Информационная безопасность образовательных учреждений в контексте противодействия угрозам терроризма и экстремизма.

Каберник Виталий Владимирович-
начальник отдела перспективных
научно-образовательных разработок
МГИМО (У) МИД России.

Когда речь заходит об информационной безопасности, обычно мы начинаем думать о компьютерах, сетях, интернете, киберпреступности и хакерах. Но для образовательной среды проблема стоит шире: в ограждении учащегося от информации, которая может негативно повлиять на его формирование и развитие, то есть о пропаганде различной направленности. Кроме того, все еще слабо осознана та часть проблемы, которая связана с общением в социальных сетях, которые сегодня все чаще подменяют собой живое общение. В виртуальном пространстве действуют совершенно иные правила, где психически неокрепшая личность не может эффективно противостоять угрозам, запугиванию, откровенным попыткам растления. И сегодня именно этот фактор начинает выходить на первые роли в обеспечении информационной безопасности в ее широком понимании: не только технической, но и когнитивной сферы во всей ее полноте.

Обзор ситуации

Зарубежный и отечественный опыт позволяет определить следующие угрозы информационной безопасности, которые стоят перед образовательными учреждениями:

- Несанкционированный доступ к данным. Эта группа угроз включает в себя подмену данных в электронных журналах, архивах, хищение информации экзаменационных билетов, личных данных учащихся и их родственников и т.п. В большинстве рекомендаций по организации

схем обеспечения информационной безопасности специалисты ограничиваются только этой, технической сферой.

- Фильтрация нежелательной информации. Эта группа угроз напрямую связана с противодействием экстремистской идеологии, но не ограничивается только ей. При рассмотрении угроз доступа к нежелательной информации следует также учитывать вопросы распространения порнографии, провокационных материалов, пропаганды наркотиков и алкоголя и т.п.
- Проблемы регулирования использования социальных сетей. Именно в этой зоне осуществляется активное давление на учащихся, запугивание, а также сравнительно новый феномен киберхулиганства.
- Кибертерроризм. Несмотря на то, что эта группа угроз находится в ведении соответствующих силовых ведомств, частично она может решаться и на уровне учебных заведений. Создание безопасной информационно-технологической среды серьезно осложняет возможные кибератаки на объекты образования, которые могут привести к нарушению функционирования управляющих автоматических систем и последующему повреждению инфраструктуры. Следует, впрочем, отметить, что эта группа угроз остается пока во многом гипотетической, так как учебные заведения в силу низкой их насыщенности автоматизированными управляющими системами не рассматриваются в качестве приоритетных целей для кибератак.

Поле технических угроз

Современные образовательные учреждения широко используют в своей деятельности информационные технологии для ведения журналов, контроля успеваемости, административно-хозяйственной деятельности и т.п. К сожалению, информационные системы, используемые в средней школе, в

большинстве своем, не отвечают даже минимальным требованиям, предъявляемым к безопасным системам.

Подавляющее большинство школьных информационных систем не проходят какой-либо сертификации, стандартизации, создаются буквально «на коленке» низко квалифицированными разработчиками, очень часто на основе устаревших решений. Перечисляя проблемы, характерные для таких информационных систем, можно отметить:

- Использование разнородных, устаревших и заведомо небезопасных платформ. Уязвимости в информационных системах, базах данных и других информационных средствах выявляются регулярно, и любая устаревшая платформа должна считаться заведомо небезопасной, если не проведены работы по устранению этих проблем. Во многих случаях информационные системы не связаны между собой, используют разные платформы, что резко осложняет их использование и поддержку.
- Отсутствие стандартизации. Несмотря на предпринятые попытки разработать унифицированные информационно-технические решения, большинство учебных заведений используют те решения, которые оказались под рукой.
- Использование публичного открытого соединения. Любая информационная система, претендующая на безопасность, должна организовывать передачу данных с использованием зашифрованных соединений по умолчанию во избежание перехвата данных.
- Отсутствие практики регулярного аудита безопасности. Без постоянной проверки и выявления потенциальных проблем даже качественно спроектированные информационные системы могут стать небезопасными при обнаружении новых видов уязвимостей.
- Низкая квалификация обслуживающего персонала или отсутствие должности специалиста по поддержке информационных систем в принципе. Качественная поддержка информационных систем требует

регулярного мониторинга их работы и превентивного устранения неполадок.

- Использование пиратского программного обеспечения. Многие образцы «взломанных» программ могут содержать в себе троянский код, упрощающий внедрение в информационные системы. Кроме того, пиратское программное обеспечение часто исключает возможность его обновления, что не позволяет противостоять вновь возникающим угрозам.
- Недофинансирование. Эта проблема является корнем всех вышеперечисленных.

К решению всех описанных проблем можно подходить на различных уровнях. Оптимальным вариантом могла бы стать разработка единой платформы для всех образовательных учреждений и ее централизованная удаленная поддержка высококвалифицированными специалистами, которые обладают необходимыми знаниями в области обеспечения безопасности информационных систем. Однако такой вариант возможен только в дальней перспективе и выглядит идеалистическим. В реальности все возникающие проблемы учебные заведения вынуждены решать самостоятельно.

Опыт МГИМО в этой сфере основан на использовании свободно распространяемого (бесплатного) программного обеспечения, платформы, на базе которой развиваются необходимые информационные системы. Специалисты по ее поддержке имеют многолетний опыт по работе именно с этим комплексом, что позволяет оперативно устранять все возникающие проблемы безопасности. Аналогичный проект может быть реализован в любом учебном заведении, либо передан им на безвозмездной основе. Однако такое решение всегда должно быть адаптировано под нужды конкретных образовательных структур. Практика (в частности, практика МГИМО) показывает, что универсальное решение, которое способно потенциально управлять всеми аспектами учебного процесса (оставляя в стороне вопрос об обеспечиваемом уровне безопасности), является крайне

сложным во внедрении, неповоротливым, требующим значительных издержек на его поддержку.

Другим направлением по обеспечению информационной безопасности технологической инфраструктуры является проведение регулярного аудита систем, который может осуществляться внешними специалистами.

Следует отметить еще один фактор, который серьезно ослабляет информационную безопасность, фактически аннулируя все усилия технических служб. Речь идет о политике распространения и смены реквизитов доступа к информационным системам. Нередко в качестве паролей используются элементарно вскрываемые комбинации, такие как номер телефона пользователя, номер паспорта, идентификационный номер в системе, почтовый индекс и т.д. Это не только проблема образовательных учреждений, она, к сожалению, встречается повсеместно. Так, например, совсем недавно при установке точек беспроводного доступа один из московских операторов без согласования с пользователями использовал в качестве пароля их номера телефонов. В результате многие люди, включая, например, пенсионеров, были вынуждены оплачивать доступ в интернет, которым они не пользовались, а вместо них его использовали не слишком добросовестные соседи.

В построении школьной информационной среды фактор политики управления реквизитами доступа обычно вообще не учитывается: пароли распространяются открыто, не меняются на протяжении многих лет, часто их знают учащиеся, которые, не секрет, умеют обращаться с современными информационными технологиями многим лучше своих родителей. Этот канал утечки, согласно статистике, является основным, и закрыть его в обозримом будущем не представляется возможным. Не имеет смысла прилагать усилия хакерского толка для взлома пароля, если его легко можно угадать, обладая минимумом информации о пользователе.

Несмотря на то, что здесь мы говорим об элементарных правилах информационной гигиены – даже не безопасности – подавляющее

большинство пользователей не имеют об этом никакого представления. На уровне образовательных учреждений результат чаще всего будет сравнительно безобиден: подлог данных в электронном журнале, подтасовка электронных дневников и т.п. Но эта проблема становится системной: если человек не знаком с такими элементарными правилами информационной гигиены, он с высокой вероятностью может стать жертвой мошенников в будущем. Поэтому в программу преподавания информатики в школах в обязательном порядке должны включаться уроки по основам информационной безопасности.

Расширенный курс информационной безопасности и все затрагиваемые в нем проблемы был бы слишком обширен, но основы его могут и должны включаться в программы повышения квалификации преподавательского состава, особенно с учетом того, что современный мир попросту пронизан информационными технологиями на всех уровнях при вопиюще низком уровне знания рисков их использования средним пользователем.

Ограничение доступа к нежелательной информации

Как уже было отмечено, информационные технологии сегодня используются настолько активно и прозрачно, что человек может даже не замечать, что он ими пользуется. Для современного ученика или студента доступ к почти неограниченным объемам информации настолько же естественен, как и простое очное общение – а нередко и более привычен, но на этом мы подробнее остановимся ниже.

Разумеется, далеко не вся информация, к которой ребенок получает доступ, безобидна. Здесь можно упомянуть проблемы распространения порнографии, идеологических материалов, пропаганды, да и даже просто новостных потоков, которые не брезгуют размещать в средствах массовой информации фотографии и видеоролики, которые вызывают оторопь у взрослых – что уж говорить о детях и подростках.

В мировой практике до недавних пор преобладало мнение о том, что интернет должен оставаться свободным, потому что эта сеть имеет

способности саморегулирования. Большинство организаций, занимающихся регулированием и развитием интернета, являются некоммерческими, не связаны с международными или государственными структурами, а поэтому любые их решения не могут иметь законодательной силы.

Ситуация начала меняться сравнительно недавно, когда ряд государств, включая Россию, все громче стал заявлять о необходимости регулирования не только технических аспектов работы интернета, но и информации, которая там распространяется. Эти инициативы продвигались на уровне ШОС, международных советов по электросвязи и других регулирующих органов, но в большинстве случаев эти попытки были безуспешными. Одним из немногих успехов на этом фронте можно назвать принятие ряда соглашений по противодействию киберпреступности, но и они остаются лишь рекомендациями, необязательными к исполнению, либо действуют на уровне взаимоотношений отдельных ведомств.

Причиной неэффективности создания действенных механизмов регулирования информации, распространяемой через интернет, является то, что в мире не существует единого органа, который уполномочен выполнять эти функции. Попытки создать его на основе уже существующих организаций, или наделить их такими функциями предпринимаются, но практически всегда сталкиваются с нежеланием поиска консенсуса в этой непростой, очень чувствительной сфере, которая кроме прочего для ряда государств остается весьма идеологизированной. Вплоть до того, что право на свободный и неограниченный доступ в интернет закрепляется через резолюции ООН.

Подробное рассмотрение проблем регулирования распространения информации в интернете остается за рамками этого доклада. Это сложная проблема, которая разрабатывается, в частности, в МГИМО уже более 10 лет, и требует глубокого обсуждения на различных уровнях власти. Пока же мы можем отметить только то, что сегодня никаких действенных механизмов международного регулирования не существует, в связи с чем регуляторные

функции ложатся на плечи национальных правительств или, что чаще, частных лиц и бизнеса.

На государственном уровне в России принят ряд законов, который ограничивает распространение информации в интернете и СМИ. Широко известно, что ввод этих законов был воспринят неоднозначно активными пользователями интернета – прежде всего, конечно, взрослыми сознательными людьми, которые воспринимают такие законы как ограничение их свобод. И действительно, упомянутые законы слабо проработаны с точки зрения практических методов их применения, а структур, которые могли бы следить за их выполнением, по сути не создано. В связи с этим ответственность за исполнение законов возлагается на структуры, которые обеспечивают доступ в интернет, на бизнес – а эти структуры просто не имеют достаточной мотивации проводить в жизнь принятые решения и решать технические и организационные вопросы вместо исполнительной власти. Нередко им проще просто прекратить предоставлять услуги, поскольку они становятся нерентабельными при исполнении внутренне противоречивого законодательства.

Поэтому едва ли стоит ожидать действенного решения проблемы контроля информации, распространяемой через интернет со стороны государства. Здесь образовательные учреждения, частные лица и, скажем, кафе, которые хотели бы предоставлять доступ в интернет своим посетителям, находятся в равной ситуации и вынуждены вырабатывать решения по ограничению доступа к информации самостоятельно.

К сожалению, арсенал средств, который мог бы быть использован для решения задач фильтрации информации, не отличается разнообразием. Наиболее эффективны технические аппаратные средства для осуществления интеллектуальной фильтрации, но их стоимость делает их совершенно недосягаемыми как для образовательных учреждений, так и для частных лиц и мелкого бизнеса. Не следует забывать и о том, что проблема ограничения доступа к информации является комплексной. Даже если она будет успешно

решена внутри отдельной школы – это можно сделать с использованием качественно настроенного фильтрующего брандмауэра, - она все равно сохранится вне учебного заведения: дома, на улице, в пунктах общественного доступа к интернету и т.п.

Следующая стадия решения проблемы могла бы заключаться в предоставлении самими учебными заведениями информации для настройки фильтрации на уровне домашних компьютеров вплоть до организации их доступа в интернет через школьный фильтрующий сервер. Такая централизованная схема позволит определять правила доступа учеников к информации согласовано, с привлечением специалистов или волонтеров, что избавит родителей от необходимости настраивать такие же фильтры самостоятельно, для чего большинство людей обычно не обладают достаточной квалификацией. Однако, такая схема все же требует довольно высокой квалификации технических специалистов и плотной работы с родителями, хорошего уровня организации процесса.

При принятии решения о создании централизованной системы фильтрации информации логичным следующим шагом становится добавление следующего уровня: центрального хранилища правил доступа, действующего на уровне региона, который обеспечивает синхронизацию всех установленных правил фильтрации для всех действующих учебных заведений. Такие системы в России уже используются провайдерами, но они осуществляют фильтрацию лишь заведомо незаконных ресурсов по решению суда. Более широкое их распространение на административном уровне могло бы способствовать созданию единой национальной системы фильтрации доступа к нежелательным ресурсам для учебных заведений. Но это пока лишь планы отдаленного будущего и их реализации вызывает сомнения в своей эффективности.

Даже при использовании качественно построенной системы фильтрации нежелательных ресурсов, можно назвать десятки способов пробить ее, или обойти. Здесь показателен опыт Китая, где использование общенациональной

системы фильтрации при действующем запрете на распространение определенных видов информации не оказывается эффективным – упомянутые фильтры лично докладчиком обходились при необходимости в течение нескольких минут. Заметим при этом, что в Китае мы имеем дело с системой фильтрации, создание которой потребовало много миллиардных вложений.

Следует четко понимать, что любая система фильтрации информации не является абсолютно устойчивой. Специалист, или даже технически образованный пользователь, способен обойти такие преграды, если у него есть мотивация это сделать. Информация о методах обхода таких фильтров широко представлена в интернете и при необходимости легко находится.

Но из этого не следует, что подобного рода механизмы фильтрации совершенно бесполезны. Они не блокируют полностью доступ к нежелательной информации, но серьезно осложняют его. Само по себе это отсекает от потребления такой информации высокий процент пользователей, не имеющих адекватной технической подготовки.

При этом не оставляет сомнений, что регулирование интернета должно развиваться. Это долгий и непростой с технической и социальной точек зрения процесс, где все решения должны приниматься взвешенно, чтобы не породить ситуацию ограничения свобод личности в пользу, казалось бы, лучшей, но на практике не отличающейся действенностью системы жесткой фильтрации информации. Здесь нет пока готовых ответов. Не исключено, что оптимальным окажется дифференцированный подход, особая, еще не сложившаяся правоприменительная практика, механизмы ювенальной юстиции. В любом случае, вопрос регулирования распространения информации требует дальнейшего широкого обсуждения как на национальном, так и на международном уровне.

Социальная сеть

Широкое распространение социальных сетей и социальных медиа ставит совершенно новые задачи в сфере обеспечения безопасности

образовательной среды, которые пока еще слабо осознаны. Принято считать, что социальные сети представляют собой лишь медиатор распространения информации, которая генерируется самими пользователями, частными лицами. Молниеносно распространяясь, она способна создавать панические настроения, формировать точку зрения больших масс людей, часто подменяя собой классические средства массовой информации, включая те из них, которые работают в поле интернета.

Кроме того, в отличие от средств массовой информации, социальные сети практически не регулируются законодательно. Одна из попыток их регулировать была предпринята как раз в России, где с недавних пор стали требовать регистрации популярных блогов и их владельцев как СМИ с соответствующей проекцией законодательных актов о СМИ на них. Такая практика едва ли окажется эффективной хотя бы по причине того, что частное лицо в принципе не способно следовать законодательству, регламентирующему деятельность СМИ. Таким образом, мы имеем дело с еще одной слабо проработанной законодательной инициативой, которую непонятно, как именно исполнять – практика применения закона не проработана и на ее создание и совершенствование уйдут еще годы.

В то же время зарубежные исследователи безопасности образовательной среды и работники учебных заведений выделяют совсем другой фактор опасности социальных сетей, с которым мы почти еще не сталкиваемся. Это киберхулиганство, запугивание и психическое давление, сексуальные домогательства и другие враждебные действия, реализуемые с использованием тех самых социальных сетей. В российской, еще не сложившейся, практике такие действия часто именуются «троллингом».

В России этот феномен практически не осознан, а в Европе лишь начинают приходить к его пониманию. В то же время проблема агрессии в социальных сетях остро стоит в Азии, в первую очередь в Японии. Именно там зарегистрировано большинство случаев доведения до самоубийства путем психического давления, оказываемого в виртуальной среде. В свою очередь,

накопленная в США статистика утверждает, что в той или иной степени агрессии в виртуальном пространстве подвергались свыше 44% учащихся, а в Канаде соответствующая цифра составляет 41%.

Европейские страны сталкиваются с описываемой проблемой в значительно меньшей степени по причине слабо распространенной практики виртуализации общения. В США и странах Азии сегодня свыше 60% всех взаимодействий подростки осуществляют через социальные сети, с использованием служб мгновенного обмена сообщениями, СМС и других электронных средств. Несложно понять, что с психологической точки зрения такое общение становится крайне выхолощенным – из него исключаются ряд сигнальных систем человека полностью. Но еще важнее понять, что данный формат подразумевает не общение личности с личностью, а двух психологических проекций между собой.

Дело в том, что при создании аккаунта в социальной сети любой человек неосознанно формирует свой образ, как избавленный от ряда недостатков, о которых он в себе осведомлен. Дополнительно могут добавляться вымышленные факты биографии, измененные личные данные. Таким образом формируется проекция в виртуальной среде, которая представляет не столько личность во всей ее полноте, сколько образ того, каким себя человек хочет видеть, аватар. Полнота и зрелость этого аватара серьезнейшим образом зависит от психической зрелости того, кто его создает, но еще и от его способностей описать внутренне непротиворечивую проекцию себя в виртуальном мире, что для детей и подростков, разумеется, почти невозможно – для этого требуется обладать подлинно писательским талантом. А поскольку формируемый образ дополняется вымыслом, изначально не полон – то эта проекция отличается крайней хрупкостью, еще большей, чем психика ребенка, который ее формирует. Таким образом, аватар человека в виртуальной среде общения чрезвычайно уязвим сам по себе, а при ограничении способов коммуникации только текстовыми

сообщениями лишен многих естественных защитных механизмов, оставляя психику человека, который стоит за аватаром, практически обнаженной.

В зарубежной практике принято считать, что осложняющим фактором является анонимизация такой травли. Давление на психику может производиться с использованием сразу нескольких виртуальных персонажей, контролируемых одним и тем же человеком. На практике, впрочем, такое происходит совсем не так часто. Ведь описываемые конфликты являются конфликтами тех самых виртуальных проекций, в каждую из которых их создатели вкладывают разные стороны своей личности. С учетом огромной численности этих аватаров всегда найдутся те, кто канализирует в интернет свою агрессию, таким образом самоутверждаясь, в то время как другие проецируют свои слабости. Их столкновения неизбежно будут происходить с соответствующими последствиями для психики. И проблема того, что «некому дать сдачи» в рассмотрении вопроса сильно преувеличена – на деле люди, привыкшие к такому выхолощенному виртуальному общению этот вариант почти не рассматривают.

Очевидно, что описанная проблема не имеет технического решения. В западной практике принято призывать к созданию различных сообществ, которые могли бы солидарно противостоять виртуальной агрессии, но признается, что это лишь полумера. Особенно наивно на фоне таких призывов смотрятся попытки создавать такие кружки групповой психотерапии в том же самом виртуальном пространстве.

Законодательные методы борьбы с агрессией в социальных сетях едва ли будут перспективны, поскольку факт собственно преступления (которое еще не осознано и не описано) крайне сложно доказать. Тем не менее, эта проблематика в той или иной мере требует защиты со стороны закона хотя бы для того, чтобы повысить уровень ответственности для тех, кто безоглядно переносит все виды социальных взаимодействий в виртуальное пространство.

Естественным способом противодействия «троллингу» является живое непосредственное общение, повышение его роли в гармоничном и всестороннем развитии личности. Ни в коем случае нельзя отмахиваться от этой проблемы – ведь интернет одновременно с созданием эффективных средств обмена информацией несет в себе и новые вызовы, одним из которых является описанное виртуальное общение и проблемы, которое оно несет в себе. Просто стоит помнить, что человеческая коммуникация сама по себе – нечто большее, чем обмен информацией, который предоставляется современной информационной средой. А нормальное, гармоничное воспитание и образование сегодня требует учета всех уже известных вызовов информационной среды и тех, которые только появятся в будущем.