УДК 349

Д. А. Свиридов
начальник кафедры уголовного процесса и криминалистики
Могилевского института МВД

НЕКОТОРЫЕ АСПЕКТЫ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

SOME ASPECTS OF INFORMATION PROTECTION LEGAL ENSURANCE

Аннотация. *В статье рассматриваются проблемные вопросы правового обеспечения защиты информации в автоматизированных информационных системах, имеющих существенное значение для отдельных секторов жизнедеятельности государства. Определяются наиболее существенные риски для информационных систем Республики Беларусь и предлагаются пути их решения.*

Ключевые слова: *информация, информационная система, автоматизированная информационная система, информационная безопасность, конфиденциальность, ограниченное распространение.*

Annotation. *The article discusses the problematic issues of legal support for the protection of information in automated information systems, which are essential for certain sectors of the state's life. The most significant risks for information systems of the Republic of Belarus are determined and ways to solve them are proposed.*

Keywords: *information, information system, automated information system, information security, confidentiality, limited distribution.*

На современном этапе развития Республика Беларусь характеризуется постоянно возрастающей ролью информационной составляющей, которая предстает в виде совокупности информации, субъектов, на которых возложены функции по сбору, формированию, выдаче и использованию информации; информационной инфраструктуры, в том числе системы, обеспечивающей регулирование общественных отношений, возникающих при этом.

Проведенное исследование о состоянии информатизации и защиты информации в Республике Беларусь показало серьезное изменение объема и важности информации, которая используется посредством технических средств ее получения, обработки, хранения, выдачи. В таких условиях представляется возможным утверждать, что в Республике Беларусь информация и информационные технологии становятся основой экономического потенциала и одним из важнейших ресурсов. При всем при этом всеобщая компьютеризация наиболее существенных и чувствительных к угрозам сфер деятельности приводит к появлению многочис-

ленных как внутренних, так и внешних угроз, несанкционированного доступа к информации и каналов ее утечки.

Одной из особенностей процесса информатизации основных сегментов Республики Беларусь является ускорение процессов передачи ряда функций автоматизированным информационным системам. В случае возникновения каких-либо нарушений или сбоев в функционировании таких систем могут возникнуть тяжелые последствия (техногенные катастрофы, социальные и экономические чрезвычайные ситуации, человеческие жертвы и т. д.).

В связи с этим необходимо обеспечить качественную работу такого рода процессов, для чего необходимо создание баз данных, соответствующих хранилищ информации, а также защищенных коммуникаций для передачи и обмена данными, привлечение к процессу управления довольно больших групп специалистов, что также может создать дополнительные риски для защиты информации. Среди наиболее существенных из них выступает уязвимость автоматизированных систем в отношении угроз безопасности информации, которая проявляется в:

• достоверности (подделка, фальсификация, мошенничество);

• целостности (искажение, потери, ошибки);

• доступности (запрет на получение, нарушение связи);

• конфиденциальности (утечка, разглашение, несанкционированный доступ) [1, с. 87].

В соответствии с Концепцией информационной безопасности Республики Беларусь (далее — Концепция) основными целями государства в данной сфере являются обеспечение комплексного подхода к проблеме информационной безопасности, создание методологической основы в целях совершенствования деятельности по ее укреплению, формирование государственной политики, выработка мер по совершенствованию системы обеспечения информационной безопасности, конструктивное взаимодействие, консолидация усилий и повышение эффективности защиты национальных интересов в информационной сфере [2]. Эти цели могут быть реализованы посредством решения ряда задач, среди которых представляется верным отметить следующие: повышение безопасности информационных систем, разработка и производство собственных средств защиты информации, обеспечение защиты информации ограниченного распространения, интенсификация международного сотрудничества Республики Беларусь в сфере противодействия угрозе информационного противоборства, а также использования информационных ресурсов.

Анализ Концепции позволил выделить следующие основные направления реализации безопасности в информационной сфере Республики Беларусь:

• информационный суверенитет;

• информационный нейтралитет;

• государственное реагирование на риски, вызовы и угрозы в информационной сфере;

• сохранение традиционных устоев и ценностей;

• информационное обеспечение и сопровождение государственной политики;

• безопасность массовой информации;

• безопасность национального сегмента сети Интернет;

• киберустойчивость критически важных объектов информатизации и государственных информационных систем;

• противодействие киберпреступности;

• защита государственной и служебной тайны;

• безопасность информации ограниченного распространения и защита персональных данных.

Анализ защищенности информационных автоматизированных систем показывает следующее: в целом организация их защиты требует незамедлительного решения возникающих вопросов для создания безопасности их функционирования; отсутствует четкий перечень внутренних и внешних угроз (имеющаяся отсылка на Концепцию национальной безопасности не в полной мере устраняет данную проблему); не точно определены каналы утечки информации и несанкционированного доступа к ней [3, с. 252–254]; существует своего рода неопределенность правового статуса и уровня требований, направленных на защиту информации личного или ограниченного характера; имеет место работа с информацией ограниченного доступа с нарушением законодательства. В целом же защита информации главным образом сводится к применению защиты операционных систем, архивированию, резервному копированию информации, а также использованию программного обеспечения антивирусного характера. Кроме того, очевидно, что уровень безопасности информационных систем существенно отстает от темпов роста внутренних и внешних угроз. Возникновение угроз информационной безопасности со стороны внешних или внутренних источников угроз чреваты утечкой информации, нарушением доступности и целостности, искажением содержания, что с высокой долей вероятности может повлечь чрезвычайные ситуации и причинение серьезного вреда национальным интересам Республики Беларусь. Ощущается недостаток квалифицированных кадров в сфере обеспечения информационной безопасности, что в свою очередь может быть следствием снижения эффективности системы образования в данной сфере.

Видится необходимым отметить факт того, что состояние нормативных правовых документов, регулирующих вопросы информационной безопасности, отстает от современного уровня развития информационных технологий, не в полной мере соответствует уровню международной нормативной правовой базы и в отдельных аспектах не учитывает международную практику. С целью сокращения такого отставания в Республике Беларусь на постоянной основе совершенствуется нормативная правовая и методологическая база в этой сфере, которая позволяет определить не только критерии оценки безопасности информационной сферы и ее отдельных компонентов, но и требования безопасности в соответствии с положениями международных стандартов.

Таким образом, вследует отметить, что правовая база, регулирующая отношения в информационной сфере, должна представлять собой целостную систему нормативных правовых актов, позволяющих оценить безопасность информационных технологий и систем, внедрение которых даст возможность обеспечить защиту информации. Следует иметь в виду и тот факт, что закрепление правовых норм обеспечения информационной безопасности в зарубежных странах произошло намного раньше постсоветского пространства, на основе чего возникли экономические преимущества. Исходя из этого, вопросам совершенствования нормативной правовой базы в сфере обеспечения информационной безопасности должно уделяться серьезное внимание. Представляется необходимым закрепление не только узкого, но и широкого подхода к понятию информационной безопасности, что в большей степени позволит отразить динамику развивающегося информационного общества Республики Беларусь.

Список основных источников

1. Ярочкин, В. И. Информационная безопасность : учебник для студентов вузов / В. И. Ярочкин. — 2-е изд. — М. : Академический проект, 2004. — 544 с.

2. О Концепции информационной безопасности Республики Беларусь [Электронный ресурс] : постановление Совета Безопасности Респ. Беларусь, 18 марта 2018 г., № 1 // ЭТАЛОН. Решения органов местного управления и самоуправления / Нац. центр правовой информ. Респ. Беларусь. — Минск, 2020.

3. Шкаплеров, Ю. П. О защите данных досудебного производства от разглашения в уголовном праве и уголовном процессе Республики Беларусь / Ю. П. Шкаплеров // Уголовная политика и культура противодействия преступности : материалы Междунар. науч.-практ. конф., 21 сент. 2018 г. : в 2 т. / редкол.: А. Л. Осипенко [и др.]. — Краснодар : Краснодар. ун-т МВД России, 2017. — Т. II. — С. 252–258.