ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БИБЛИОТЕК

Свергунова Н.М.

Россия, Орел, Орловский государственный технический универститет

Становление индустриального и постиндустриального общества, развитие науки и производства вызвали большой рост информации и знаний. Информационные процессы стали необходимым атрибутом обеспечения деятельности государственных органов, различных предприятий и организаций, отдельных граждан.

Все более возросла роль информационной сферы – совокупности норм, регулирующих взаимосвязанные области производства и преобразования информации, необходимых для формирования информационных ресурсов; получения и распространения информационных продуктов; предоставления информационных услуг; поиска; получения и потребления информации пользователями; создания и применения механизмов и средств обеспечения информационной безопасности.

Под информационной безопасностью понимается состояние защищенности национальных интересов Российской Федерации в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Информационная безопасность является одним из важнейших аспектов интегральной безопасности, на каком бы уровне ни рассматривалась бы последняя – национальном, отраслевом, корпоративном или персональном.

Обеспечение безопасности создаваемых и хранимых в библиотеках страны традиционных, магнитных и электронных информационных ресурсов, применяемых для этого технологий, должно рассматриваться как один из вопросов национальной безопасности РФ и тесно увязываться с утвержденной Концепцией национальной программы сохранения информационных ресурсов.

Рассматривая информационную безопасность как защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуре, необходимо найти правильный, с методологической точки зрения подход к проблемам информационной безопасности. Начинается он с выявления объектов информационных отношений и интересов субъектов, связанных с использованием информационных систем. К объектам информационной безопасности в библиотечной сфере относятся права и свободы личности, материальные и духовные ценности общества.

Информационная безопасность библиотек, прежде всего, рассматривается с точки зрения доступности информации. Можно выделить общедоступную информацию, конфиденциальную информацию (ограниченного доступа) и

информацию, составляющую государственную тайну (закрытая информация). Общедоступная информация свободно предоставляется, передается, тиражируется, распространяется по принципу: что не запрещено законом, то доступно. Именно общедоступная информация является объектом накопления, переработки, анализа, хранения в библиотеках.

Информационная безопасность – многогранная, можно сказать многомерная область деятельности, она не сводится исключительно к защите информации, это принципиально более широкое понятие. Здесь успех может принести только систематический, комплексный подход. Необходимо учитывать как интересы субъектов информационных отношений, так и меры защиты этих интересов.

Спектр интересов субъектов, связанных с использованием информационных ресурсов, можно разделить на следующие основные категории:

- доступность (возможность за приемлемое время получить требуемую информационную услугу);
- целостность (актуальность и противоречивость информации, ее защищенность от разрушения и несанкционированного изменения);
- конфиденциальность (защита от несанкционированного ознакомления).

Для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней:

- законодательного (законы, нормативные акты, стандарты и т.п.);
- административного (действия общего характера, предпринимаемые руководством организации);
- процедурного (конкретные меры безопасности, имеющие дело с людьми);
- программно-технического (конкретные технические меры).

Меры законодательного характера можно разделить на две группы:

- меры, направленные на создание и поддержание в обществе негативного (в том числе карательного) отношения к нарушениям и нарушителям информационной безопасности;
- направляющие и координирующие меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности.

Законодательство об информационной безопасности состоит из конституционных норм, ФЗ “О безопасности” от 05.03.92г., “О государственной тайне” от 19.09.97г., “О федеральных органах правительственной связи и информации” от 19.02.93г., ФЗ “Об информации, информатизации и защите информации” от 20.02.95г., ФЗ “Об участии в международном информационном обмене” от 04.07.96г., ФЗ “Об архивном фонде Российской Федерации и архивах” от 07.07.93г. и других актов, которые закрепляют правовые основы обеспечения безопасности личности, общества и государства, систему безопасности и ее функций, порядок организации органов, занимающихся

обеспечением безопасности, а также контролем и надзором за законностью в сфере обеспечения безопасности. Важное значение в руководстве деятельностью по обеспечению информационной безопасности личности, общества и государства принадлежит Совету безопасности РФ – конституционному органу, осуществляющему поддержку решений Президента РФ в этой сфере. В частности, с его участием была разработана Доктрина информационной безопасности Российской Федерации, утвержденная Президентом РФ 09.09.2001г.

Вместе с тем, законодательный уровень информационной безопасности не в полной мере соответствует потребностям общества и государства.

Административный уровень – белое пятно в отечественной практике информационной безопасности. Нет законов, обязывающих организации иметь политику безопасности. Ни одно из ведомств, курирующих информационную безопасность, не предлагает типовых разработок в данной области. Ни одно учебное заведение не готовит специалистов по разработке политики безопасности. Мало кто из руководителей знает что такое политика безопасности, еще меньшее число организаций такую политику имеют.

К процедурному уровню относятся меры безопасности относятся меры, реализуемые людьми. В отечественных организациях накоплен богатый опыт составления и реализации процедурных (организационных) мер, однако проблема состоит в том, что они пришли из докомпьютерного прошлого, и поэтому нуждаются в существенном пересмотре.

Можно выделить следующие группы процедурных мер, направленных на обеспечение информационной безопасности:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушение режима безопасности;
- планирование восстановительных работ.

На программно-технический уровень приходится львиная доля активности в области информационной безопасности.

Механизмы безопасности должны функционировать в разнородной, распределенной среде. Это означает, что программно-технические средства должны опираться на общепринятые стандарты, быть устойчивыми к сетевым угрозам, учитывать специфику отдельных сервисов.

Система информационной безопасности призвана обеспечить защиту информационных ресурсов библиотек и их информационно-телекоммуникационной инфраструктуры от воздействия чрезвычайных (т.ч. аварийных) ситуаций, компьютерного терроризма, применения оружия и других криминальных посягательств, а также от угроз, связанных с интенсификацией информационного обмена через Интернет.

Основные направления государственной информационной политики в этой области применительно к библиотекам можно сформулировать следующим образом:

- учет требований информационной безопасности при выработке стратегии политики библиотечной информатизации и осуществлении всех ее мероприятий;
- тесное взаимодействие мероприятий государственной информационной политики с мероприятиями, проводимыми в рамках государственной политики обеспечения информационной безопасности;
- выработка согласованной политики, правил и процедур интегрирования российских библиотек и их информационных ресурсов в международные телекоммуникационные сети, сводные каталоги, базы и банки данных;
- выработка и осуществление единой научно-технической политики государства в области создания технических средств обеспечения информационной безопасности всей структуры взаимодействия библиотек, применяемых в них информационных систем и технологий, а также их информационных ресурсов.

При рассмотрении проблем информационной безопасности необходимо учитывать в совокупности вопросы обеспечения безопасности: а)личности; б)информации; в) всей системы в целом.

Первым шагом в обеспечении информационной безопасности библиотек должен стать анализ угроз, как реальных (действующих в настоящий момент), так и потенциальных (могущих возникнуть в будущем).

Обеспечение информационной безопасности личности в сфере библиотечной деятельности имеет целью защиту конституционных прав и свобод человека и гражданина, связанных с развитием, формированием и поведением личности, свободой массового информирования, использования культурного, духовно-нравственного наследия, реализацией конституционных ограничений прав и свобод человека и гражданина в интересах сохранения и укрепления нравственных ценностей общества, традиций патриотизма и гуманизма, здоровья граждан, культурного и научного потенциала.

Законодательство РФ устанавливает право гражданина на получение информации и соответствующие обязанности библиотеки предоставлять эту информацию. Конституция Российской Федерации (ч.4. ст.29) официально закрепляет основополагающее право человека “свободно искать, получать, передавать, производить и распространять информацию любым законным способом”.

Обращаясь в библиотеку за получением какого-либо документа, пользователь реализует свое право на информацию путем осуществления конкретных действий в информационной сфере.

Удовлетворение прав и свобод личности в информационной сфере является первым этапом обеспечения информационной безопасности личности.

Выражаемая в определенных формах потребления, восприятия, информация в разных формах материального выражения используется обществом, его структурами как средство воспитания, организации, с одной стороны, и как средство разложения морального, разложения личности – с

другой. Она выполняет не только позитивную роль и несет позитивный заряд знания, но одновременно является опасным средством воздействия на сознание и поведение человека. Через информацию распространяются и негативные, и преступные намерения, и вредные сведения для здоровья, сознания и поведения человека.

Отсюда проблема информации как социального оружия.

Современные библиотеки – это не только источники идей, мыслей, технологий, материализованных в виде книг, журналов, диссертаций, но и автоматизированные информационные центры, имеющие в своей структуре медиатеки, интернет-кафе. Применяя в своей работе аудио- и видео-оборудование, спутниковое телевидение, интернет-технологии, библиотеки волей неволей могут стать распространителями приемов и сведений, наносящих вред личности гражданина (порнография, наркомания, бранные выражения, 25-й кадр, расистские высказывания, азартные игры и др.). Здесь же может иметь место манипулирование информацией (дезинформация, сокрытие или искажение информации).

Ограничение доступа к такого рода информации – следующий этап в обеспечении информационной безопасности личности.

В этой связи следует отметить явное несоответствие: с одной стороны – обеспечение неограниченного доступа к информационным ресурса, с другой – ограничение доступа к информации.

Нарушение технологической обработки информации также может стать проблемой информационной безопасности. Несвоевременная обработка и анализ поступающей информации; ошибки, неизбежные при обработке информации, особенно массовой; неправильное заполнение полей при вводе информации в автоматизированные библиотечные информационно-поисковые системы становятся тормозом, а порой и преградой в поиске и получении информации. Отсюда следует весьма распространенная в библиотеках ситуация: документ, который, может быть, крайне необходим читателю, десятилетиями остается невостребованным и в конце концов уничтожается как ненужный только потому, что читатель и не подозревал о его существовании. Такая ситуация нарушает основное право человека на информацию.

Поскольку библиотеки открывают уникальный доступ к информационным ресурсам, достижениям науки и техники, произведениям литературы, культуры, искусства, предоставляя своим читателям возможность знакомиться с книгами, периодическими изданиями, кинофильмами, видеофильмами, музыкальными произведениями и электронными документами, необходимо уделить внимание информационной безопасности как самих информационных ресурсов, так и содержащейся в них информации.

К числу угроз информационной безопасности информационных ресурсов, информации, самим библиотекам следует отнести:

- стихийные бедствия;
- пожары;
- производственные аварии;
- террористические акты;

- кражи;
- перехват информации;
- компьютерные преступления;
- использование некачественных продуктов для создания информационных ресурсов.

В отличие от всех остальных угроз, стихийные бедствия, производственные аварии, пожары, террористические акты являются угрозами не отдельным документам, а всему массиву информационных ресурсов, хранящихся в определенной библиотеке. Именно поэтому, при обеспечении информационной безопасности по этим направлениям следует уделить первоочередное внимание, повышая прочность зданий, сооружений, сантехнических устройств и т.д.; соблюдая правила пожарной безопасности.

Для обеспечения безопасности от краж как непосредственно самих информационных ресурсов, содержащихся на различных носителях (бумажных, магнитных, электронных), так и систем, обеспечивающих их эффективное взаимодействие (компьютерное оборудование, базы и банки данных) необходимо уделить особое внимание установкам сигнализационных и охранных систем.

Проблема перехвата информации, впрочем, как и компьютерных преступлений, особенно остро встала в период повсеместного внедрения современных информационных технологий.

При использовании технологий электронной доставки документов; электронной почты, а также и традиционных средств передачи информации (межбиблиотечный абонемент) проблема перехвата информации выходит на первый план, ставя во главу угла сохранность документов.

Среди компьютерных преступлений, наносящих вред информационным ресурсам, являются преступления против конфиденциальности и целостности компьютерных данных и систем, а также правил доступа к ним. Сюда относятся: незаконный доступ, вмешательство в данные; распространение компьютерных вирусов, “электронного мусора” (спамов).

И, наконец, еще одним немаловажным аспектом обеспечения информационной безопасности является использование “вечной бумаги”, поскольку самой большой опасностью для библиотек сегодня является использование в течение последних 150 лет так называемой “бумаги из целлюлозы кислотной варки”, обладающей “врожденной способностью” к самоуничтожению. На основе изложенного можно сделать нижеследующий вывод.

Свобода, процветание и развитие общества и личности принадлежат к основным человеческим ценностям. Однако, действенное участие в жизни общества возможно только при условии удовлетворительного образования, ровно как и свободного, неограниченного доступа к знаниям, идеям, культуре, информации. Именно поэтому, информационная безопасность Российской Федерации не мыслима без информационной безопасности основных хранилищ информационных ресурсов, их информационно-телекоммуникационной инфраструктуры. И обеспечение информационной безопасности является

первоочередной задачей всех сторон информационных отношений. В свою очередь, выполнение этой задачи невозможно без соблюдения вышеизложенных принципов.