БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

О.В. Балыко[1], О.Г. Пташинский[2]

[1] – студентка 3 курса, ФУС, группы УБНУ-2, Белорусского государственного экономического университета

[2] – научный руководитель, доцент кафедры информационных технологий, Белорусского государственного экономического университета, Минск 220672, Партизанский пр.,26.

Аннотация. В условиях развития и становления информационного общества особую актуальность приобретают проблемы обеспечения информационной безопасности. В работе будут отражены наиболее важные моменты по решению данной проблемы. Поэтому предлагаю рассмотреть вопросы о методах и способах защиты от информационно-психологического воздействия, о сертификации программных средств, а также правовое обеспечение информационной безопасности.

Ключевые слова: информационные системы, защита информационных систем, сертификация программных средств, правовое обеспечение информационной безопасности.

1. МЕТОДЫ И СПОСОБЫ ЗАЩИТЫ ОТ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ.

В настоящее время проблеме информационной безопасности уделяется большое внимание во всех сферах деятельности. Однако при этом само понятие такой безопасности трактуется, как правило, крайне узко и сводится зачастую лишь к защите от НСД.

Между тем эту проблему следует понимать гораздо шире. Так как в сфере обеспечения безопасности информации в качестве объектов рассматриваются: и право личности на доступ к информации, и право неприкосновенности частной жизни, и защита человека и общества от "вредной" информации, и многое иное. Одним из важнейших и одновременно наименее разработанных направлений, обеспечивающих безопасность и развитие жизненно важных интересов общества и каждого отдельного гражданина, является направление, связанное с методами и способами защиты от информационно-психологического воздействия.

Опасность такого воздействия, его распространенность в эпоху внешних и внутренних «информационных войн» выдвигают задачи обнаружения этих явлений и противостояния им на одно из первых мест в иерархии негативных последствий информатизации общества.

Косвенным признанием важности данной проблемы является, например, ее наличие в качестве одной из областей исследований в паспорте специальности 05.13.19 «Методы и система защиты информации и информационной безопасности» - «изучение методов и способов информационно-психологического воздействия на отдельные личности и людские ассоциации с помощью техническиех средств, на основании которых разрабатываются средства и методы выявления и манипулятивного воздействия и противодействия ему».

Информационно-психологическое воздействие известно и широко применяется с древнейших времен. Им всегда пользовались правители и политические лидеры, журналисты, писатели, учителя... Да, любой человек, пытающийся убедить в чем-то своего собеседника. Умелые ораторы, гипнотизеры, поэты всегда владели этим искусством. Тем не менее они не всегда могли объяснить, как это у них получается.

По-настоящему опасным информационно-психологическое манипулирование стало лишь с появлением и развитием научных методов такого воздействия.

В 1952 году американский психолог Чарльз Осгуд разработал метод семантического дифференциала (СД), позволяющий измерять так называемое коннотативное значение - те состояния, которые следуют за восприятием символа-раздражителя и необходимо предшествуют осмысленным операциям с символами. В методе СД измеряемые объекты оцениваются по ряду биполярных градуальных шкал, полюса которых заданы с помощью вербальных антонимов.

Современные психолингвистические и

психоакустические исследования показали, что фонетика речи оказывает довольно сильное воздействие на подсознание человека. При этом благодаря синестезии такое воздействие зачастую оказывается даже более сильным, чем воздействие на семантическом - сознательном уровне (А.П.Журавлев, А.А. Леонтьев, В.В. Левицкий).

В психотерапии новой волны выделяется направление, известное под названием нейро-лингвистического программирования (НЛП). Основная мысль здесь заключается в том, что наша речь является средством программирования чужого и своего собственного сознания.

Одна и та же мысль, но выраженная разными словами, не обязательно в устной форме, может вызвать совершенно разную реакцию. Она может усыпить, может оставить равнодушной, а может и подвигнуть к активным действиям. Примеров такого воздействия довольно много.

Отличительной особенностью методов НЛП является возможность использования, в частности, речи как средства психологического воздействия, причём в техниках НЛП это воздействие реализуется в основном на бессознательном уровне за счет незаметного проникновения во внутренний неосознаваемый мир человека.

Особенно опасными становятся подобные методы, когда для их реализации используются современные информационные технологии.

Примером такого рода является система ВААЛ.

Это психолингвистическая экспертная система. Основное ее назначение - оценка воздействия на подсознание человека русскоязычных текстов. Она также позволяет:

1) составлять тексты с требуемыми характеристиками воздействия;

2) оценивать воздействие на подсознание человека отдельных слов русского языка;

3) настраиваться на различные социальные и профессиональные группы людей, которые могут быть выделены по используемой ими лексике;

4) оценивать эффективность коммуникации по тому, к каким сенсорным каналам восприятия апеллируют в тексте.

Система ВААЛ реализована в виде многооконного текстового редактора. Она позволяет создавать новые и редактировать уже имеющиеся текстовые файлы. Текстовые файлы хранятся в виде ASCII кодов. Поэтому имеется возможность редактировать тексты, набранные в других редакторах, которые поддерживают импорт/экспорт файлов.

Последние версии системы ВААЛ обладают неизмеримо более богатыми возможностями анализа текстов. Они реализованы в виде расширения текстового процессора Microsoft Word 6.0/7.0 for Windows. Это дает возможность пользователю работать в привычной среде одного из наиболее популярных текстовых процессоров. В то же время посредством меню доступны различные функции ВААЛа для оценки и коррекции редактируемого текста. ВААЛ позволяет:

1) оценивать фонетическое воздействие;

2) производить коррекцию текста в желаемом направлении с использованием словаря синонимов на 25 тыс. слов;

3) оценивать нагрузку на каналы восприятия;

4) оценивать уровень агрессивности текста;

5) оценивать уровень архетипичности текста (сколь глубокие слои психики человека затрагиваются данным текстом);

6) оценивать уровень сексуальности текста в отношении использования языковых сексуальных символов по З.Фрейду, оценивать особенности употребления сексуальных символов в контексте употребления личных местоимений;

7) оценивать психологическую акцентуацию автора текста по пяти шкалам: гипертим-ности, демонстративности, возбудимости, цепрессивности, параноидальности.

Совершенно очевидно, что широкое распространение и использование подобных систем создает принципиально новую ситуацию, многократно повышает опасность массового манипулирования сознанием целых социальных групп и слоев, требует адекватных средств выявления скрытого воздействия, разработки соответствующих методов противодействия.

В настоящее время в Саратовском юридическом институте МВД РФ разрабатывается методика экспертной оценки текстов с целью обнаружения скрытого психологического воздействия.

2. СЕРТИФИКАЦИЯ ПРОГРАММЫХ СРЕДСТВ.

Важным условием эффективного использования программных средств защиты информации является научно-техническое и производственное обеспечение процессов создания, сертификации, архивизации, тиражирования, эксплуатации и идентификационного контроля. Задействованные в рамках данного обеспечения средства и методы должны позволять не только создавать и эффективно эксплуатировать новые компоненты программных средств защиты информации, но и улучшать характеристики ранее созданных компонентов.

При этом необходимо учитывать действие ряда объективных и субъективных факторов, повышающих уязвимость и снижающих безопасность и качество программных продуктов.

Основными объективными факторами являются:

1) усложнение режимов функционирования программных и аппаратных средств информационных систем: широкое внедрение многопрограммного режима, включая режимы разделения времени и реального времени;

2) организация сетевого межмашинного обмена информацией, в том числе и на больших расстояниях;

3) расширение круга пользователей, имеющих непосредственный доступ к ресурсам информационных систем и находящимся в них массивам данных;

4) постоянное увеличение объемов накапливаемой, хранимой и обрабатываемой информации;

5) сосредоточение в единых базах данных информации различного назначения и различной принадлежности.

К субъективным факторам относятся:

1) использование в информационных системах аппаратных и программных средств, заимствованных по неофициальным каналам, либо в качестве «НОУ-ХАУ»;

2) отсутствие контроля на необходимом уровне за качеством и корректностью разрабатываемых и производимых программных продуктов;

3) несовершенство технологических и инструментальных средств обеспечения всех этапов жизненного цикла программных продуктов;

4) несовершенство нормативной и законодательной базы в части безопасности и качества программных продуктов;

5) возможные изъяны в концепции архитектуры компьютеров, заключающиеся в излишней функциональной унификации средств вычислительной техники, предназначенных для работы в качестве объектных единиц, что позволяет компьютеру при обработке сбойных ситуаций изменять свои собственные управляющие программы на конкретных объектах.

Так как устранение объективных факторов, оказывающих отрицательное воздействие на безопасность и качество компьютерных систем, ущемляет интересы пользователей, основные усилия должны быть направлены на борьбу с перечисленными выше субъективными факторами, полное либо частичное устранение которых сможет существенно ослабить негативное влияние и объективных факторов.

Основными факторами, оказывающими позитивное влияние на безопасность и качество сертифицированных программных продуктов, являются:

1) тщательность и полнота формулирования требований к программным продуктам в задании на их разработку;

2) уровень инструментально-технологического, методического и организационного обеспечения разработки и сопровождения программных продуктов;

3) наличие средств контроля и обеспечения безопасности и качества программных продуктов на всех стадиях жизненного цикла;

4) наличие и уровень полноты законодательного, нормативно-технического и методического обеспечении процессов создания, оценки, эксплуатации и сопровождения программных продуктов;

5) наличие средств информационного обслуживания разработки, эксплуатации и сопровождения программных продуктов.

Разрабатываемые средства и методы сертификации должны устранять или блокировать все возможные пути реализации потенциальных угроз по:

- раскрытию информации о сертифицируемых программных продуктах, приводящему к нарушению конфиденциальности программных продуктов или его отдельных

элементов и заключающегося в том, что информация о программных продуктах может быть обнаружена и стать несанкционированно доступной отдельным лицам, модулям или процессам;

- компрометации информации о сертифицируемых программных продуктах или самих сертифицируемых программных продуктов, заключающейся в искажении информации о сертифицируемых программных продуктах или самих сертифицируемых программных продуктов, в результате чего необходимо предпринимать дополнительные усилия для выявления изменении и восстановления истинного состояния. Следствием использования скомпрометированной информации или программных продуктов является возможность принятия неверных решений со всеми вытекающими отсюда последствиями;

- отказу в обслуживании, вызывающему прекращение санкционированного доступа к ресурсам или задержку операций, критичных по времени выполнения для сертифицируемых программных продуктов;

- отказу от информации, связанной непосредственно с сертифицируемыми программными продуктами либо с результатами их деятельности, состоящему в непризнании получателем или отправителем фактов ее получения или отправки соответственно, а также отказа от авторства, т.е. отрицание причастности к какому-либо документу или версии сертифицируемых программных продуктов.

Источниками перечисленных угроз являются:

- несанкционированный доступ к информационным ресурсам, вследствие которого может произойти раскрытие и компрометация информации, а также отказ в обслуживании;

- ошибки разработчиков, изготовителей и обслуживающего персонала, в результате которых может произойти отказ в обслуживании, компрометация информации и несанкционированный доступ к информационным ресурсам;

- ошибки пользователей, которые могут проявляться в виде отказа от информации, повлечь ее раскрытие и компрометацию, а также вызвать отказ в обслуживании;

- физический отказ аппаратуры, являющийся основной причиной отказов в обслуживании, а в отдельных случаях вызывающий компрометацию и раскрытие информации.

Кроме непосредственного устранения и блокирования возможных путей реализации потенциальных угроз, средства и методы, входящие в состав научно-технического и производственного обеспечения сертификации программных продуктов, должны осуществлять своевременное обнаружение и ликвидацию последствий в случае их проявления.

Для достижения перечисленных целей в рамках организации сертификации программных продуктов следует обеспечивать комплексное использование и взаимодействие физических, аппаратных и программных средств защиты, дающих возможность:

- контроля и разделения всех попыток доступа как к сертифицируемым программным продуктам, так и к взаимодействующим с ними информационным ресурсам;

- шифрования конфиденциальной информации перед передачей по открытым каналам связи либо записью на недостаточно защищенный носитель, а также последующее ее расшифрование;

- идентификации объектов и проверку на принадлежность объекта некоторому субъекту либо объекту более высокого уровня, что одновременно может являться и подтверждением достоверности объекта;

- сертификации на безопасность инструментальных и технологических средств, используемых для разработки программных продуктов или взаимодействующих с ними на других этапах жизненного цикла;

- контроля за соответствием конкретной реализации сертифицируемого программного продукта его проектным решениям;

- контроля за правильностью функционирования и локализации причин, вызывающих отклонения;

- обеспечения логической целостности информации о сертифицируемых программных продуктах и ее восстановление в случае компрометации;

-протоколирования событий, позволяющее установить причины нарушения безопасности и качества сертифицируемых программных продуктов;

- регистрации и анализ сбойных ситуаций с целью своевременного обнаружения наиболее уязвимых мест в сертифицируемых

программных продуктах, а также попыток проведения атак на компьютерные системы;

- своевременного уничтожения информации, не предназначенной для дальнейшего хранения.

К программным средствам защиты относятся специальные программы, которые предназначены для выполнения логических (интеллектуальных) функций защиты и включаются либо в состав программного обеспечения систем обработки данных, либо в состав средств, комплексов и систем аппаратуры контроля за сертифицируемыми программными продуктами.

Все средства, отвечающие за реализацию механизмов защиты, в первую очередь сами они, должны быть безопасны и защищены от любого вмешательства в их работу.

Определение номенклатуры и характеристик средств, используемых для обеспечения безопасности и качества организации сертификации програмных продуктов, должно производиться в каждом конкретном случае в соответствии с документально оформленными требованиями.

3. ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Республика Беларусь имеет богатейший опыт в области электронизации народного хозяйства, компьютеризации и информатизации различных сфер деятельности. Не нужно доказывать, что информатизация привела к существенному повышению статуса информации как знания для принятия решений в сферах государственного управления, образования и научных исследований, финансово-кредитной, промышленного производства, бизнеса и др. Информация стала важнейшим ресурсом во всех сферах жизнедеятельности общества. Информационные системы на базе компьютерной техники стали основой систем управления важнейшими объектами инфраструктуры, обеспечивающей процессы жизнедеятельности в стране.

Зарубежные научные и профессиональные традиции, признавая определяющую гуманитарную суть информатизации, характеризуются прагматичным подходом к причинно-следственным связям между общественной потребностью в информации, технологическими инновациями в целом и между информатизацией и компьютеризацией в частности.

Разрабатывая в свое время программу информатизации страны, мы четко представляли положительный эффект этого процесса и пытались прогнозировать его отрицательные последствия, используя некоторые данные мирового опыта. Действительность оказалась намного мрачнее наших прогнозов. Нарушения информационной безопасности и компьютерные преступления стали реалиями нашей жизни. Национальное законодательство не успевает за развитием отношений в информационной сфере, не успевает соотносить механизмы реализации права в отношении компьютерных технологий, информационных продуктов и услуг с развитием этих технологий, информационной инфраструктуры и возможностями их использования.

Современные информационные технологии существенно меняют взаимодействие специфических законов развития техники (технократизм) и социальной среды (гуманизм) и, соответственно, правовой среды обитания человека как члена информационного общества. Скорость развития технологических средств информатизации уже сегодня начинает определенным образом диктовать отношения в информационном обществе, которые требуют своего правового и законодательного оформления.

Преимущество возможностей информационных технологий над механизмами правового регулирования отношений в информационной среде породило проблему информационной безопасности. Основными угрозами безопасности информационному обществу являются информационная война, информационный терроризм, информационный криминал. В основе их лежит противоправное использование современных средств информационных технологий для совершения преступлений в отношении физических и юридических лиц, государства, общества в целом, в том числе противоправных деяний в отношении информационных объектов, находящихся в собственности различных субъектов, с целью нанесения ущерба этим субъектам.

Обзор законодательства США в сфере

информатизации показывает, насколько актуальной является проблема регулирования отношений в информационной сфере, как тесно она увязана с проблемой информационной безопасности личности, государства, общества.

Республика Беларусь имеет достаточно хорошо развитую информационную инфраструктуру, однако создание информационных ресурсов, имеющих общественную значимость, и защита сообщений в информационных системах и коммуникациях идет медленными темпами. В условиях передела собственности и правовой неразберихи информационные ресурсы практически выпали из сферы, охраняемой государственными институтами.

Сложности возникают из-за несовершенства регулирования информационного взаимодействия государственных и негосударственных структур, недостатка системности в организации работ по формированию информационных ресурсов, отсутствия необходимых нормативных актов, стандартов. Мы не можем дать своей стране современные аппаратные средства связи и вычислительной техники и поэтому используем импортные средства.

То же касается и программных средств общего назначения. Большой бедой является уход высококлассных программистов в коммерческие структуры, работающие во многом на экспорт интеллектуальной продукции (США, Германия). Поэтому в системах государственных органов адаптируются импортные прикладные и системные продукты. Отсутствие документации на применяемые средства не дает возможности проверить их на наличие скрытых каналов и закладок. Специальное тестирование перед вводом в эксплуатацию систем на базе таких средств в настоящее время не дает гарантий провоциро-вания отказов, утечки информации.

В настоящее время на телефонных линиях устанавливается цифровое коммутационное оборудование зарубежного производства. Это сложные программно-технические комплексы, которые по сути дела не подконтрольны эксплуатирующим структурам, а его разработчики имеют возможность дистанционного несанкционированного их отключения, прослушивания, иных воздействий. В банковских и промышленных структурах остро стоит проблема защиты от хакерства.

Открытым по всем аспектам является вопрос о "ненападении" в информационной сфере, о мирном в этом отношении использовании космического пространства. В настоящее время международных договоров в этой сфере не существует.

Таким образом, проблема информационной безопасности для нашей республики является актуальнейшей. Она должна решаться с учетом собственного и мирового опыта защиты информационной инфраструктуры и национальных информационных ресурсов, налаживания международного информационного взаимодействия, обеспечивающего вхождение Беларуси в мировое информационное пространство без потерь для суверенитета республики и без ущерба субъектам, осуществляющим деятельность в информационной среде.

ЛИТЕРАТУРА

1. Кляуззе В.П. Безопасность и компьютеры. Нормы и рекомендации по безопасной эксплуатации вычислительной техники. – Минск., 2001, - 156 с.
2. Нехорошев А.Б. «О проблеме защиты от информационно-психологического воздействия» // Российско-белоруский научно-практический журнал Управление Защитой Информации, Том 5 №3, 2001, с.265-266
3. В.В. Анищенко, А.М. Криштофик «К вопросу о сертификации программных средств защиты информации» // Российско-белоруский научно-практический журнал Управление Защитой Информации, Том 5 №3, 2001, с.317-319