К ВОПРОСУ О ПРАВОВОМ СООТНОШЕНИИ ПОНЯТИЙ: «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ», «ЗАЩИТА ИНФОРМАЦИИ» И «КИБЕРБЕЗОПАСНОСТЬ»

Андрей СМОКИНЭ, доктор хабилитат права, профессор
Светлана ГРИЩУК–БУЧКА, докторант ИИГиП АНМ, мастер права

The information revolution of the 1990s of the last century was a historic moment frame construction of the new «information society», based on the active introduction and widespread use of modern technology in all spheres of human activity. Along with technological advances and changes began to change and improve the legal framework of society. In the national legal systems of different countries there separate laws regulating absolutely new category of legal relationship in information sphere. Similarly, gradually began to form an independent branch of law designed to regulate social relations in the field of application and use of information technology.

This paper analyzes the relationship of basic legal concepts of a new branch of law governing the specific category of legal relations arising from the field of information and telecommunications technologies — "Information security", "protection of information" and "cybersecurity."

Keywords: *information law, information society, information security, protection of information, cybersecurity*

В статье представлен анализ правового соотношения базовых понятий новой отрасли права, регулирующей категорию правоотношений, возникшие с области информационных и телекоммуникационных технологий — «информационная безопасность», «защита информации» и «кибербезопасности».

Ключевые слова: *информационное право, информационное общество, информационная безопасность, защита информации, кибербезопасность*

Информационная революция 1990–х годов прошлого столетия стала историческим моментом отсчета построения нового «информационного общества», основанного на активном внедрение и повсеместном применении современных технологических решений во всех сферах человеческой деятельности[1]. Вместе с технологическими новшествами и изменениями стала меняться и совершенствоваться правовая основа общества.

В национальных системах права большинства стран мира появились отдельные законы, регулирующие совершенно новую категорию правоотношений

1 A good summary of this normative claim 1990s is found in Michael Geist, Cyberlaw 2.0 (2003)

возникающих в информационной сфере[2]. Подобным образом, постепенно стала формироваться самостоятельная отрасль права, призванная регулировать общественные отношения в сфере применения и использования информационных технологий. Данную отрасль права стали именовать «Информационное право»[3], «Киберправо»[4], «Право в сети Интернет»[5], «Интернет право» «Информационно–технологическое право»[6], «Компьютерное право»[7] и т.д. Однако, вопрос о самостоятельности данной отрасли права все еще остается дискуссионным и открытым. Ряд ученых всецело рассматривают ее в качестве формирующейся отрасли права, иные же отрицают этот факт, считая, что информационное право — это всего лишь совокупность ряда новых политик, социальных и экономических целей, регулируемых новыми правовыми парадигмами, отличающимися от традиционных[8]. Учитывая тот факт, что теория права предопределяет в качестве базовых предпосылок к формированию самостоятельной отрасли права наличие специфического предмета правового регулирования[9], как основного критерия отличия норм одной отрасли права от другой, и метода правового регулирования, в качестве особого режима, создаваемого отраслью права для участников регулируемых ею отношений, следует констатировать наличие данных атрибутов в информационном праве, что позволяет выделить статус информационного права в качестве самостоятельной отрасли современного права.

Среди базовых понятий данной отрасли права наиболее сложными с правовой точки зрения, на наш взгляд, являются понятия: «информационная безопасность», «защита информации» и «кибербезопасность», поскольку очень часто их рассматривают в качестве синонимов. Целесообразно с правовой точки зрения, определить сущность данных понятий в рамках различных правовых школ и направлений, и степень их соотносимости.

«Информационная безопасность». Рассматривая различные научные точки зрения на анализируемую дефиницию, можно отметить отдельные общие подходы к определению «информационная безопасность», а также ряд существенных различий во мнениях некоторых ученых.

Российская правовая школа. Термин «информационная безопасность» активно используется представителями российской школы права. Именно российскими

---

2 Rowland Diane *Information technology law* (2005). Table of European Legislation

3 Раца А. Становление информационного права в Республике Молдова//Закон и жизнь. — №7. –2007 — с.42–47

4 Lawrence Lessig *The law of the horse: What cyberlaw might teach* (1999), Dennis M.Powers Cyberlaw: The Major Areas, Development, and Information Security Aspects (2009)

5 Edvards, Lilian and Charlotte Waelde *Law and the Internet* (2010)

6 Brian Napier *The future of international law* (1992), Lloyd Ian *Information technology law* (2008)

7 Reed Chris *Computer Law: the law and regulation of information technology* (2007)

8 Rowland Diane *Information technology law* (2005)

9 Хропанюк В.Н. Теория государства и права — М.: 2008. — с.113

учеными представлены наиболее объемные определения данного понятия. В частности, В.Н.Лопатин, под информационной безопасностью понимает состояние защищенности национальных интересов страны (жизненно важных интересов личности, общества и государства на сбалансированной основе в информационной сфере от внешних и внутренних угроз)[10]. А. А. Малюк рассматривает информационную безопасность как «такое состояние рассматриваемой системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой — ее функционирование не создает информационных угроз для элементов самой системы и внешней среды»[11]. Ряд других авторов, говоря об информационной безопасности, нередко понимают этот термин узко, как набор аппаратных и программных средств для обеспечения сохранности, доступности к конфиденциальности данных в компьютерных сетях. Информационной безопасностью также называют «меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе». Отдельные же авторы, в частности К.Ушаков, под информационной безопасностью понимают «защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры»[12], выделяя в итоге уже два объекта защиты — информацию и информационную структуру. В.И. Галатенко и В.К.Левин, имея сходную позицию относительно информационной безопасности, понимают под ней защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуре. Высказанный подход акцентирует два основных объекта защиты: собственно информацию и информационные структуры[13]. Ранее обеспечение информационной безопасности сводилось лишь к защите информации (да и то не всей, а лишь государственной и служебной тайны), скорее всего, по инерции некоторые ученые ошибочно отождествляют два совершенно разных по своей сущности понятия «защита информации» и «информационная безопасность».

---

10 Лопатин В.Н. Информационная безопасность России: Человек. Общество. Государство. — СПб: Фонд «Университет»,2000. — с.79

11 Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для ВУЗов. — М.: Горячая линия — Телеком, 2004 — с.34

12 Ушаков К. Интернет–мошенничество: о формах и масштабах явлений, средствах и методах борьбы www.cio–world.ru

13 Галатенко В.И., Информационная безопасность// Открытые системы, 1996 — №1(15). — с. 38–43; Левин В.К. Защита информации в информационно–вычислительных системах и сетях//Программировние. –1994. –№5 — с.5

Опыт зарубежных стран. Законодательству ряда зарубежных стран, в частности Великобритании, Франции, Германии, Соединенных Штатам Америки исторически знакома правовая дефиниция «защита информация». Именно защита информации рассматривается данными государствами как основная правовая категория информационного права. Тенденции последних лет, в частности, принятие нормативных актов обеспечивающих защиту информации в виртуальном пространстве, выводят кибербезопасность совершенно на новый уровень. В частности, по мнению президента США Б.Обамы, экономическое процветание Америки в XXI веке будет зависеть от кибербезопасности[14]. Это же является вопросом государственной и национальной безопасности, а защита информационной инфраструктуры будет приоритетом национальной безопасности. 16 мая 2011 года Вашингтон впервые заявил о принятии Соединёнными Штатами стратегии кибербезопасности[15], которая затрагивает международное сообщество в целом. Подход Соединенного Королевства также направлен на развитие кибербезопасности. В июне 2009г. была опубликована «Стратегия кибербезопасности» Великобритании (UK Cyber Security Strategy)[16], а в 2010г. были приняты новые варианты документов «Стратегии национальной безопасности» (National Security Strategy)[17] и «Доклада стратегической обороны и безопасности» (Strategic Defense and Security Review) Великобритании[18]. Государства Европейского Союза так же, как и США, активно проводят политику развития ИКТ. Программа «Электронная Европа» («e–Europe») явилась результатом анализа опыта развития ИКТ в европейских странах. Концептуальное и административное оформление данной политики делает ее интегральной частью стратегии ЕС по повышению конкурентоспособности европейской экономики и повышению уровня жизни[19].

Политика ЕС в области развития информационного общества состоит из 4 основных компонентов:

— телекоммуникационная политика, в т.ч. либерализация рынка телекоммуникаций.

---

14 Батуева Е. В. Политика администрации Барака Обамы в области обеспечения информационной безопасности // Вестник МГИМО. — №13 — с.271–276

15 International strategy for cyberspace http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

16 Cyber Security Strategy of the United Kingdom safety, security and resilience in cyber space http://www.official–documents.gov.uk/document/cm76/7642/7642.pdf

17 A Strong Britain in an Age of Uncertainty: The National Security Strategy http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf)

18 Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191634.pdf

19 Europes Information Society http://ec.europa.eu/information_society/eeurope/2005/index_en.htm

— поддержка технологического развития информационно– коммуникационных технологий (ИКТ).
— создание условий для конкурентоспособности сектора ИКТ в ЕС.
— создание общеевропейских транспортных, энергетических и телекоммуникационных сетей.

В настоящее время Европейский союз также осознал необходимость в защите от киберпреступности на государственном уровне. Для выполнения ЕС принял ряд директив, фокусирующихся на проблемах защиты интеллектуальной собственности, Интернет– маркетинге, правовых аспектах электронной коммерции[20],[21].

В 2001 г. в Европейском Союзе была принята специальная Конвенция о киберпреступности, где декларируется необходимость борьбы с данным явлением[22]. В 2008 г. Европейское агентство по сетевой и информационной безопасности (ENISA)[23] представило первое исследование (European Information sharing and Alert Systems) (EISAS), информирующее компании и граждан ЕС об угрозах, уязвимостях и атаках. Кроме того, ЕС может собирать и анализировать «эффективную практику» специалистов из разных стран и в случае необходимости предлагать оптимизацию в той или иной области защиты информации.[24] В функции ЕС включается поддержка новых национальных систем в государствах–членах, ЕС отдается роль посредника между странами–членами союза в отношении политики защиты информации.В ближайшее время в ЕС планируется формирование подразделения по регулированию в сфере Интернет–угроз. В качестве аргументов приводятся примеры кибератак из Эстонии, Литвы и Грузии за последние годы, к которым страны ЕС оказались совершенно не готовы. В Евросоюзе высказываются опасения, что в течение следующих 10 лет подобные атаки будут повторяться. При этом если выход в Интернет будет заблокирован в течение одного месяца, это приведет к убыткам в экономике региона не менее чем в 200 млрд.долл.[25]

---

20 Смирнов А.А. Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза: монография/ А.А.Смирнов. — М.: ЮНИТИ–ДАНА: Закон и право,2012. — с.145–148.

21 EC Directives http://www.etsi.org/index.php/about/our–role–in–europe/public–policy/ec–directives

22 Convention on Cybercrime (Budapest. 23.XI.2001)// Council of Europe http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

23 EuropeanNetwork and Information Security Agency http://www.enisa.europa.eu/

24 Кравцев И.Н. Стратегия национальной безопасности России и особенности информационно–технической борьбы на современном этапе // Национальная безопасность России в условиях трансформации международных отношений: Сб.статей / М.: МАКС Пресс, 2009.– С. 178–179.

25 США создают кибер–войска http://telecomb2b.cnews.ru/news/top/index.shtml?2009/05/06/346422

В сентябре 2012 Европейские ведомства приняли меры по усилению собственной киберзащиты, путем создания команды быстрого реагирования на угрозы информационной безопасности (Computer Emergency Response Team, CERT–EU)[26]. Данное решение было принято правительством после успешно пройденного испытательного периода команды — европейский CERT работал год в качестве пилотного проекта. Соответственно, наличие собственной CERT, работающей на постоянной основе позволит на должном уровне обеспечить благосостояние и конкурентоспособность стран участниц Европейского Союза в посредством обеспечения кибербезопасности.

Вопросы разработки базового документа в сфере правового закрепления и обеспечения кибербезопасности в рамках Европейского Союза получили широкое обсуждение в начале 2010–х годов. В частности, в программе работы Европейской комиссии на 2012 год[27] утверждалось, что комиссия разработает Стратегию безопасности Интернета для Евросоюза. Разработка стратегии была возложена на главный директорат DG CONNECT (DG INFSO)[28]. Стратегия кибербезопасности и стратегия безопасности Интернета — это несколько разные вещи, хотя они имеют много общего, например, определение и предложение подходящей правительственной модели, нацеленность на предотвращение и борьбу с инцидентами безопасности. Задача главного директората DG CONNECT была правильно разместить существующие и планируемые мероприятия в глобальном политическом контексте в рамках сети Интернет. Директорат также должен был подготовить программу дальнейших действий с перспективой представления Евросоюзу комплексного, целостного и структурированного подход к проблеме безопасности Интернета[29]. Важно отметить тот факт, что в настоящий момент в рамках Европейского Союза единая стратегии кибербезопасности — «Открытое, безопасное и надежное киберпространство»[30] принята в рамках Еврокомиссии.

Национальная школа права. Молдавские ученые, в частности, А.Д.Урсул и Т.(Ф.) Н.Цырдя рассматривают информационную безопасность в качестве способности государства, общества, социальной группы, личности, во–первых, обеспечить с определенной вероятностью достаточные и защищенные социальный интеллект и информационный ресурс, оптимальную социальную энтропию и инфосреду для поддержания жизнедеятельности и жизнеспособности,

---

26 Press Release Cyber security strengthened at EU institutions following successful pilot scheme// European Commission http://cert.europa.eu/cert/plainedition/en/pressrelease.html

27 COM(2011) 777 final VOL.1/2 http://ec.europa.eu/atwork/programmes/docs/cwp2012_en.pdf

28 С 1ого июля 2012 года DG INFSO переименовано в DG CONNECT

29 ROADMAP:Proposal on a European Strategy for Internet http://ec.europa.eu/governance/impact/planned_ia/docs/2012_infso_003_european_internet_security_strategy_en.pdf

30 EU Cyber Security Strategy — open, safe and secure http://eeas.europa.eu/top_stories/2013/070213_cybersecurity_en.htm

устойчивого функционирования и развития социума; во–вторых, противостоять информационным опасностям и угрозам, негативным информационных воздействиям на индивидуальное и общественное сознание и психику людей, а также на компьютерные сети и другие технические источники[31]. Плотяну Н. под информационной безопасностью рассматривает систему (организационную) правовых действий, организационного, технических и иного характера органов центральной и региональной власти, органов местного публичного управления. предприятий, организаций и учреждений, уполномоченных обеспечивать государственную безопасность, сохранность государственных секретов и иной информации ограниченного доступа, включая служебную и коммерческую, защиту информационных ресурсов, технологических систем[32].

Совершенно очевидно, что понятие «информационная безопасность» взаимосвязано с понятием «безопасность информации». Довольно часто их используют как синонимы. Но, как известно, «безопасность» не существует сама по себе, безотносительно к объекту, «без определения объекта понятие «безопасность» является неопределенным, лишенным внутреннего смысла»[33]. Выбор объекта безопасности предопределяет содержание понятия «безопасность». Поэтому, если в качестве объекта защиты выступает собственно информация, то правовая дефиниция «информационная безопасность» и «безопасность информации» действительно становятся синонимами. Но, если в качестве объекта защиты рассматривается некий объект (субъект) — участник информационных отношений, то слово «информационная» в термине «информационная безопасность» указывает на направление деятельности, посредством которой может быть причинен вред объекту защиты и понятие «информационная безопасность» в этом случае следует трактовать как состояние защищенности данного объекта от угроз информационного характера. С.П.Расторгуев, характеризуя современное состояние проблемы, пишет: «В результате проблема защиты информации, которая ранее была как никогда актуальна, перевернулась подобно монете, что вызвало к жизни ее противоположность — защиту от информации. Теперь уже саму информационную систему и, в первую очередь человека,– необходимо защищать от поступающей «на вход» информации, потому что любая поступающая на вход самообучающейся системы информация неизбежно изменяет систему. Целенаправленное же деструктивное информационное воздействие может привести систему к необратимым изменениям и, при определенных условиях, к самоуничтожению»[34]. Безопасность информации при этом должна

31 Урсул А. Д, Цырдя Т.(Ф.) Н. Информационная безопасность. Сущность, содержание и принципы обеспечения. http://security.ase.md/publ/ru/pubru22.html

32 Ploteanu N., S. Maftea, R. Griniuc Pasul II în ciberspațiu: Securitatea Informațională. — Chișinău, 2008 — p.13

33 Стрельцов, А.А. Содержание понятия «обеспечение информационной безопасности» // Информационное общество. 2001. № 4. — С.12.

34 Расторгуев, С.П. Философия информационной войны. М.: МПСИ, 2003г — с.68 (301)

рассматриваться как составная часть общей проблемы обеспечения безопасности объекта защиты, причем не самой главной, а лишь в той части, в которой необеспечение безопасности информации, имеющей отношение к объекту защиты, может нанести ему вред, который, в свою очередь, может привести к нарушению его структурной целостности и функциональной цельности.

Проведенный анализ позволяет констатировать следующее: нельзя отождествлять такие категории как «защита информации» и «информационная безопасность». В первом случае подразумевается конкретная деятельность по охране информации, реализация способов, механизмом ее сохранения, включая и виртуальную среду — «кибербезопасность». Тогда как, информационная безопасность — это особое состояние информации, подчеркивающее ее значимость от стороннего вмешательства, это своего рода степень возможного доступа к ее получению. Информационная безопасность не может сводится только лишь к защите информации, это значительно более широкое понятие. Информационная безопасность, в качестве предмета научного исследования выступает многогранным понятием, базовым институтом информационного права, включающем субинститут «защита информации», соотносящийся с кибербезопасностью как общее и частное, поскольку защита информации осуществляется как в реальном, так и в виртуальном пространстве.