мониторы, фильтры, сканеры.
- Межсетевые экраны (брандмауэры) и шлюзы.
- Средства обеспечения отказоустойчивости и резервного копирования.

Результаты опроса работников образования Республики Марий Эл

Опрос проводился ГОУ ДПО(ПК) С «Марийский институт образования» http://www.mari-edu.ru в конце февраля 2010 г. Всего респондентов 1792 педагогов всех районов Республики Марий Эл. Из них большинство работники школ (гимназия, лицей) – 95 % (82 % учителя и 7 % руководители ОУ). Ежедневно компьютер используют 67 %учителей. Ежедневно в сети Интернет работает 49 % и 2–3 раза в неделю – 29 %.

Проблемы информационной безопасности в ОУ решают (занимаются):



Уверенность в том, что компьютер, который используется педагогом, надежно защищен от угроз:

5 % – уверены полностью;

85 % – совершенно не уверены;

10 % – даже и не задумывались по этому поводу.

Как можно заметить, почти каждая школа рассчитывает своими силами (причин этому несколько) решать возникающие проблемы в использовании ИКТ технологий, обеспечении инфорной безопасности и в обслуживании большого парка компьютерной техники. Но вместе с тем у подавляющего большинства учителей нет уверенности в безопасности информации, с которой он работает, и в том, что компьютер, на котором он работает, есть кому починить в случае возникновения разного уровня проблем. Давайте посмотрим, как в различных регионах предлагается решать проблемы информационной безопасности в ОУ.

Например:

1. Школьная компьютерная «скорая помощь», где активную роль играют старшеклассники школы как наиболее знающие специалисты в области ИКТ технологий. (Плюсы и минусы этого решения очевидны).

2. На Алтае предложено регулярно направлять на практику в ОУ студентов, которые и помогут решать возникающие проблемы, кроме этого им рекомендуется активно оказывать помощь учителям в подготовке ЦОР к урокам.

3. Активно использовать курсы повышения квалификации для педагогов, которые как раз и являются теми специалистами, которые в силу различных причин и привлекаются к решению внутришкольных проблем организации информационной безопасности в ОУ (в основном это учителя информатики).

4. Заключаются договоры с коммерческими фирмами на обслуживание ОУ.

Наверное, это правильные решения, но все-таки, помимо этого очень важно каждому пользователю (учителю, администратору, школьнику) быть хотя бы в курсе тех угроз (и знать механизм их возникновения) которые составляют основные проблемы в обеспечении информационной безопасности, знать, как организовать собственными действиями защиту информации и компьютера и владеть простейшими технологиями для отражения угроз информационной безопасности при работе на компьютере, в сети Интернет, работая с базами данных и др. Это позволит более оперативно решать возникающие проблемы, вести профилактическую работу по обеспечению информационной безопасности ОУ, быть уверенным в защищенности той информации, с которой он работает как на работе, так и дома. Исключить из работы домашнее использование компьютера совершенно невозможно, так как при использовании носителей информации (например, флешка) происходит настоящая эпидемия – взаимозаражение компьютеров. Это так же повысит долю ответственности педагогов за обеспечение информационной безопасности на рабочем месте. Ведь какой-либо «дядя» не будет ежедневно проверять все флешки и диски на вирусы, обновлять программы и ОС, находить безопасные приемы работы с информацией, нести ответственность, в конце концов, за эту информацию. Я за широкое и активное просвещение учительства в вопросах информационной безопасности. Социальные сети (В помощь учителю http://www.openclass.ru/wiki-pages/26731 «Лаборатория Касперского» информационная безопасность превыше всего http://www.openclass.ru/ node/47691 и др.) также активно подключаются к решению этих проблем, кроме этого существует еще и множество сайтов, созданных серьезными организациями, занимающимися информационной безопасностью, которые многое делают для школ, детей, родителей советуя, предлагая, оказывая поддержку и др.

Перечислим наиболее популярные:

• Обеспечение информационной безопасности в учебных заведениях. На портале Сети творческих учителей. http://www.it-n.ru/communities.aspx?cat_no = 71586&tmpl = com

• Вопросы обеспечения информационной безопасности от компании Microsoft http://www.microsoft.com/ rus/protect/default.mspx#

• Вопросы безопасности – сайт от компании Semantec http://www.symantec.com/ru/ru/norton/clubsymantec/ library/article.jsp?aid = cs_teach_kids

• Ребенок в сети. Сайт от компании Panda http://www.detionline.ru/

• Специальный портал, созданный по вопрсам безопасного использования сети Интернет. Безопасный Интернет http://www.saferinternet.ru/. Документы, материалы и многое другое.

• «Антивирусная школа» http://av-school.ru. Данный портал создан с целью информирования интересующихся пользователей о возможностях использования персонального компьютера в повседневных делах и учебном процессе, формирования понимания роли информационных технологий, получения новых знаний и навыков для работы с компьютером, общения и обмена опытом между участниками. Этот портал создан специалистами «Лаборатории Касперского».

• Форум «VirusInfo» http://virusinfo.info/forum.php?referrerid = 775 здесь также можно получить ответы и помощь в решении проблем информационной безопасности.

• Сайт «Безопасность в Интернете», который создан специально для детей, родителей и учителей, на котором можно найти много интересной информации и советов

http://www.e-teaching.ru/SiteCollection Documents/pil/inet_safety/html/etusivu.htm.

• http://www.nachalka.com – сайт для людей от 6-и лет и старше, имеющих отношение к начальной школе. Для детей это безопасная площадка, где можно узнавать что-то интересное, создавать что-то новое, играть в умные игры, общаться со сверстниками, участвовать в проектах и конкурсах. «Пока мы спорим «пущать» или «не пущать» учеников начальной школы в Интернет – они уже здесь. Мы снова опоздали. Очевидно, что сейчас невозможно гарантировать стопроцентную защиту детей от нежелательного контента. Никакие фильтры никогда такой гарантии не дадут. Но мы можем формировать у ребят навык «безопасного» поведения в Интернете. Как?» Этому и не только посвящен раздел сайта «Безопасность детей в Интернете» http://www.nachalka.com/bezopasnost.

• От компании Microsoft: книга «Безопасность детей в Интернет»
http://www.ifap.ru/library/book099.pdf

• Всероссийский интернет-урок информатики «Безопасность детей в Интернете». Это проект Компании Microsoft совместно с АПКиППРО http://www.e-teaching.ru/history/Pages/i-yrok.aspx

• Эксперты предлагают родителям рекомендации для обеспечения безопасности детей
http://school-sector.relarn.ru/wps/?p = 1758

• Интерактивная игра «Джунгли Интернета» http://school-sector.relarn.ru/wps/?p = 1706 Игра предназначена для детей в возрасте от 7 до 10 лет и по заказу совета Европы «Строим Европу для детей и вместе с детьми». http://www.wildwebwoods.org/popup.php?lang = ru

• Детский сайт ТВИДИ. Правила безопасности в сети Интернет. Безопасный поиск, общение http://www.tvidi.ru/ch/main/safe.aspx

• Детский поисковик AGAKIDS http://www.agakids.ru/#section_main Визуальная поисковая система детских сайтов «AGAKIDS» создана в помощь детям для поиска детских ресурсов на просторах Интернета.

• http://www.gogul.tv/ Детский браузер.

• http://www.moskids.ru/ Детский портал для детей города Москвы. Очень яркий и интересный для детей, родителей и учителей портал.

Основные правила информационной безопасности:

Для того, чтобы защитить свой компьютер, нужно совсем не так много усилий, как кажется некоторым на первый взгляд. Главное, прилагать эти усилия заблаговременно (т. е. заранее), а не тогда, когда у вас начнут появляться проблемы... И не менее важно быть всегда последовательным и аккуратным в вопросах организации защиты информации на собственном ПК. Я очень быстро пройдусь по основным «бастионам» защиты и подробнее на особенностях тех или иных программ.

Регулярная установка всех критических обновлений ОС (операционной системы). Это обычно производится с помощью сайта компании Microsoft Update: http://update.microsoft.com, комментировать процедуру обновления операционной системы нет необходимости. Все это происходит, как правило, в автоматическом режиме. Пользователю потребуется только ответить на несколько вопросов и предложений. Для школ более приемлемым может быть вариант, когда скачивают с портала компании Microsoft все критичные обновления и Сервис Паки и затем локально устанавливают на все

школьные компьютеры. Это позволяет экономить трафик и при медленном и нестабильном подключении к сети Интернет будет более эффективно.

Установка антивирусной программы. Одна из самых популярных в России антивирусных программ – Антивирус Касперского (имеется в пакете «Первая Помощь»). К сожалению, на слабых машинах (а их большинство, особенно в регионах) антивирус Касперского заметно тормозит работу системы и программ. Его можно ускорить, но при этом придется отключить ряд функций. Это не всегда устраивает пользователей, поэтому попробуйте присмотреться к альтернативным, бесплатным программам. Популярные бесплатные программы:

avast! Home Edition http://www.avast.com/eng/download-avast-home.html

AntiVir® PersonalEdition Classic http://free-av.com/en/download/index.html

AVG Free http://free.grisoft.com;

Microsoft Security Essentials http://www.microsoft.com/Security_essentials/.

Не за горами тот день, когда пакет программ «Первая помощь» станет невозможно использовать в полном объеме. И проблема использования, и выбора антивируса перед не самым богатым российским образованием действительно станет проблемой! Кроме этого, важно иметь в виду, что антивирусная программа на компьютере должна быть только одна. Компьютер просто перестанет работать, если на нем, например, с целью большей защищенности будет поставлен еще один или больше антивирусов. Это абсолютно неграмотное решение. А с такой ситуацией можно очень часто сталкиваться. Не забывайте, что антивирусные базы требуют ежедневного обновления. Обновление как баз вирусов, так и самих программ, происходит с помощью сети Интернет. Программы «сами об этом знают» и самостоятельно (по вашему разрешению либо отдельно, либо в процессе установки) будут обновлять базы и версии программ.

Использование фейервола (встроенный брандмауер есть в Windows и можно им воспользоваться) или попробовать бесплатный фейервол, например Comodo Firewall http://www.personalfirewall.comodo.com/. Это один из популярных в сети Интернет фейерволов.

Установка операционной системы в нестандартный каталог, например OS, MyWindows и т. д. Это позволит ввести в заблуждение отдельные вредоносные программы, которые используют жестко закрепленные пути, например C:\Windows. Правда, как бы и самому не запутаться, где тут у меня установлена операционная система.

Использование альтернативного браузера. Так как большинство вирусов написаны в расчете на использование пользователем стандартной программы Internet Explorer, то большинство случаев заражения происходит через уязвимость этого популярного браузера, хотя с 1 марта этого года компания Microsoft в комплект дистрибутива операционной системы включила и альтернативные браузеры. Их предложено несколько. Использование альтернативной программы позволит резко снизить вероятность поражения компьютера через браузер, хотя IE так же придется оставить на компьютере, так как отдельные интерактивные формы, заполняемые в сети Интернет, могут не работать с бесплатными альтернативными браузерами. Вот ссылки на наиболее популярные программы: Mozilla Firefox http://www.mozilla.ru/; Opera http://www.opera.com/download/.

Внимание! Для более эффективной организации информационной безопасности при использовании браузера Mozilla Firefox можно добавить к браузеру с помощью меню Инструменты – Дополнения специальные модули. Их множество. С перечнем рекомендуемых можно познакомиться перейдя по ссылке https://addons.mozilla.org/ru/firefox/browse/type:1/cat:12

Наиболее востребованы:

Adblock Plus – не пропускает и (или) блокирует нежелательные окна, рекламу;

NoScript-регулирует исполняемость скрытых команд-скриптов на web-страницах.

Использовать вспомогательные программы для обеспечения защиты своего компьютера. Одна из наиболее популярных программ **Spybot-Search & Destroy (Спайбот – найти и уничтожить)** поможет обнаруживать и удалять с Вашего компьютера различного рода шпионское программное обеспечение. Как правило, не все антивирусные программы его обнаруживают. Сайт поддержки – http://www.safer-networking.org/ru/home/index.html. На странице http://www.safer-networking.org/ru/tutorial/index.html размещен учебник с почти пошаговой инструкцией установки и использования данной программы.

Отключить возможность автозапуска и автозагрузки на компьютере. Эти функции используют вирусы, которые приходят к нам с помощью носителей информации. Это легко можно сделать, воспользовавшись программой **Autorun Guard.** Это бесплатная программа для управления автозапуском на внешних носителях в ОС Windows. Она позволяет полностью отключить автозапуск в Windows и тем самым **защититься от проникновения autorun-вирусов**, она также позволяет восстановить работу автозапуска, если автозапуск или автозагрузка были нарушены сторонними программами. http://autorunguard.com/ru/. Эту операцию можно сделать и вручную с помощью использования параметров групповой политики для отключения всех функций автозапуска (пример для ОС Windows XP):

1. Выберите в меню Пуск пункт Выполнить, введите Gpedit.msc в поле Открыть и нажмите кнопку ОК.

2. Последовательно разверните узлы Конфигурация компьютера, Административные шаблоны и Система.

3. В области Параметры щелкните правой кнопкой мыши элемент Отключить автозапуск и выберите пункт Свойства.

Примечание. В системе Windows 2000 параметр политики называется **Отключить автозапуск**.

4. Щелкните элемент **Включено**, а затем выберите вариант **Все диски** в окне **Отключить автозапуск**, чтобы отключить автоматический запуск для всех дисков.

5. Нажмите кнопку **ОК**, чтобы закрыть диалоговое окно **Свойства выключения автозапуска**.

6. Перезагрузите компьютер.

Архивирование важных данных. Особенно **важно** работая с базами (для их сохранности), например с базой ОУ Хронограф Школа 2,5, которая активно используется многими школами, с целью сохранения информации необходимо регулярно сохранять копию этой информации на отдельном жестком диске или удаленном компьютере. В случае возникновения либо технических, либо программных проблем с сервером или локальным компьютером, на котором так же может храниться важная информация, использование пользователем программы для **архивного копирования** позволит избежать потерь рабочей информации. А это вложенный большой человеческий труд и временные издержки, которые непременно бы возникли. Ярким примером подобных программ может служить свободная программа **Cobian Backup** http://www.cobian.se. Эта программа может работать как автоматически – по расписанию, так и в ручном режиме – по требованию пользователя АРМ.

Оптимизация операционной системы и наиболее часто используемых программ. Программа **Xp-AntiSpy** http://www.xp-AntiSpy.org поможет изменить некоторые настройки операционной системы Windows и пакета программ Microsoft Office с целью отключения ненужных вам в вашей работе сервисов, в частности: **автозагрузки**, ограничение количества ПК в локальной сети (свыше 10 машин в случае одноранговой сети), отчетов об ошибках, работы с мультимедиа и др.

Оптимизировать систему и работу отдельных программ можно при помощи программ – твикеров, позволяющих в считанные минуты устранить неполадки в системе и ускорить работу. Одной из них является **BoostSpeed**. http://www.auslogics.com. Lite версия этой программы бесплатна, в ней есть все необходимое для комплексной оптимизации системы. Программа оптимизирует файловую систему и автоматически или по вашему требованию отключит невостребованные системные службы. Кроме этого пользователь может увеличить скорость загрузки Windows, выбрать оптимальный по скорости работы внешний вид операционной системы, ускорить работу почтовых и офисных программ, браузеров и некоторых системных компонентов. Помимо вышеперечисленного BoostSpeed имеет несколько дополнительных утилит, среди которых есть Banner Killer – утилита, блокирующая нежелательную рекламу. В ее постоянно обновляемой базе данных имеется список сайтов, с которых обычно загружаются всплывающие окна.

Схема распределения ролей в сети. Для каждой группы пользователей имеются свои настройки. Вход, естественно, под паролем. Рекомендуется пароль администратора – не менее 10 символов, а пароли пользователей – не менее 6 символов, т. е. возникают группы учитель, ученик, администратор. В рамках этих групп устанавливаются ограничения на пользование сетью и ограничивается доступ к определенным ресурсам. Там же может быть ограничено время пребывания в сети, доступ к ряду «опасных» сайтов.

Осуществлять режим жесткого входного контроля всей информации, которая поступает на ваш компьютер, от электронной почты до любых документов, которые вам принесли на флешке. Для того чтобы обезопасить себя от случайного поражения вирусами вашего компьютера необходимо быть внимательным в общении и не общаться со случайными людьми (электронная почта) и различными сайтами. Это может произойти в основном в двух случаях: если вы посещаете сайты сомнительного содержания и открываете постороннее вложение в электронных письмах (программы, документы, картинки и др). В первом случае достаточно свести к минимуму посещение сомнительных сайтов. Правда для этого существует система СКФ, которую тоже необходимо настраивать и регулярно пополнять базу программы ссылками на недопустимые адреса, установленная на каждом компьютере в школе. Интернет можно раздавать (осуществлять входной контроль и запросы пользователей) с помощью бесплатного варианта программы NetPolice Lite http://www.netpolice.ru/filters/netpolice-lite/. Это контент фильтр, который позволяет весьма эффективно ограничивать посещение нежелательных сайтов. Возможность ограничения нежелательного контента можно организовать с помощью дополнения к известному браузеру Mozilla Firefox в виде детского браузера Гогуль http://www.gogul.tv/, который обеспечит контроль посещения ребенком сайтов в Интернете. Для контроля запуска других браузеров возможно использование бесплатной программы Angry Duck (необязательный компонент). Со вторым случаем сложнее. Письма с вирусами могут приходить как от незнакомых, так и от знакомых людей. Если пришло письмо от незнакомого человека, и в письме есть вложение, открывать его можно лишь в том случае, если из текста письма вы четко поняли: что это письмо для вас; что именно находится во вложенном файле; что содержимое вложения вам нужно. Никогда не следует открывать файлы, которые случайно попали к вам.

Теперь самое важное! Все системы защиты информации будут работать действительно на сто процентов, только если вы установите эти программы на чистый без вирусов компьютер. Для того чтобы убедиться в том, что он чист, существуют специальные программы-утилиты, которые к тому же распространяются бесплатно и не требуют установки на компьютер. Эти программы можно запускать с диска (CD или DVD), защищенной от модификаций флешкой (с ключом защиты от записи) или с помощью загрузочного диска (так называемого Live CD).

Теперь попробуем проверить свой компьютер на вероятность его поражения вирусами. Не стоит уповать на установленный антивирус, это, к сожалению, не гарантирует компьютер от внедрения вирусов. Только комплексные меры и собственная «чистоплотность» в какой то мере даст вам возможность безопасно работать с информацией.

Проверяем все локальные диски антивирусной программой. Очень удобно здесь как раз и воспользоваться утилитой **CureIt** http://www.drweb.com. При обнаружении вируса мы предложим антивирусу попробовать вылечить файл. Если это не получится, то удаляем его совсем. Обычно легко лечатся документы MS Word, Excel и другие документы MS Office. Программные и системные файлы лечатся с большим трудом. Велика доля вероятности, что они не поддадутся лечению. Тогда их надо удалять без сожаления, потому что это уже не те программы, которые работали на вас. Это уже мутанты, которые никогда не будут делать то, что делали раньше, а будут выполнять новые задачи, поставленные вирусописателем, либо компьютер будет вести себя не адекватно вашим действиям с информацией.

Если антивирус будет сообщать о невозможности удаления каких-либо файлов, приготовьтесь перезагрузить компьютер в безопасный режим Safe Mode (Защищенный режим) и повторить сканирование сначала, хотя есть специальные программы именно для удаления таких проблемных файлов, например Unlocker http://ccollomb.free.fr/unlocker.

Проанализировать состояние компьютера можно также с помощью утилиты **AVZ** http://z-oleg.com/secur/avz/. Антивирусная утилита AVZ является инструментом для исследования и восстановления системы, и предназначена для автоматического или ручного поиска и удаления:

- SpyWare, AdvWare программ и модулей (это одно из основных назначений утилиты);
- руткитов и вредоносных программ, маскирующих свои процессы;
- сетевых и почтовых червей;
- троянских программ (включая все их разновидности, в частности Trojan-PSW, Trojan-Downloader, Trojan-Spy) и Backdoor (программ для скрытного удаленного управления компьютером);

• троянских программ-звонилок (Dialer, Trojan.Dialer, Porn-Dialer);

• клавиатурных шпионов и прочих программ, которые могут применяться для слежения за пользователем.

Эта утилита **не лечит компьютер**, а только помогает найти уязвимые места и вирусы, которые потом **придется убрать вручную** или с помощью других программ.

Для того чтобы перевести компьютер в безопасный режим, необходимо в момент включения компьютера при появлении меню загрузки Windows нажимать на клавишу «**F8**», чтобы на экране появилось меню дополнительных режимов загрузки. Теперь передвигаемся с помощью клавиш вверх/вниз и, остановившись на надписи «**Safe Mode**» (Защищенный режим), нажимаем «Enter».

Когда сканирование будет закончено, и все найденные антивирусом вредоносные файлы вылечены/удалены, перезагружаем компьютер, и восстанавливаем поврежденную защиту (переустановка антивирусов и вспомогательных программ).

Если после антивирусной чистки перестали работать какие-то нужные вам программы, следует переустановить их с имеющихся у вас дистрибутивов.

Внимание!

Например, на сайте поддержки антивирусных продуктов Касперского http://www. kaspersky.ru/ можно проверить компьютер как целиком, так и отправить отдельный файл на проверку.

Также имеется сервис http://www.VirusTotal.com, который анализирует подозрительные файлы и облегчает быстрое обнаружение вирусов, червей, троянов и всех видов вредоносных программ, определяемых антивирусами. На этом сервисе можно проверить файл сразу несколькими антивирусами.

Информационные системы широкого доступа и ИКТ-готовность граждан к электронным услугам

Бакшаева Наталия Витальевна (n_bakshaeva@mail.ru)

ГОУ ВПО «Чувашский государственный университет им. И.Я. Яковлева, г. Чебоксары

Аннотация

Изложенные материалы отражают текущее развитие информационных систем широкого доступа для оказания государственных услуг населению Росси в электронном виде. Приводятся данные исследования международных экспертных сообществ по оценки электронных правительств различных стран, включая российское правительство. В статье дается оценка единого портала госуслуг и ИКТ-готовность граждан к использованию предоставляемых электронных транзакционных сервисов.

Реализация программы развития электронного правительства в России завершается в 2010 году. Эстафету решений принимает стратегия развития информационного общества. Среди ряда программных решений в завершающем периоде особое внимание уделяется предоставлению государственных услуг гражданам в информационных системах широкого доступа не только в форме информационного насыщения нормативного и документального пространства взаимодействия, запланированного на первых этапах развития электронного правительства, но и транзакционных услуг, ускоренная подготовка к реализации которых наблюдается на федеральном и региональных уровнях РФ в последнее время. Следует отметить, что в процесс создания электронного правительства (E-Goverment) вовлечены многие страны как с развитой, так и развивающейся экономикой с 1991 года и имеют правительственные порталы, откуда граждане получают доступ ко всем государственным учреждениям. Мониторинг процесса информатизации общества, определение открытости и доступности информации, готовность органов власти к оказанию государственных услуг в электронном виде осуществляется различными организациями. Довольно широко цитируются результаты Департамента экономических и социальных вопросов ООН (Global Survey), Европейской комиссии (European Commission Directorate General for Information Society and Media), Waseda University International E-Government Rankings (Университет Васэда, Япония), Global E-Government (Университет Брауна, Провиденс, США).

В России подобным анализом занимаются Институт развития информационного общества, Высшая школа экономики, Институт развития свободы информации, аналитическое агентство CNews Analytics