Манжуева Оксана Михайловна

ЭТИКО-ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В статье определено значение этико-правовых норм в процессе применения информационных технологий. Выделена проблема компьютерной преступности в качестве животрепещущих тем современного общества, подчеркнута роль единых стандартов в решении проблем информационной безопасности. Затронута тема защиты авторских прав и обеспечение конфиденциальности информации в процессе широкого использования информационных технологий. Подчеркнута необходимость повышения общего уровня информированности в обществе, в целях заблаговременного предотвращения компьютерных преступлений.

Адрес статьи: www.gramota.net/materials/3/2014/5-2/36.html

Источник

Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики

Тамбов: Грамота, 2014. № 5 (43): в 3-х ч. Ч. II. С. 131-134. ISSN 1997-292X.

Адрес журнала: www.gramota.net/editions/3.html

Содержание данного номера журнала: www.gramota.net/materials/3/2014/5-2/

УДК 004.056.5:34
Юридические науки

В статье определено значение этико-правовых норм в процессе применения информационных технологий. Выделена проблема компьютерной преступности в качестве животрепещущих тем современного общества, подчеркнута роль единых стандартов в решении проблем информационной безопасности. Затронута тема защиты авторских прав и обеспечение конфиденциальности информации в процессе широкого использования информационных технологий. Подчеркнута необходимость повышения общего уровня информированности в обществе, в целях заблаговременного предотвращения компьютерных преступлений.

Ключевые слова и фразы: законодательство; интеллектуальная собственность; информационная безопасность; конфиденциальность информации; стандарты и спецификации.

Манжуева Оксана Михайловна, к. филос. н., доцент
Восточно-Сибирская государственная академия культуры и искусств
ocydenova@yandex.ru

ЭТИКО-ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ©

Попытки наложить новую культуру на существующие правовые порядки в тех областях, где широко применяются информационные технологии, не могут оставаться без изменений, поскольку прежние правовые доктрины теряют свое действие. Такие оформившиеся области права, как конституционное, контрактное, патентное и авторское, претерпели серьезные перемены. Компьютерные преступления значительно изменили структуру уголовного процесса и уголовного кодекса, поскольку существовавшие юридические нормы не предусматривали наказания за «высокотехнологичные» преступления. Из истории информационной безопасности известно, что подобные шаги создания систем защиты в некоторых важных областях были предприняты во второй половине прошлого столетия: Закон об информационных записях и свободах (Франция, 1978 г.), Акт о данных (Швеция, 1973 г.), Закон об общественных информационных системах (Югославия, 1981 г.), Акт о защите федеральной компьютерной системы (США, 1984 г.). Сегодня, как и тогда, специалисты видят решение данной проблемы на пути одновременного создания новых законов и адаптации уже существующих юридических принципов к имеющейся технологии.

Межграничные потоки данных, то есть электронная информация, курсирующая через национальные границы с целью хранения, обработки и дальнейшего использования [10, p. 155], важная проблема для многих стран, поскольку законы, рассчитанные на соблюдение их на определенной территории, в этом случае не действуют, отсюда возникает необходимость в подписании договоров. Подобные документы применяются для предотвращения принятия несовместимых местных законов, помимо прочего на них возлагается функция способствовать возникновению единых стандартов на законодательные акты в данной области. В поисках решения проблем в этой области, специалисты выделили наиболее «удобный» подход к международному регулированию межграничного потока данных – это регулирование технических аспектов, в том числе и установление универсальных стандартов [3, с. 211]. В результате чего, основные технические характеристики информационно-компьютерной коммуникации были оформлены в виде коммуникационных протоколов, и совместно использовались сторонами, в свою очередь, общие стандарты снижали стоимость и повышали эффективность.

Практика дня сегодняшнего диктует обязательное знание для специалистов в области информационной безопасности соответствующих стандартов и спецификаций, которые выступают в качестве основного апробированного средства обеспечения совместимости аппаратно-программных средств на процедурном и программно-техническом уровнях безопасности. В области информационной безопасности число стандартов и спецификаций бесконечно, но специалисты выделяют следующие. Стандарт, разработанный Министерством обороны США «Критерии оценки доверенных компьютерных систем» [6], завоевавший международное признание как «Оранжевая книга», раскрывает практически весь понятийный базис информационной безопасности. Руководящие документы Гостехкомиссии России [1], а также «Критерии безопасности информационных технологий» [8] Федерального стандарта США регламентируют важные технические аспекты информационной безопасности, такие как организация работы сервисов безопасности, например, криптографических модулей и межсетевых экранов. В свою очередь «Гармонизированные критерии Европейских стран» [9] унифицируют требования к информационным технологиям, кроме того, необходимо отметить, что данный документ заложен в основание международного стандарта ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» [5], чаще именуемый в литературе «Общими критериями». Стандарт «Общие критерии» назван оценочным мегастандартом современности, определяющим инструменты безопасности и порядок использования их в информационных системах. Каждый из перечисленных нормативных документов внес свой невосполнимый вклад в формирование научно-методологической базы в области информационной безопасности.

В то же время, техническая сторона вопроса является важной, но далеко не единственной проблемой обеспечения безопасности, кроме того, как показала практика применения информационных технологий, в стандартизированные компьютерные системы легче проникнуть злоумышленнику. Действительно,

в информационном обществе весьма важной областью законодательства становится борьба с компьютерными или информационными преступлениями. Как правило, в мировой практике, информационное законодательство классифицирует в качестве правонарушения следующие действия:

- несанкционированное использование информационно-технических средств;
- ввод искажающих данных в информационные системы;
- изменение или нарушение информации, массивов информации;
- хищение финансовых средств или сведений, ценных данных.

Компьютерная преступность наносит большой ущерб, но при этом установить факт совершения преступления весьма сложно. Ввиду отсутствия свидетельств, назвать даже приблизительное число совершаемых преступлений невозможно. Эксперты считают подобного рода преступность серьезной проблемой и оценивают приносимый ущерб в несколько миллиардов долларов в год. Кроме того, среди специалистов нет единства относительно состава компьютерных преступлений [4]. Утверждения традиционных законов о собственности, которую можно украсть, должна быть ощутимой (вещественной), и при краже изменить владельца в случае с такими категориями, как программное обеспечение и базы данных, теряет всякий смысл. Компьютерное преступление может совпадать со следующими признанными категориями преступлений: финансовые преступления, кража собственности и вандализм. Кроме того, встает вопрос об оценке украденной собственности, который позволяет дифференцировать крупные и мелкие преступления при вынесении наказания.

Существующие законы, относительно хищений, вторжения в частную жизнь, нарушения конфиденциальности, торговых секретов, авторского права и подделок электронных документов, использующиеся для наказания компьютерных преступлений, вызывают в ходе реализации ряд трудноразрешимых вопросов. Например, в случае обвинения в хищении торговых секретов может возникнуть вопрос о «незащищенном вскрытии». Подобная ситуация возникает при отсутствии должного внимания к мерам защиты со стороны собственника информации, которую похитили, в таких случаях закон не имеет силы. Другой проблемой является несанкционированный доступ к файлам сверхсекретной важности, даже с целью только демонстрации способностей индивида преодолевать меры безопасности. В чем состав преступления, если информация не стиралась, не копировалась и не использовалась? Предполагая всю опасность подобных действий со стороны хакеров, конечно, их нельзя оставлять без должного внимания. Кроме того, необходимо указать, что наказание различных типов информационных правонарушений, например, несанкционированный доступ, не затрагивает вопросы, касающиеся «осязаемости» краденного и признаков «обладания», которые являются определяющими при рассмотрении обычных краж. Возможно, наиболее эффективные способы уголовного наказания будут обнаружены при детальном рассмотрении криминального компьютерного поведения в квалификации наказаний и идентификации преступлений.

Несмотря на общие цели и задачи в борьбе с компьютерными преступлениями, уголовные законодательства разных государств существенно отличаются [2]. Каждая страна дает свое определение преступлениям в информационной среде и определяет размер наказания, в то же время общая характеристика проблем примерно одинакова. На фоне отдельных нюансов правого регулирования каждого государства, одним из важнейших вопросов для всех стран международного содружества остается проблема реализации законодательной базы страны в информационной сфере. Автор особо выделяет проблему урегулирования законопроектной системы с международной практикой. Дело в том, что ситуация, в которой законодательство второй страны может оказывать влияние на расследование в области компьютерных преступлений, не всегда складывается благоприятно. Современный мир глобальных сетей дает дополнительную возможность для злоумышленников совершать компьютерные атаки не только в пределах собственной страны. В тех случаях, когда какое-либо государство не предусматривает наказания в сфере компьютерных преступлений, оно имеет право не оказывать содействие в расследовании преступлений. Поэтому с целью решения вопросов о международном сотрудничестве в борьбе с правонарушениями в информационной среде Совет Европы подписал Конвенцию о преступности в сфере компьютерной информации (ETS № 185 23.11.2001). Основной задачей данного документа являлось создание правовых условий в киберпространстве. В результате чего, все преступления в интернет-пространстве были разделены на четыре группы, для предотвращения которых налагались определѐнные требования странам, подписавшим Конвенцию. В то же время некоторые общественные организации (США, Великобритания, Испания) сформулировали обращение, выражающее протест против действия требований Конвенции [7], поскольку увидели в ряде ее положений противоречия статье о защите прав человека Европейской Конвенции. В частности, такие действия интернет-провайдеров, как фиксация и перехват при помощи технических средств информации для правоохранительных органов, тем самым воплощающие в нормы практики контроль над частными коммуникациями. Стоит предположить, что вопросы в сфере этико-правового урегулирования отношений в информационно-компьютерной среде еще не проявили всю свою палитру красок и послужат поводом для многих дебатов.

Общие принципы применения действующих правовых актов в сфере использования информационных технологий дают возможность выделить наиболее важные направления с точки зрения гармонизации национальных законов и международных правовых норм функционирования в информационной среде. К числу важных для рассмотрения проблем необходимо отнести следующие: обеспечение безопасности и тайны данных; признание прав на данные.

Вопросы безопасности данных и их сохранность предполагают, что все попытки расширить информационный обмен должны основываться на развитии правовых положений, которые в первую очередь будут обеспечивать два аспекта: необходимую безопасность и внедрение новых технологий. При замене физической основы документа с бумажной на электронную современные информационные технологии предоставляют широкий выбор средств обеспечения его аутентичности.

Сохранение тайны данных, или иначе конфиденциальности информации, определяют как способность индивида контролировать использование относящейся к нему информации [1]. Использование информационных технологий при обработке данных о личности, усложнение компьютерных систем и сетей отчетливо обозначили проблему сохранения тайны данных. Одно фундаментальное положение гласит: обладание информацией о личности оборачивается властью над ней, что превращает вопрос о неприкосновенности данных в одно из основных прав человека. Сегодня информация о личности попадает в чрезвычайно разветвленные сети, сложность и возможности которых выходят за рамки понимания. При этом передача данных базируется исключительно на доверии к государственным органам и уверенности в том, что с подобной информацией обращаются должным образом все участники информационных отношений, что она находится под охраной закона и ее нельзя использовать в целях, наносящих какой-либо вред индивиду. Сегодня возможности информационных технологий позволяют непредсказуемым образом сочетать данные, кроме того к ним могут получить доступ лица и организации, не имеющие на это право и использующие их в своих иных целях, нежели это предусматривалось. Тайна и безопасность данных неразрывны. Поэтому должен существовать баланс между правом человека на защиту от злоупотреблений данными, относящимися к нему, и опасностью несанкционированного доступа к конфиденциальной информации.

Следующий вопрос поддержания необходимого контроля безопасности затрагивает тему признания прав данных. Признание прав данных в первую очередь предполагает действие авторских прав, лицензий и ограничений по отношению к определенным видам информации с целью достижения максимально эффективного функционирования информации. Традиционно законодательство об интеллектуальной собственности (патентное, авторское право) применялось для защиты скорее носителя информации, чем самого содержания. Ситуация изменилась, когда данные были освобождены от своего физического выражения. На сегодняшний день специалисты выделяют наиболее слабые места защиты прав на интеллектуальную собственность, характеризующиеся следующими положениями:

– существующее законодательство применимо к различным проявлениям информационной технологии в большинстве случаев лишь по аналогии;

– вследствие развития новых технологий воспроизведения информации права на интеллектуальную собственность практически невозможно защитить.

Наиболее ярким примером вышесказанного служат все типы компьютерных записей, разработанные программистами, которые при желании должны подлежать защите авторским правом. Однако данное право не предполагает защиту идей и не дает право контроля над распространением проданного материала, оттого, возможно, желательный уровень юридический защиты следует искать не только в авторском праве, но и в совокупности с такими способами защиты, как лицензирование и лизинг.

В процессе принятия юридических требований с целью защиты тайны информации важную роль в обеспечении интересов производителей интеллектуальной собственности приобретает закон об утрате конфиденциальности. Он применяется к широкому ряду информационных материалов, таких общепринятых, как формулы, чертежи, производственные секреты, списки потребителей, финансовая информация, но также дополнительно включает следующую категорию – секреты личного свойства. Действие закона распространяется на письма, бумаги и переговоры (прямые, пересказанные или записанные). При этом необходимо отметить, что большинство стран, регулирующих обращение с конфиденциальной информацией, сочли непрактичной разработку детальных правил обращения с различными видами информации, будь то государственная, коммерческая, финансовая или частная информация, что признано целесообразным, так как это наличие достаточно гибкой правовой основы, распространяющейся на любую информацию. В данном ключе намечена тенденция сочетать Закон о нарушении конфиденциальности с правилами безопасности. Однако на этом пути важно помнить, что данное стремление защитить информацию не должно ограничиваться только требованиями военной или национальной безопасности, но и распространяться на защиту частной жизни, защиту от убытков, мошенничества, злоупотреблений и т.п.

Остается добавить, что главной заботой правительства должно являться предотвращение информационных преступлений, в противном случае их быстрейшее установление в целях минимилизации риска. Для чего необходим постоянный контроль и анализ возможных рисков, то есть определение потенциально уязвимых мест в информационных системах от случайных или преднамеренных угроз.

Как показывает юридическая практика в сфере информационной безопасности, для достижения минимальной защиты от информационных преступлений необходимо иметь ряд соответствующих законов:

– требования по безопасности и сохранности данных, основанных на международно принятых технических стандартах;

– законы, гарантирующие пользователям применение юридических инструментов в необходимых случаях, защищающих интересы граждан;

– законы и правила, регулирующие межграничные потоки данных и гарантирующие сохранение национальных интересов в информационной сфере для каждой страны.

Таким образом, каждое государство в целях реализации эффективно действующей системы информационной безопасности должно разработать и обеспечить успешное функционирование двух следующих групп мер. Первая группа мер направлена на формирование в обществе негативного образа нарушителя информационной безопасности, помимо сказанного она включает четко сформулированные санкции и наказания за отдельные виды нарушений. Вторая группа содержит координирующие меры, направленные на повышение

уровня информированности и образованности общества в сфере информационной безопасности. В конечном итоге совокупное функционирование перечисленных мер должно стать определяющим в процессе обеспечения информационной безопасности, поскольку выделенные меры заблаговременно предупреждают появление различного характера нарушений в информационной среде.

Список литературы

1. **Гостехкомиссия России**: руководящие документы Гостехкомиссии России [Электронный ресурс]. URL: http://www.ivtechno.ru/files/rd_filter.pdf (дата обращения: 05.02.2013).
2. **Громов Е. В.** Развитие уголовного законодательства о преступлениях в сфере компьютерной информации в зарубежных странах (США, Великобритании, ФРГ, Нидерландах, Польше) // Вестник Томского государственного педагогического университета. 2006. № 11. С. 30-35.
3. **Управление государственными информационными системами: элементы стратегии и политики** // Информационная революция: наука, экономика, технология. М.: ИНИОН РАН, 2009. С. 202-235.
4. **Хужин А. М.** Философские понятия вины и невиновности // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики: в 3-х ч. Тамбов: Грамота, 2011. № 2 (8). Ч. II. С. 196-200.
5. **Common Criteria for Information Technology Security Evaluation Security** [Электронный ресурс]. URL: http://www.ipa.go.jp/security/jisec/cc/documents/CCPART1V3.1R4.pdf (дата обращения: 05.02.2013).
6. **Department of Defense Trusted Computer System Evaliation Criteria, TCSEC, DoD 5200.28-STD, December 26, 1985** [Электронный ресурс]. URL: http://csrc.nist.gov/publications/history/dod85.pdf (дата обращения: 05.02.2013 г.).
7. **Electronic Frontier Foundation** [Электронный ресурс]. URL: https://www.eff.org/ (дата обращения: 10.01.2012).
8. **Federal Information Technology Security Assessment Framework** [Электронный ресурс]. URL: http://csrc.nist.gov/drivers/documents/Federal-IT-Security-Assessment-Framework.pdf (дата обращения: 05.02.2013).
9. **Federal Office for Information Security** [Электронный ресурс]. URL: http://www.bsi.bund.de/EN/Home/home_node.html (дата обращения: 05.02.2013).
10. **Management of Government Information Systems, Elements of Strategies and Policies.** N. Y., 2009. 192 p.

ETHICAL-LEGAL ASPECTS OF INFORMATION SECURITY

Manzhueva Oksana Mikhailovna, Ph. D. in Philosophy, Associate Professor
East-Siberian State Academy of Culture and Arts
ocydenova@yandex.ru

The article determines the value of ethical-legal norms in the process of information technologies application. The problem of computer crime is highlighted as a burning topic of modern society, the role of unified standards in solving information security problems is emphasized. The topic of copyright protection and ensuring the confidentiality of information in the broad use of information technologies is touched upon. The necessity of increasing the common level of awareness in society is emphasized for the purpose of preventing computer crimes in advance.

Key words and phrases: legislation; intellectual property; information security; confidentiality of information; standards and specifications.

УДК 32.019.5
Политология

Статья посвящена Интернету как новому каналу манипулятивного воздействия на массовое политическое сознание. В статье проводится сравнительный анализ телевидения и Интернета как каналов распространения информации; выделяются основные отличительные особенности Интернета как канала манипулятивного воздействия. На основании полученных данных проводится анализ влияния основных отличительных особенностей Интернета на появление новых технологий политического манипулирования.

Ключевые слова и фразы: Интернет; телевидение; информация; канал манипулятивного воздействия; массовое политическое сознание; политическое манипулирование.

Маслова Анна Александровна
Санкт-Петербургский государственный университет
knorozochka@yandex.ru

ИНТЕРНЕТ КАК НОВЫЙ КАНАЛ МАНИПУЛЯТИВНОГО ВОЗДЕЙСТВИЯ НА МАССОВОЕ ПОЛИТИЧЕСКОЕ СОЗНАНИЕ©

Начиная со второй половины XX в. основным каналом манипулятивного воздействия на массовое сознание являлось телевидение, что позволило некоторым исследователям выдвинуть тезис о начале принципиально