ПРОБЛЕМЫ ВНЕДРЕНИЯ В УКРАИНЕ СТАНДАРТОВ ЕВРОПЕЙСКОГО СОЮЗА В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИНИМАТЕЛЬСТВА

В. АБАКУМОВ,
соискатель
Харьковского национального университета внутренних дел

SUMMARY

The main standards of European Union in the sphere of entrepreneurship's informational security guaranteeing are analyzed in the article. Priority directions of developing the state policy of Ukraine in the sphere of entrepreneurship's informational security guaranteeing are suggested on the basis of analysis of European Union experience. It is concluded that corresponding national authority agencies have to actively participate in realizing necessary measures on a European level, to raise the level of cooperation with institutions of European Union and agencies of public administration of States parties, as well as to harmonize the legislation of Ukraine in accordance with European demands and standards in the sphere of guaranteeing informational security.

Key words: European Union, standards, informational safety, entrepreneurship.

* * *

В статье анализируются основные стандарты Европейского Союза в сфере обеспечения информационной безопасности предпринимательства. На основе анализа опыта Европейского Союза предлагаются приоритетные направления развития государственной политики Украины в сфере обеспечения информационной безопасности предпринимательства. Сделан вывод, что соответствующим национальным органам власти необходимо принимать активное участие в реализации комплекса необходимых мер на общеевропейском уровне, повышать уровень взаимодействия с институциями Европейского Союза и органами публичной администрации государств-участников, а также гармонизировать законодательство Украины в соответствии с европейскими требованиями и стандартами в сфере обеспечения информационной безопасности.

Ключевые слова: Европейский Союз, стандарты, информационная безопасность, предпринимательство.

Постановка проблемы. Обеспечение информационной безопасности предпринимательства в Украине является комплексной задачей, которая требует от соответствующих органов государственной власти реализации комплекса административно-правовых и организационных мер, направленных на обеспечение эффективности системы информационной безопасности субъектов хозяйственной деятельности.

Актуальность темы исследования. Качественное обеспечение информационной безопасности предпринимательской деятельности в Украине требует изучения и внедрения положительного опыта деятельности органов публичной администрации в зарубежных странах по обеспечению информационной безопасности, в том числе в сфере осуществления предпринимательской деятельности.

Состояние исследования. Проблемам изучения специфики обеспечения информационной безопасности уделяли свое внимание в научных работах такие ученые, как И. Л. Бачило, В. М. Гужва, В. И. Гурковский, В. М. Желиховский, Б. А. Кормич, И. Д. Лазаришина, В. А. Липкан, Ю. Е. Максименко, А. Г. Постевой, А. П. Сиротинская, Л. С. Харченко, А. К. Юдин и др. Однако необходимо обратить внимание, что в современной юридической науке на данный момент практически отсутствуют исследования, посвященные как вопросам обеспечения информационной безопасности предпринимательства в Украине, так и специфике деятельности органов публичной администрации зарубежных стран по обеспечению информационной безопасности предпринимательства. Учитывая евроинтеграционные стремления Украины и то внимание, которое в странах Европейского Союза уделяется вопросам защиты информации и обеспечения информационной безопасности во всех сферах жизнедеятельности общества, чрезвычайно актуальными являются вопросы разработки действенного административно-правового механизма обеспечения информационной безопасности предпринимательства в Украине с учетом опыта зарубежных стран.

Целью и задачей статьи является определение на основе анализа стандартов Европейского Союза в сфере обеспечения информационной безопасности предпринимательства приоритетных направлений развития государственной политики Украины в данной сфере.

Изложение основного материала. Прежде чем перейти непосредственно к изучению практики Европейского Союза в сфере обеспечения информационной безопасности предпринимательства, необходимо определиться с некоторыми теоретическими моментами: что такое информационная безопасность предпринимательства, какова ее цель, способы ее обеспечения.

Под информационной безопасностью предпринимательства следует понимать совокупность определенных на уровне нормативно-правовых актов, которые регламентируют предпринимательскую деятельность и определяют особенности защиты информации субъектами предпринимательской деятельности, и внутренних правил конкретного предприятия мер, направленных на защиту информационных ресурсов предприятий, нейтрализацию и ликвидацию угроз эффективному функционированию информационной системы субъекта предпринимательской деятельности и деятельности данного субъекта в целом.

Эффективное функционирование информационной безопасности предпринимательства невозможно без обеспечения ее стабильности, которое

достигается в результате деятельности органов государственной власти путем принятия необходимых нормативно-правовых актов и деятельности соответствующих субъектов, на которых возложена непосредственная обязанность по разработке и реализации нормативных, организационных и технических мер, направленных на обеспечение информационной безопасности на предприятии.

Целью обеспечения информационной безопасности предпринимательства является создание условий для беспрепятственного осуществления предпринимательской деятельности (предпринимательства) путем обеспечения эффективного функционирования информационной системы хозяйственной деятельности.

Особое внимание разработке действенной системы обеспечения информационной безопасности должны уделять крупные компании, т.к. именно им, в первую очередь, приходится решать вопросы организации работы удаленных пользователей корпоративных информационных систем. Для локальной сети этот вопрос не стоит так остро, а в случае, если коммуникативной средой является Интернет, то вопросы безопасности (в частности несанкционированный доступ, шифровка информационных потоков, защита компьютеров клиентов от заражения вирусами) стоят очень остро [1].

Таким образом, после того, как определены ключевые теоретические вопросы, касающиеся информационной безопасности предпринимательства, перейдем непосредственно к изучению стандартов Европейского Союза в сфере обеспечения информационной безопасности предпринимательства. Анализ данных стандартов будет способствовать разработке перспективных направлений повышения качества обеспечения информационной безопасности предпринимательства в Украине.

Первоначально позиция международного сообщества относительно необходимости обеспечения информационной безопасности во всех сферах жизнедеятельности европейского сообщества была определена на 56 сессии Генеральной Ассамблеи Организации Объединенных Наций. На данной сессии было закреплено, что информационная и сетевая безопасность означает защиту личной информации об отправителях и получателях, защиту информации от несанкционированных изменений, защиту от несанкционированного доступа к информации и создание надежного источника поставки оборудования, услуг и информации [2, с. 217].

Политика Европейского Союза в сфере обеспечения информационной безопасности основывается на таких составляющих:

- обеспечение прикладного характера правовых норм на основе общего понимания основных вопросов информационной безопасности и специальных мер ее обеспечения;

- необходимость постоянного совершенствования правового регулирования с учетом технического прогресса и порождаемых им новых угроз;

- потребность в дополнении рыночных механизмов политическими мерами;

- формирование европейского внутреннего рынка информационно-коммуникационных услуг [3, с. 94].

Одним из ключевых нормативно-правовых актов, принятых в рамках Европейского Союза в сфере обеспечения информационной безопасности, в том числе и в сфере предпринимательства, являются Рекомендации Комиссии Европейских Сообществ 94/820/ЕС от 19 октября 1994 года, касающиеся правовых аспектов электронного обмена данными [4]. Под электронным обменом данными следует понимать электронную межкомпьютерную передачу коммерческих и административных данных с использованием согласованного стандарта структуры сообщения электронного обмена данными.

В соответствии с данными рекомендациями, все экономические субъекты и организации, осуществляющие свою торговую деятельность с использованием электронного обмена данными, должны использовать Европейское типовое соглашение об электронном обмене данными. Особое внимание уделяется вопросам безопасности сообщений электронного обмена данными, в частности процедурам и мерам безопасности от рисков несанкционированного доступа, изменения, задержки, уничтожения или утраты информации; конфиденциальности и защите персональных данных.

Таким образом, можно сделать вывод, что Рекомендации Комиссии Европейских Сообществ 94/820/ЕС от 19 октября 1994 года являются одним из шагов в направлении обеспечения информационной безопасности функционирования как отдельных субъектов предпринимательской деятельности, так и предпринимательства в целом.

В Рекомендациях Комиссии Европейских Сообществ 97/489/ЕС от 30 июля 1997 года, касающихся сделок, совершаемых с использованием электронных платежных инструментов и, в частности, отношений между эмитентом и держателем [5], особое внимание уделяется прозрачности условий сделок, которые совершаются субъектами предпринимательской деятельности; особенностям работы с информацией после совершения сделки; вопросам ответственности субъектов предпринимательской деятельности за несоблюдение правил работы с информацией; перечень обязанностей, которые возникают в связи с совершением сделки (предпринимательской деятельности); порядок разрешения споров и т.д.

В связи с необходимостью разработки действенного механизма защиты персональных данных принята Директива 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 года о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных [6]. Данная директива преимущественно касается физических лиц («субъектов данных»): ее нормами определен порядок сбора, записи, организации, хранения, изменения, извлечения, использования, раскрытия посредством передачи, распространения информации, связанной с идентифицированным или идентифицируемым физическим лицом. Однако следует отметить, что во время осуществления предпринимательской деятельности, которая в последнее время происходит с учетом развития информационных технологий и уровня прогресса информационного общества, также можно наблюдать циркуляцию различной информации, в том числе и информации, связанной с персональными данными физических лиц.

В данном контексте следует упомянуть о таком направлении предпринимательской деятельности как виртуальная экономика или электронная коммерция (интернет-магазины, электронные платежи, денежные переводы), т.к. именно в этих случаях существуют риски утечки информации о физических лицах – продавцах, покупателях, инвесторах, кредиторах и заемщиках (их идентификационные номера, данные паспортных документов, номера платежных карточек и их коды). Это вызвано недостаточным решением проблем информационной безопасности в сетях информационных систем виртуальной экономики, развитием информационной системы виртуальной экономики, в результате чего формируются новые более разнообразные и масштабные проявления угроз в виде компьютерных преступлений [7, с. 388-389].

Особое внимание следует обратить также на Директиву 2002/58/ЕС Европейского парламента и совета от 12 июля 2002 года, касающуюся обработки персональных данных и охраны тайны частной жизни в секторе электронных коммуникаций [8]. В данной директиве определен порядок обработки персональных данных в связи с оказанием в рамках Европейского Союза общедоступных услуг электронных коммуникаций по сетям коммуникаций общественного пользования; сформулированы гарантии уровня безопасности, соответствующего представляемому риску. В соответствии с положениями Директивы 2002/58/ЕС от 12 июля 2002 года государства-участники обеспечивают через национальное законодательство конфиденциальность сообщений и связанных с ними данных трафика с использованием коммуникационных сетей общего пользования и общедоступных услуг электронных коммуникаций [8].

Необходимо отметить, что положения данной Директивы непосредственно не предусматривают порядок обеспечения безопасности хранимой информации, приобретения доступа к информации, обработки информации, касающейся конкретного субъекта хозяйственной деятельности, или предоставления каких-либо других информационных услуг. Но, хотелось бы обратить внимание, что основными правилами обработки данных должны руководствоваться все субъекты (пользователи или абоненты коммуникационных сетей общего пользования и общедоступных услуг электронных коммуникаций), деятельность которых имеет отношение к информации, электронным коммуникациям, в том числе и субъекты предпринимательской деятельности.

В контексте анализа опыта зарубежных стран в сфере обеспечения информационной безопасности предпринимательства необходимо проанализировать также основные положения Международного стандарта ISO/IEC 27002 «Информационные технологии. Свод правил по управлению защитой информации», нормами которого закреплены руководящие и основные принципы управления защитой информации в организации [9]. С помощью данного международного стандарта любой субъект, деятельность которого связана со сбором, использованием информации (в том числе и субъект предпринимательской деятельности), сможет разработать и внедрить с учетом специфики своей деятельности действенную систему защиты информации, а также разработать собственную методику управления защитой информации.

Стратегия конкретного предприятия в сфере управления защитой информацией должна быть распространена по всей организации пользователям в форме, которая должна являться доступной и понятной всем сотрудникам [9].

А.А. Смирнов указывает, что в Европейском Союзе к числу основных мер противодействия угрозам информационной безопасности относятся:

- повышение осведомленности, обмен передовым опытом, в том числе и в сфере обеспечения информационной безопасности предпринимательской деятельности;
- учреждение Европейской системы предупреждения и информирования;
- обеспечение технологической поддержки, связанной со стратегией развития системы информационной безопасности;
- обеспечение рыночно ориентированных способов стандартизации и сертификации;
- обеспечение безопасности в правительственных учреждениях;
- международное взаимодействие, предусматривающее как расширение диалога между государствами-участниками по поводу повышения эффективности обеспечения информационной безопасности предпринимательства, так и диалога самих субъектов предпринимательской деятельности [3, с. 96-97].

Комплексное решение перечисленных мер на уровне соответствующих органов публичной администрации государств-участников Европейского Союза, активное участие субъектов предпринимательской деятельности в разработке государственной политики являются крайне важными элементами формирования и реализации европейской политики в сфере обеспечения информационной безопасности во всех сферах жизнедеятельности общества, в том числе и в сфере предпринимательства.

Таким образом, в рамках данной работы коротко проанализированы основные стандарты Европейского Союза в сфере обеспечения информационной безопасности, которые могут применяться также в деятельности различных субъектов предпринимательской деятельности. В результате проведенного анализа можно сделать вывод о необходимости имплементации данного опыта в Украине как на уровне национального законодательства, так и на уровне внутренних норм и правил, которые разрабатываются и применяются в отдельных субъектах предпринимательской деятельности. Разделяем точку зрения А.А. Смирнова, что с учетом технического прогресса и порождаемых им новых угроз соответствующим органам исполнительной власти необходимо постоянно предпринимать меры по совершенствованию законодательства [3, с. 94].

В связи с этим необходимо принять соответствующий нормативно-правовой акт, в котором была бы сформулирована общая стратегия обеспечения информационной безопасности субъектов предпринимательской деятельности всех форм собственности и предусмотрена обязанность данных субъектов на ее основе разрабатывать собственную стратегию безопасности с учетом

специфики своей деятельности. Целью принятия данной стратегии должно быть обеспечение перехода к экономике, осуществляемой с помощью информационных технологий, противодействие использованию потенциала информационных и коммуникационных технологий в целях нанесения ущерба субъектам предпринимательской деятельности в Украине, что в результате должно привести к эффективному обеспечению информационной безопасности предпринимательства. Необходимо также обратить внимание на целесообразность разработки региональных целевых программ по обеспечению информационной безопасности предпринимательства в конкретном регионе страны.

Особое внимание должно быть уделено разработке процедур обращения с информацией, хранения информации, защиты этой информации от неразрешенного раскрытия или неправильного использования. В данном случае во время разработки системы защиты информации необходимо учитывать вид информации: информация в документах, компьютерных системах, сетях, мобильных компьютерных средах, мобильных системах связи, электронной почте, голосовой почте и т.д. Необходимо также предусмотреть возможность осуществления соответствующими органами исполнительной власти контроля над соблюдением субъектами предпринимательской деятельности ключевых правил информационной безопасности. В связи с этим чрезвычайно актуальным является вопрос постоянного совершенствования правоприменительной практики в сфере обеспечения информационной безопасности предпринимательства в Украине.

Выводы. Подводя итог сказанному, можно резюмировать, что в Европейском Союзе информационная безопасность рассматривается как одно из основных условий успешного развития информационного общества, в связи с чем большое внимание уделяется обеспечению информационной безопасности во всех сферах жизнедеятельности, в том числе и в сфере предпринимательства. Учитывая это, а также евроинтеграционные стремления Украины, соответствующим национальным органам власти необходимо принимать активное участие в реализации комплекса необходимых мер на общеевропейском уровне, повышать уровень взаимодействия с институциями Европейского Союза и органами публичной администрации государств-участников, а также гармонизировать законодательство Украины в соответствии с европейскими требованиями и стандартами в сфере обеспечения информационной безопасности. Надлежащее выполнение перечисленных действий в результате приведет к стабильному развитию предпринимательства в Украине, выходу украинских предприятий на европейский и мировой рынок, повышению имиджа страны на международной арене.

Список использованной литературы:

1. Інформаційна безпека – одна із основних складових успішного бізнесу сучасного підприємства / В.І. Мазур, О.Ю. Мазур, О.В. Іванкевич, О.О. Мелешко // Науково-технічний журнал «Захист інформації». – 2007. – № 3. – С. 69-76.

2. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції : навчальний посібник / В.А. Ліпкан. – К.: КНТ, 2006. – 280 с.

3. Смирнов А.А. Обеспечение информационной безопасности в условиях виртуализации общества: опыт Европейского Союза : монография / А.А. Смирнов. – М.: ЮНИТИ-ДАНА, 2011. – 196 с. [Электронный ресурс] – Режим доступа: http://spkurdyumov.narod.ru/smirnov.pdf

4. Commission Recommendation 94/820/EC of 19 October 1994 relating to the legal aspects of electronic data interchange // Official Journal of the European Communities. – 1994. – L 338. – P. 0098-0117.

5. О сделках, совершаемых с использованием электронных платежных инструментов и, в частности, отношений между эмитентом и держателем : Рекомендации Комиссии Европейских Сообществ 97/489/ЕС : от 30.07.1997 // Official Journal of the European Communities. – 1997. – L 208.

6. О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных : Директива 95/46/ЕС Европейского парламента и Совета Европейского Союза : от 24.10. 1995 [Электронный ресурс] – Режим доступа : http://tzi.com.ua/21.html

7. Протидія економічній злочинності / П.І. Орлов, А.Ф. Волобуєв, І.М. Осика, Р.Л. Степанюк, І.М. Зарецька, Едвард Картер, Річард Ворнер. – Харків: Нац. ун-т внутр. справ, 2004. – 568 с.

8. Об обработке персональных данных и охране тайны частной жизни в секторе электронных коммуникаций : Директива 2002/58/ЕС Европейского парламента и совета : от 12.07.2002 [Электронный ресурс] – Режим доступа : http://nlau.edu.ua/tempus/library/doc/ecom/add/Add10.pdf

9. Информационные технологии. Свод правил по управлению защитой информации : международный стандарт ISO/IEC 27002 [Электронный ресурс] – Режим доступа : http://www.pqm-online.com/assets/files/standards/iso_iec_27002-2005.pdf