УДК 004.056.57:316.4

О. П. Пунченко, доктор философских наук, профессор, заведующий кафедрой философии и истории Украины (Одесская национальная академия связи им. А. С. Попова, Украина)

ЗАЩИТА ИНФОРМАЦИИ КАК МАРКЕР ЦИВИЛИЗАЦИОННОГО РАЗВИТИЯ ЧЕЛОВЕЧЕСТВА

В статье обосновывается сущность и жизненно важная необходимость защиты информации как маркера цивилизационного развития социума. Раскрываются основные системы, методы и средства защиты информации – криптографические, технические и социально-психологические. Раскрывается понятие информационной безопасности, которая структурирована по сферам деятельности человечества.

The article explains the essence and the vital need to protect the information as a marker of civilizational development of society. In addition, this article reveals the basic systems, methods and means of information protection – cryptography, technical and socio-psychological. Also is revealed the concept of information security, which is structured according to the spheres of human activity.

Введение. Анализ цивилизационного развития человечества позволяет выделить в этом процессе ряд мегатрендов и маркеров, игнорирование которых не позволяет объективно раскрыть сущностные и смысловые характеристики этого процесса. Среди многообразия маркеров, входящих в архитектонику цивилизаций, особое место принадлежит защите информации, решающей стратегическую задачу информационной безопасности социума.

Еще на заре становления традиционной цивилизации в истории человечества и целенаправленного развития информационного производства возникает необходимость защиты интеллектуальной собственности как отдельных ученых-теоретиков и практиков, так и государства в целом. «Охота» за интеллектуальной собственностью личности и государства породила, а затем и постоянно совершенствовался проблему защиты информации. В качестве примера можно вспомнить деятельность иранских компиляторов, которые все достижения Древней Индии и Древнего Китая перевели на персидский язык и в этом уже готовом виде преподнесли Европе. Нельзя думать, что все свои достижения Древняя Индия и Древний Китай «подарили» иранским компиляторам. Несомненно, в процессе защиты информации, недостаточно глубоко организованной, имела место «утечка» интеллектуальной собственности этих древних стран. «Можно вспомнить, что и секреты производства шелка, бумаги, фарфора, пороха, пушек, чертежи строительства больших кораблей, достижения в медицине, астрономии, математике и других науках, попали в Европу не в качестве дара Востока Западу. Причины необходимо искать в слабо организованной защите интеллектуальной собственности этих стран в тот период» [1, с. 288–289].

Но это не означает, что научной мыслью Древнего Востока и Запада не разрабатывались средства защиты информации и что их не интересовала информация о государственной тайне соседних государств. Об этом свидетельствуют различные теоретические источники, анализ которых показывает, что уже в этот период возникли организационная, техническая и криптографическая система защиты информации.

Защита информации, информационная безопасность социума – это не порождение XX века, они всегда были тесно связаны с развитием материального и духовного производства. Новации, складывающиеся в этих сферах различных стран, требовали своей защиты, организации информационной безопасности, поскольку они отражали разносторонние военные, политические, экономические и другие интересы конкретного государства. И сегодня защита информации, организация и реализация мер, направленных на информационную безопасность страны, выступают в качестве приоритетной деятельности любого государства.

Цель работы: на основе раскрытия основных типов защиты информации обосновать сущность информационной безопасности как постулирующего маркера современного этапа цивилизационного развития.

Основная часть. Если совершить краткий дискурс в историю формирования и особенностей развития средств защиты информации в страны Древнего Востока и Древнего Запада, то можно обнаружить в этих средствах общее, через социальные приоритетные направления деятельности государств, а также особенное, которое отражалось в методах защиты и функциональной деятельности тех, кто по роду занятий осуществлял информационную безопасность социума.

В Древней Индии основные задачи и методы защиты информации были заложены в древнеиндийском трактате. «Артхашастра» (букв. – наука о пользе, о практической жизни), который

составлялся примерно в 4 веке до н. э. – 2–3 вв. н. э. Этот трактат содержал собрание наставлений по управлению государством, где затрагивались вопросы защиты государственной информации.

Основное направление и главная задача защиты информации были связаны с защитой государственной тайны. Государственная тайна – это система сведений, сокрытие которых дает возможность государству обеспечить свою безопасность и преимущества над противником с наименьшими затратами сил и средств. Основная работа по защите государственной тайны осуществлялась агентами, в функции которых входило следующее: сбор информации в сфере государственного управления экономикой, внешней торговли; контроль и наблюдение за деятельностью отдельных должностных лиц; наблюдение за деятельностью и поведением каст: сбор информации в военной области – борьба с преступностью; охрана главы государства и контроль за его родственниками; выявление шпионов; внешний шпионаж; контроль за послами; пограничная охрана. Практически эти функции сохранились и сегодня, но они расширили свое содержание, а также возникло ряд новых направлений в сфере этой деятельности, особенно в XX веке.

Концепция информационной безопасности Древнего Китая наиболее полно нашла свое отражение в работе древнекитайского военного теоретика и полководца Сунь Цзы (в 6–5 вв. до н. э.). «Трактат о военном искусстве», проникнутого стихийной диалектикой (связь войны и политики, факторы победы, стратегия и тактика военных действий). В этом трактате особое значение отводилось защите информации как стратегического ресурса, необходимого для победы. Основу информации, подлежащей защите в первую очередь, также составляла государственная тайна. Она связана была не только с сохранением внутренней целостности китайской империи, но и с проводимой внешней политикой, которая была связана с постоянными войнами, которые вело государство.

Для защиты информации в Древнем Китае широко применялись такие методы как кодирование информации и ее дробление, то есть вводились элементы криптографии. С целью кодирования была введена система бирок из восьми уровней, каждый из которых отличается длиной, а она соответствовала определенному содержанию. Система кодирования была известна лишь императору и командующему войсками. В вышеназванном трактате были сформулированы задачи разведки и контрразведки, что относились к важнейшим функциям государства, поскольку это были эффективные методы предупреждения войн.

Что же касается Японии, то до установления феодального строя (5–8 вв. н. э.) конкретных источников и указаний по защите информации не обнаруживается. До указанного периода в этой стране были известны и применялись трактаты Древнего Китая о военном искусстве. С установлением феодального строя в Японии утверждается кодекс «Тойхоре» (701 г.), закрепивший результаты реформ Тайка. Эти реформы были осуществлены при императоре Котоку (645–654 гг.), они касались и защиты информации. Вся военная информация, военные источники и сочинения являлись секретными. В них отражено было содержание государственной тайны и методов государственного управления.

Японский кодекс «Тойхоре» оставался документом японского права вплоть до 60-х годов XIX века, когда в 1867–1868 гг. произошла незавершенная буржуазная революция, поскольку власть перешла к буржуазно-помещичьему блоку. В это время меняются основания феодального государства и кодекс утрачивает свою силу. В настоящее время в Японии широко используются методы и средства информации, о которых речь пойдет ниже.

Аналогичные Древнему Востоку задачи, функции и методы защиты информации, начиная с государственной тайны и включая различные стороны деятельности государства, например военную, обнаруживаются в странах Древнего Запада. Здесь начинают развиваться строго научные методы этого процесса, вначале криптографические средства защиты информации, а затем технические и социально-психологические.

Одно из древнейших криптографических устройств подарила Древняя Спарта – скиталу. «Первые сведения про использование шифров в военном деле, – пишут авторы «Современной криптографии», – связаны с именем спартанского полководца Лисандра (шифр скитала). Такой шифр использовали спартанцы для военных сообщений во время войны Спарты против Афин в V в. до н. э. Скиталою назвали деревянный валик, на который тщательно наматывали ленту пергамента или шкуры. Сведения писали рядками вдоль поверхности валика так, чтобы в рядке на один виток ленты выпадала только одна буква. Лента, снятая с валика, вмещала непонятную последовательность букв. Их можно было прочитать, только намотавши ленту на валик такого же диаметра . То есть, в этом случае ключом для прочтения сведения был диаметр валика» [2, с. 14].

Считается, что автором взлома шифра скиталы является Аристотель, который наматывал ленту на конусообразную палку до тех пор, пока не появились читаемые куски текста.

Древняя Греция и Древний Рим подарили миру и такие криптографические устройства и методы шифровки информации, как «диск и линейка Энея», «квадрат Полибия», «шифр Цезаря» и другие менее известные.

Все эти средства защиты информации прошли многовековой путь. Но сегодня законодательствами ряда ведущих стран закреплены два: криптографический и технический. Что же касается социально-психологических и других средств защиты информации, они законодательно не закреплены, их методика составляет государственную тайну.

Криптографическая защита информации – это вид ее защиты, который реализуется путем превращения информации с использованием специальных (ключевых) данных с целью сокрытия/возобновления содержания информации, подтверждения ее подлинности, целостности, авторства и тому подобное.

Криптографическая защита информации применяется для защиты информации, которая передается по каналам связи или хранится в базах данных, рабочих станциях, содержится у парольных и ключевых данных систем аутентификации и разграничения доступа. Потребителями услуг этой системы являются субъекты органов государственного управления, обороны, чрезвычайных ситуаций, правопорядка, национальной безопасности, разведки и тому подобное.

Техническая защита информации – это вид защиты информации, направленный на обеспечение с помощью инженерно-технических мероприятий и/или программных и технических средств недопущения утечки, уничтожения и блокировки информации, нарушения ее целостности и режима доступа к ней.

Система технической защиты информации представляет собой совокупность организационных структур, нормативно-правовых документов и материально-технической базы. В последнюю входят защитные технические средства и способы контроля за эффективностью всей системы технической защиты информации.

Техническая система защиты информации, согласно государственному стандарту, является совокупностью организационных структур, нормативно-правовых документов и материально-технической базы, в которую в свою очередь входят защищенные технические средства; средства технической защиты информации; средства контроля эффективности технической защиты информации, к которым можно отнести и криптографию.

Криптографические средства защиты информации здесь имеют узко ограниченное, но неотъемлемое применение. Они используются для защиты информации, которая хранится на носителях и передается по каналам связи между элементами информационной системы. Среди организационных средств защиты информации существенную роль играют услуги и механизмы защиты, связанные с персоналом.

Система технической защиты информации широко используется в информационно-технической борьбе с целью защиты информационной среды общества и защиты объектов информационной деятельности. Потребителями услуг этой системы защиты информации являются в большинстве случаев подразделения, которые защищают информацию с ограниченным доступом. Это банки, коммерческие структуры, структуры военной безопасности, что заставляет организовывать защиту по принципу «круговой обороны».

В современных условиях две вышеотмеченных системы защиты информации дополняются третьей – социально-психологическими средствами.

Социально-психологическая защита информации – это вид защиты информации, направленный на обеспечение с помощью организационных и психологических мероприятий, а при необходимости инженерно-технических и криптографических средств, противодействия влияния на информацию, уничтожения и блокировки информации, нарушения целостности и режима доступа к информации. Эта система играет не второстепенную роль, несмотря на то, что она не является ни идеологической системой, ни политическим органом, она преследует цель конкретного информационно-психологического влияния. Это влияние есть целенаправленное, заранее осмысленное производство и распространение специальной информации, которая вызывает непосредственное позитивное или негативное влияние на социальный капитал, на функционирование и развитие информационно-психологической среды общества, психику и поведение политической элиты, персонал экономической и технической инфраструктуры и население страны.

Какие бы системы защиты информации сегодня ни использовались – криптография, технические или социально-психологические, все они направлены на достижение безопасности. Понятие «безопасность» и «защита» тесно связаны между собой. Безопасность – это конкретное определенное состояние объекта или субъекта, при котором им не угрожает какого-либо вида опасность. Защита же выступает как действия, направленные на достижение конкретного вида безопасности.

Защита – это:

1) попытка предотвратить, оградить от неблагоприятных влияний, вмешательства;

2) средства для ограничения доступа и использования всей или части информационной системы; юридической, организационной, технической, а также мероприятия по предотвращению доступа к аппаратуре, программам и данным.

Защита информации – это организационные, программные и технические методы и средства ограничения доступа к информации, которая обрабатывается или хранится, но не подлежит всеобщей огласке.

Безопасность можно структурировать по сферам деятельности человечества.

Во-первых, это глобальная безопасность, отражающая состояние глобальных процессов, при которых обеспечивается гармоническое сочетание интересов народов, наций, государств и интересов всего человечества; эффективное решение задач, стоящих перед человечеством и различного рода отдельными администрациями; всестороннее развитие и обеспечение потребностей каждого человека.

Во-вторых, биологическая безопасность, включающая в себя экологическую, медицинскую, продовольственную, пожарную безопасность и охрану труда.

В-третьих, природная безопасность к которой необходимо отнести ресурсную, энергетическую, климатическую, производственную, а также безопасность от стихийных бедствий.

В-четвертых, социальная безопасность, главными задачами которой выступает обеспечение государственной, политической, экономической, военной, коммерческой, гуманитарной, психологической безопасности, а также безопасность персонала, потребностей, культурно-развлекательных мероприятий.

В-пятых, информационная безопасность, в которую входит обеспечение безопасности информационного пространства, информационных систем, электронного документооборота; киберсреды, персональных данных и др.

Информационная безопасность занимает особое положение в системе безопасностей. С одной стороны, она является составляющей и одним из механизмов любой безопасности ввиду того, что сбор и хранение информации должны обеспечить ее целостность и достоверность. Информация должна обрабатываться и распространяться для достижения целей обеспечения безопасности. С другой стороны, обеспечение информационной безопасности есть самостоятельная область деятельности ввиду ее роли и влияния на все стороны деятельности человека и социума.

Информационная безопасность – это:

1) состояние защищенности потребностей в информации личности, общества и государства, при котором обеспечивается их существование и прогрессивное развитие независимо от наличия внутренних и внешних информационных угроз и которое обеспечивается защитой от влияния некачественной информации, защитой информации и информационных ресурсов от неправомерного влияния на их содержание посторонних лиц, защитой прав и свобод человека и гражданина;

2) состояние защищенности информационной среды общества, которое обеспечивает его формирование, использование и развитие в интересах граждан, общества, государства;

3) состояние защищенности жизненно важных интересов личности, общества, государства в информационных отношениях.

С технологической стороны безопасность информации – это состояние информации, в котором обеспечивается сохранение определенных политикой безопасности свойств информации.

Как видим, информационная безопасность – это сложное многостороннее понятие, как и сама информация. Определение информационной безопасности зависит от особенности того объекта или субъекта, где она обеспечивается.

Одна из глобальных угроз современного информационного производства связана с экспоненциальным ростом объема информации. Возможности человека по восприятию и обработке информации ограничены. «Неконтролируемый рост объемов информации при существенных физиологических ограничениях на возможности ее обработки (восприятия и осмысление) может привести к информационному коллапсу» [3, с. 277]. Все большая часть информации будет передаваться для обработки автоматизированным интеллектуальным системам. Есть риск утери контроля над этими системами.

Однако можно возразить, что природа находит способы эффективной обработки и запоминания все большего объема информации. В сфере непрерывных систем и сигналов действует, например закон Вебера-Фехнера: «Раздражение любого из наших органов чувств отображается мозгом в виде ощущения, пропорциональном логарифму раздражения» [3, с. 167]. Благодаря этому существенно расширяется диапазон интенсивности воспринимаемых сигналов. В дискретной сфере и в области управления действуют законы иерархии. Каждый верхний уровень иерархии составляет свои объекты из элементов нижнего уровня. Число объектов, а также степеней свободы и число переменных уменьшается с ростом номера уровня иерархии. Это помогает справиться с огромными массивами информации.

Другая глобальная угроза состоит в следующем. Информационные технологии уже

значительное время развиваются стремительно, но экстенсивно. Значительное количество еще исправного компьютерного оборудования выбрасываются на свалку в результате их неоправданно быстрого морального старения. При этом огромное количество дефицитных редкоземельных материалов, которые используются в производстве электроники, попадает в естественную среду и отравляет ее. Информационная безопасность пронизывает всю систему национальных интересов – хозяйственную, техническую, военную, ресурсную, экологическую, энергетическую, финансово-денежную, медицинскую и другие. С этих позиций информационная безопасность государства выражает уровень защищенности его интересов от относительно опасных, дестабилизирующих, деструктивных влияний, которые способны поражать государственные интересы.

Информационная безопасность включает в себя защиту информационных систем, сетей, ресурсов, программных средств объектов интеллектуальной собственности и других активов, блокировки информации, ее несанкционированной утечки. Эта безопасность требует сегодня разработки нормативно-правовых документов, где должно быть четко выделено ядро государственного информационного ресурса, которое составляет государственную или другую предусмотренную законом тайну и подлежит защите.

Особое место среди различных видов и форм безопасности принадлежит безопасности личности. Информационная безопасность личности – это защищенность ее психики и сознания от опасных влияний манипулирования, дезинформации, побуждения к асоциальным действиям и т. д., что приводит к неадекватному восприятию ею действительности.

Существующие системы защиты информации ориентированы, в основном, на ее защиту с ограниченным доступом. Но в защите нуждается и большой массив открытой информации. Он постоянно растет, его трудно классифицировать с позиций применения средств защиты. Массив этой информации предстает как открытая система, ее нельзя скоррелировать линейно, а следовательно, методы и средства защиты должны носить неординарный, специфический характер, что будет свидетельствовать о постоянном расширении диапазона систем, методов и средств защиты интеллектуальной собственности государства и личности, укреплению их информационной безопасности.

Заключение. Все системы, методы и средства защиты информации тесно взаимосвязаны между собой и обеспечивают общую стратегию реализации главной функции страны – информационную безопасность. Вне этой функции современное информационное производство, с одной стороны, будет тормозиться субъективным фактором, не ощущающим защиты интеллектуальной собственности, а с другой стороны, будет способствовать расширению хаоса в этой сфере общественного производства. Ярким примером внесения хаоса в проблему информационной безопасности стран мира, особенно Европы, явилось разоблачение Э. Сноуденом американской системы прослушивания информации, являющейся и государственной, и личной тайной. Лидеры европейских стран резко осудили эту практику, а Россия заявила, что она разворачивает процесс «прослушивания информации в мировом пространстве», что вызывает не только недоверие между странами, но и новый виток информационной войны.

Таким образом, становление нового этапа цивилизационного развития человечества связано не только с производством, обработкой, передачей и хранением информации, но и с развитием средств и способов защиты ее как интеллектуальной собственности конкретного общества, конкретной личности.

Литература

1. Пунченко О. П. Цивилизационное измерение истории человечества. Одесса: Астропринт, 2013. 448 с.

2. Емец В., Мельник А., Попович Р. Современная криптография. Основные понятия. Львов: Атлас, 2003. 144 с.

3. Мунин П. И. Теория устойчивого развития. Информационные основы. М.: Книжный дом «Либроком», 2009. 312 с.

Поступила 14.01.2014