МРНТИ 10.87.89

Раев А.

докторант Алматинской академии МВД Республики Казахстан
имени Макана Есбулатова, майор полиции, Казахстан, г. Алматы,
e-mail: mvdas88@gmail.com

УГОЛОВНО-ПРАВОВАЯ ОХРАНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННОМ ЗАРУБЕЖНОМ ЗАКОНОДАТЕЛЬСТВЕ

В представленной работе проводится комплексный анализ преступлений против информационной безопасности. Уточняются их понятие и система, рассматриваются вопросы оптимизации уголовно-правового регулирования. Автор выделяет информационную безопасность в качестве самостоятельного объекта уголовно-правовой охраны. Обосновывается положение о том, что информационная безопасность может выступать как основным, так и дополнительным объектом посягательства. Об актуальности выбранной темы свидетельствует тот факт, что борьба с преступлениями в информационной сфере является одной из главных задач правоохранительных органов не только Казахстана, но других стран. Автором проанализирован позитивный зарубежный опыт закрепления национальных стратегий по обеспечению кибербезопасности. В этом аспекте немалый научный интерес представляет анализ законодательных инициатив и механизмов, которые обеспечивают кибербезопасность в США. В рамках работы подробно освещены актуальные направления стратегий обеспечения информационной безопасности в таких передовых европейских странах, как Великобритания, Германия, Франция, Швеция, Швейцария и др. Рассматриваются возможности использования накопленного зарубежного опыта в отечественном уголовном законодательстве. В рамках статьи сформулированы предложения по дальнейшему совершенствованию уголовного законодательства Республики Казахстан в этом направлении.

Ключевые слова: информационная безопасность, кибербезопасность, национальная стратегия противодействия преступности, уголовные правонарушения против информационной безопасности, уголовная ответственность.

Raev A.

Doctoral student of the Makan Yesbulatov, Almaty academy of the Ministry
of Internal Affairs of the Republic of Kazakhstan, major of police, Kazakhstan, Almaty,
e-mail: mvdas88@gmail.com

Criminally-legal protection of information security in modern foreign legislation

In the work presented, a comprehensive analysis of crimes against information security is conducted. The task is to clarify their concept and system, to consider the optimization of criminal law regulation. The author singles out information security as an independent object of criminal-legal protection. The author substantiates the provision that information security can act as the main and additional object of encroachment. The relevance of the chosen topic is evidenced by the fact that the fight against crimes in the information sphere is one of the main tasks of the law enforcement bodies of not only Kazakhstan but other countries. The author analyzes the positive foreign experience of developing national strategies for ensuring cybersecurity. In this aspect of scientific interest is the analysis of legislative initiatives and mechanisms that ensure cybersecurity in the United States. In the framework of the work, the current trends in information security strategies in such advanced European countries as the United Kingdom, Germany, France, Sweden, Switzerland and others are described in detail.The possibilities of using the accumulated

foreign experience in the domestic criminal legislation are analyzed. The article formulates proposals for further improvement of the criminal legislation of the Republic of Kazakhstan in this direction.

Key words: information security, cybersecurity, a national strategy for combating crime, criminal offenses against information security, criminal liability.

Раев А.

Қазақстан Республикасы ІІМ Мақан Есболатов атындағы
Алматы академиясының докторанты, полиция майоры, Қазақстан, Алматы қ.,
e-mail: mvdas88@gmail.com

Қазіргі шетелдік заңнамасында ақпараттық қауіпсіздікті қылмыстық-құқықтық қорғау

Жұмыста ақпараттық қауіпсіздікке қарсы қылмыстардың кешенді талдауы жүргізілуде. Олардың түсініктемесі мен жүйесін айқындау, қылмыстық-құқықтық реттеуді оңтайландыру мәселелері қарастырылады. Автор ақпараттық қауіпсіздікті қылмыстық-құқықтық қорғаудың дербес объекті ретінде таңдайды. Автор ақпараттық қауіпсіздік қылмыстың негізгі және қосымша объектісі ретінде бола алады деген ережені негіздейді. Ақпараттық саладағы қылмыстарға қарсы күрес тек Қазақстан ғана емес, басқа елдердің құқық қорғау органдарының басты міндеттерінің бірі болып табылатыны таңдалған тақырыптың өзектілігін растайды. Авторлар киберқауіпсіздікті қамтамасыз ету жөніндегі шетелдік ұлттық стратегиялардың оң тәжірибесін талдайды. Осы тұрғыдан алғанда, АҚШ-тағы киберқауіпсіздікті қамтамасыз ететін заңнамалық бастамалар мен тетіктердің айтарлықтай талдауы елеулі ғылыми қызығушылық тудырады. Жұмыстың шеңберінде Ұлыбританияның, Германияның, Францияның, Швецияның, Швейцарияның және басқа да алдыңғы қатарлы еуропалық елдердегі ақпараттық қауіпсіздік стратегиясының қазіргі үрдістері толығырақ сипатталған. Отандық қылмыстық заңнамаға жинақталған шетелдік тәжірибені пайдалану мүмкіндіктеріне назар аударылады. Осы мақала нәтижесінде Қазақстан Республикасының қылмыстық заңнамасын одан әрі жетілдіру мақсатында ұсыныстар әзірленді.

Түйін сөздер: ақпараттық қауіпсіздік, киберқауіпсіздік, қылмысқа қарсы күрестің ұлттық стратегиясы, ақпараттық қауіпсіздікке қарсы қылмыстық құқық бұзушылықтар, қылмыстық жауапкершілік.

Введение

Современный уровень информационных технологий обусловил не только переход национальных экономик и социальных структур на принципиально новый уровень развития и функционирования, но и привел к возникновению новых угроз безопасности, породив целый комплекс негативных последствий. Отражением таких угроз стало появление новых терминов, как информационная атака, информационное оружие, информационный терроризм, информационная война, а также революции и перевороты с использованием информационных технологий и т.п. Их разрушительное воздействие вполне сопоставимо с применением оружия массового уничтожения.

При рассмотрении способов и приемов уголовно-правовой охраны информационной безопасности в зарубежном законодательстве необходимо четко очертить само содержание данного понятия.

По мнению А.В. Мнацаканян, информационная безопасность отдельных государств в международном информационном пространстве включает в себя:

1) безопасность информационного пространства государства от информационных угроз, информационных операций, информационного давления и информационных войн со стороны других акторов международных информационных отношений;

2) защиту государственного информационного рынка от незаконных посягательств акторов международных информационных отношений;

3) защиту и ограничение международного оборота информации в целях государственной информационной безопасности;

4) построение и обеспечение надлежащего функционирования информационного общества;

5) защиту своих частных лиц от незаконных посягательств акторов международных информационных отношений и т.д. (Мнацаканян, 2015: 51).

Основная часть

О приоритетности вопросов обеспечения информационной безопасности однозначно высказался Президент Казахстан Н.А. Назарбаев в своем Послании «Третья модернизация Казахстана: глобальная конкурентоспособность», по-

ручив Правительству и Комитету национальной безопасности разработать систему «Киберщит Казахстана» (Назарбаев, 2017: 2).

Необходимо отметить, что первые национальные стратегии информационной безопасности за рубежом начали появляться в начале XXI века.

Начало процесса было положено с принятием в США National Strategy to Secure Cyberspace (2003), выступавшей частью National Strategy for Homeland Security, напрямую связанной с последствиями терактов 11 сентября 2001 года. В 2005 году в Германии был принят National Plan for Information Infrastructure Protection (NPSI). В 2006 году Швеция принимает Strategy to improve Internet security in Sweden. В 2008 году Эстония, впервые среди членов Европейского союза, публикует национальную стратегию кибербезопасности. С указанного времени явление приобретает лавинообразный характер, Стратегии принимаются большинством стран Евросоюза, причем в национальных стратегиях отражаются некоторые специфические особенности (Елин, 2016: 22).

Национальная стратегия кибербезопасности США определяет векторы политики по семи основным направлениям: экономика, защита информационных сетей, применение права, оборона (Вооруженные силы), управление Интернетом, международное развитие и свобода Интернета. США заявляют о своей приверженности политике сохранения и расширения преимуществ цифровых сетей для общества и экономики. Вместе с тем, признается, что рост этих сетей приводит к новым вызовам для национальной и экономической безопасности, а также для всего мирового сообщества.

В американской национальной стратегии кибербезопасности отмечается, что США будут противостоять злоумышленникам, разрушающим системы и сети, используя при этом необходимые и адекватные методы и средства.

Если проанализировать меры в сфере правоприменения, предусмотренные в Национальной стратегии кибербезопасности США, то в качестве таковых предусмотрены следующие:

– активное участие в разработке международной политики в сфере киберпреступности;

– гармонизация законов о киберпреступности на международном уровне путем присоединения к Будапештской конвенции;

– совершенствование законодательства путем противодействия незаконной деятельности, а не путем ограничения доступа в Интернет;

– пресечение возможности использования Интернета террористами и другими преступниками для оперативного планирования нападений и их финансирования (International Strategy for Cyberspace: 30).

Надо отметить, что вышеназванная Будапештская конвенция – это Европейская конвенция по киберпреступлениям (преступлениям в киберпространстве), которая была принята в Будапеште 23 ноября 2001 года. Целью Конвенции является предотвращение правонарушений, направленных против конфиденциальности, целостности и доступности компьютерных систем, сетей и данных, а также неправомерного использования указанных систем, сетей и данных через придание этим действиям статуса преступления, а также путем применения властных полномочий, достаточных для эффективного противодействия указанным правонарушениям путем облегчения обнаружения, расследования и судебного преследования указанных правонарушений (http://inter.criminology.onua.edu.ua/materials).

В указанной Конвенции впервые была представлена классификация преступлений против информационной безопасности (киберпреступлений). В нее вошли, в частности, преступления против конфиденциальности, целостности и доступности компьютерных данных и систем (незаконный доступ к компьютерной системе, незаконный перехват компьютерных данных, вмешательство в компьютерные данные, ненадлежащее использование устройств), преступления, связанные с компьютерами (подлог компьютерных данных, компьютерное мошенничество); правонарушения, связанные с содержанием (преступления, связанные с детской порнографией); преступления, связанные с нарушением авторского права и смежных прав.

Например, в ряд статей УК Голландии, предусматривающих ответственность за совершение традиционных преступлений (вымогательство (ст. 317, 318), запись (прослушивание, копирование) информационных коммуникаций, кража путем обмана служб (ст. 362 с)), были внесены дополнения в редакции других статей (саботаж (ст. 161, 351), подлог банковских карточек (ст. 232)), даны специальные разъяснения. Были значительно изменены такие составы, как шпионаж (ст.ст. 98, 98a), вмешательство в коммуникации (ст. 139a, 139b), порнография (ст. 240b), что позволяет в настоящее время использовать данные составы преступлений, в соответствующих слу-

чаях, и для борьбы с компьютерными преступлениями (Громов, 2006: 33).

В Уголовном кодексе ФРГ отсутствует отдельный раздел, содержащий составы «компьютерных» преступлений. Соответствующие нормы встречаются в различных разделах кодекса. Например, состав «компьютерного мошенничества» включен в раздел XXII Особенной части «Мошенничество и преступное злоупотребление доверием», он примыкает к основному составу мошенничества. Параграф 263а законодательно устанавливает новую форму специфических действий, направленных на причинение вреда чужому имуществу. При этом человек вводится в заблуждение только посредством использования компьютерной техники. На основании параграфа 263а УК ФРГ, «тот, кто умышленно или с намерением создать для себя или третьего лица противоправную имущественную выгоду, наносит ущерб другому лицу тем, что влияет на результат обработки данных, создавая неправильные программы, используя неправильные или неполные данные, неправомочно используя данные или иным образом неправомерно воздействуя на указанный процесс, наказывается лишением свободы на срок до 5 лет или денежным штрафом» (Dvoretskiy, 2006: 33).

Уголовный кодекс Швейцарии в рассматриваемой части аналогичен Уголовному кодексу ФРГ. Наряду со ст. 146 раздела «Преступные деяния против имущества», устанавливающей уголовную ответственность за традиционное мошенничество, существует ст. 147 «Мошенническое злоупотребление с установкой для обработки данных». На основании данной статьи уголовно наказуемым признается мошенничество, совершенное путем неправильного, неполного или неправомерного использования данных, что может воздействовать также на процесс обработки или передачи данных» (Dvoretskiy, 2006: 34).

Национальная стратегия обеспечения информационной безопасности в Великобритании The UK Cyber Security Strategy нацелена на подключение полиции и поощрение судебной власти к более широкому использованию существующих законов в Великобритании для борьбы с киберпреступностью и расширению международного сотрудничества.

Отмечается, что преступники используют Интернет для различных преступлений, включая мошенничество, кражи личных данных, кражи финансовой информации и корпоративной интеллектуальной собственности и эксплуатации детей. Многие преступники рассматривают Интернет как выгодный и низкорисковый канал для совершения преступлений, а поскольку он не имеет границ, они могут базироваться в странах, которые вряд ли преследуют их.

Так, в Великобритании правительство работает над тем, чтобы правоохранительные органы и судебная система использовали существующее законодательство для борьбы с киберпреступностью и защиты общественности. Такие законы включают «Заговор с целью обмана», «Закон о защите данных» 1998 года и Закон 1990 года о компьютерном неправомерном использовании. Суды также могут контролировать или ограничивать использование компьютеров киберпреступниками.

В противодействии киберпреступности объединена работа подразделения электронной преступности в Агентстве по опасной организованной преступности и Отдела электронной преступности полиции. Этот блок должен будет заниматься самой серьезной киберпреступностью на национальном уровне и обеспечивать поддержку другим полицейским силам (The UK cyber security strategy: Landscape review: 28).

Французская национальная стратегия по обороне и безопасности информационных систем принята в феврале 2011 года и определяет 4 основные цели государственной политики:

– стать мировой державой в сфере кибероборонs;

– охранять возможность Франции принимать решения посредством защиты информации, связанной с ее суверенитетом;

– укрепление кибербезопасности ключевой национальной инфраструктуры;

– обеспечение безопасности в киберпространстве.

В соответствии с поставленными целями определены основные направления деятельности:

– анализ и прогнозирование;

– выявление, сообщение и реагирование;

– усиление и поддержка научного, технического, отраслевого и человеческого потенциала;

– защита информационных систем государства и операторов ключевой инфраструктуры;

– адаптация французского законодательства;

– развитие международного сотрудничества (http://constitutions.ru/?p=11393: 9).

Как видим, принятие национальных стратегий кибербезопасности позволяет определить приоритетные аспекты государственной полити-

ки, обратить внимание на наиболее актуальные и перспективные направления деятельности.

Заключение

Национальные концепции кибербезопасности учитывают национальный опыт правового регулирования, национально-культурные особенности, уровень информационно-технического развития страны. В силу этого каждая национальная концепция обладает своими особенностями и нюансами.

Вместе с тем, все концепции, так или иначе, затрагивают вопросы уголовно-правового регулирования вопросов обеспечения информационной безопасности. Действительно, нельзя не признать, что действенность, результативность и эффективность информационных отношений напрямую зависит от того, насколько они обеспечиваются средствами правовой охраны на национальном уровне, что, на наш взгляд, обусловлено спецификой понимания проблем информационной безопасности с точки зрения их внутреннего национального содержания.

Литература

Мнацаканян А.В. Информационная безопасность в Российской Федерации: уголовно-правовые аспекты: дис. …канд. юрид. наук. – М., 2015. – 216 с.

Назарбаев Н.А. Третья модернизация Казахстана: глобальная конкурентоспособность: Послание от 31 января 2017 года // Интернет-ресурс. – Режим доступа: URL: http://adilet.zan.kz/rus/docs/K1700002017

Елин В.М. Сравнительный анализ правового обеспечения информационной безопасности в России и за рубежом. – М.: МИГУиП, 2016. – 168 с.

International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World. – Washington, 2011. – 30 p.

Европейская конвенция по киберпреступлениям (преступлениям в киберпространстве). Будапешт, 23 ноября 2001 года // Интернет-ресурс. – Режим доступа: URL: http://inter.criminology.onua.edu.ua/materials

Громов Е.В. Развитие уголовного законодательства о преступлениях в сфере компьютерной информации в зарубежных странах (США, Великобритании, ФРГ, Нидерландах, Польше) // Вестник ТГПУ. – 2006. – № 11. – С. 30-35.

Дворецкий М.Ю., Копырюлин А.Н. Оптимизация уголовной ответственности и проблемы квалификации преступлений в сфере компьютерной информации. – Тамбов: Изд-во ТГУ им. Г.Р. Державина, 2006. – 212 с.

The UK cyber security strategy: Landscape review. Report by the Comptroller and Auditor General. – London: The Stationery Office, 2013. – 43 p.

Стратегия по защите и безопасности информационных систем Франции. Февраль, 2011 г. // Интернет-ресурс. – Режим доступа: URL: constitutions.ru/?p=11393

References

Mnatsakanyan A.V. (2015) Informatsionnaya bezopasnost’ v Rossiyskoy Federatsii ugolovno-pravovyye aspekty: dis. …kand. yurid. nauk. – M. – 216 s.

Nazarbayev N.A. Tret’ya modernizatsiya Kazakhstana global’naya konkurentosposobnost’: Poslaniye ot 31 yanvarya 2017 goda // Интернет-ресурс. – Режим доступа: URL: http://adilet.zan.kz/rus/docs/K1700002017

Elin V.M. (2016) Sravnitel’nyy analiz pravovogo obespecheniya informatsionnoy bezopasnosti v Rossii i za rubezhom. – M.: MIGUiP . – 168 p.

International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World. – Washington, 2011. – 30 p.

Yevropeyskaya konventsiya po kiberprestupleniyam (prestupleniyam v kiberprostranstve). Budapesht, 23 noyabrya 2001 goda // Internet-resurs. – Rezhim dostupa: URL: http://inter.criminology.onua.edu.ua/ materials/zakony/konvents/ciberprest.htm

Gromov Ye.V. Razvitiye ugolovnogo zakonodatel’stva o prestupleniyakh v sfere komp’yuternoy informatsii v zarubezhnykh stranakh (SSHA, Velikobritanii, FRG, Niderlandakh, Pol’she) // Vestnik TGPU. – 2006. – № 11. – S. 30-35.

Dvoretskiy M.YU., Kopyryulin A.N. Optimizatsiya ugolovnoy otvetstvennosti i problemy kvalifikatsii prestupleniy v sfere komp’yuternoy informatsii. –Tambov: Izd-vo TGU im. G.R. Derzhavina, 2006. – 212 s.

The UK cyber security strategy: Landscape review. Report by the Comptroller and Auditor General. – London: The Stationery Office, 2013. – 43 P.

Strategiya po zashchite i bezopasnosti informatsionnykh sistem Frantsii. Fevral’, 2011 g. // Internet-resurs. – Rezhim dostupa: URL: http://constitutions.ru/?p=11393