

Только принятие скоординированных мер в международном степени даст возможность правильно противодействовать нынешним призывам и угрозам информационной безопасности. При этом из числа вероятных направлений партнёрства подразумевается помощь исследованию международно-правовой основы партнёрства и формирование общего механизма в области обеспечения информационной безопасности.

Литература

1. Department of justice, Computer Crime and Intellectual Property Section (CCIPS). Seizing computers and obtaining electronic evidence in criminal investigations. Washington, DC: U.S. Department of Justice 2001, 558 p.
2. Freedom of Information: The Right to Know. World Press Freedom Day 2010. Typeset by UNESCO. CI-2011/WS/1 Rev. 141 p.
3. Johnson Joseph and Susan J. Lincke. A Comparison of International Information Security Regulations. Interdisciplinary Journal of Information, Knowledge, and Management Volume 9, 2014, 88-116 p.
4. Mathiesen Kay. Access to Information as a Human Right. Conference Paper / Presentation. P. 6.
5. Singh Rajeev Kumar. Right to Information: The Basic Need of Democracy. Journal of Education & Social Policy. Vol. 1, No. 2; December 2014, 86-96 p.

УДК 342 (043.2)

Ибрагимова Айтекин, доктор философии по праву, доцент,
Бакинский государственный университет, г. Баку, Азербайджан

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ

Под информационной безопасностью организации понимается проведение необходимого анализа безопасности и применение превентивных мер с целью выявления информированных лиц, выявления уязвимых моментов и их защиты от нежелательных угроз [1, с. 233]. Информационная безопасность может быть определена в основном как совокупность систем защиты информации и защиты от несанкционированного доступа, использования, разглашения, изменения, применения, повреждения информации, охватываемой системой, и связанных с ними мер [4, с. 394]. Здесь следует обратить внимание на рассмотрение понятия информационной безопасности независимо от используемой технологии. Информация, будь то на бумаге или в электронном виде, всегда нуждается в защите от угроз, исходящих ее хранителей и пользователей. Изначально информационная безопасность рассматривалась только как комплекс мер, направленных на защиту национальной безопасности. Однако в результате цифровизации

информации, ее размещения и хранения в системе вследствие развития информационных и коммуникационных технологий проблема безопасного хранения, защиты и использования информации стала общей проблемой для всех владельцев информационных систем. С переходом к информационному обществу все информационные системы, от персональных компьютеров до самых сложных информационных технологий начали хранить информацию, и вследствие этого понятие информационной безопасности приобрело значимость наряду с цифровизацией.

Определение информации: для лучшего понимания концепции информационной безопасности, вначале необходимо определить информацию, которая является базовой основой информационных и коммуникационных технологий. Понятие «информация» используется как эквивалент понятий, используемых в английском языке для обозначения понятий, связанных с информацией (data, information, knowledge). Однако более подходящим является использование в качестве перевода этих терминов слов «данные», «информация», «знание» [2, с. 168]. Следующие определения этих терминов раскрывают разницу между ними.

Данные (data): Данные - это название не связанных с друг другом цифровых сетей. Данные, существующие в этой информационной системе, состоят из чисел и сами по себе не имеют никакого значения (например: 1.400; 6.3 или 29000 AZN). С другой стороны, с точки зрения информационных технологий, данные можно объяснить как еще не связанные с друг с другом информации об одной проблеме, или, вкратце как сигналы, существующие и передающиеся в цифровой среде.

Информация (information): форма данных, которая структурирована или организована в значимой форме. Для использования данного его необходимо преобразовать в форму информации. Данные, существующие в информационной системе, представляются пользователю в содержательной форме в виде сообщения.

Знание (knowledge): знание следует интерпретировать как приобретение или понимание реалий, истин или информации, полученных в результате опыта, обучения или внутреннего наблюдения. Знание состоит из четырех классов: знание того, **что, для чего, как и кто** есть нечто. Ответ на эти четыре основных вопроса формирует объем знания в целом. Вышеупомянутые понятия, как данные, информация, знание, являясь теоретическими понятиями, также приводят к ряду практических последствий [7, с. 175].

Носители информации: носители, которые содержат информацию в информационной системе и доступны, могут быть написаны и организованы для всей системы управления. Некоторые из этих носителей имеют решающее значение для запуска и работы системы. Эти носители информации называются основными носителями информации. Целью

информационной безопасности является обеспечение безопасности носителей информации, обеспечивающих полное и доступное хранение информации в информационной системе [6, с. 189]. Базы данных в информационной системе, электронная почта, сетевой сервер, сетевые браузеры, используемые для доступа к этим ресурсам, могут рассматриваться как основные носители информации информационной системы.

Круг охвата информационной безопасности: информационная безопасность - это концепция управления безопасностью, которая охватывает широкий спектр информационных систем, от персональных компьютеров до всех информационных систем на корпоративном и национальном уровнях [8]. На корпоративном уровне информационная система включает пользователей, которые используют информационные системы в качестве третьей стороны, и программное обеспечение, обеспечивающее техническую поддержку информационных систем. Информационная безопасность - это процесс хранения и обработки информации в цифровой среде безопасным способом для предотвращения несанкционированного доступа без нарушения целостности информации. Для обеспечения этого необходимо определить и внедрить соответствующие политики безопасности. В более общем смысле информационная безопасность рассматривается как ветвь «инженерии безопасности», которая подробно занимается вопросами безопасности [3, с. 257]. Английский термин «information security» переводится как информационная безопасность. Использование в качестве эквивалента термина «information assurance» термина «информационное обеспечение» будет более уместным [5, с. 173]. В информационном обеспечении технические и долгосрочные потребности информационной безопасности в информационной системе рассматриваются на более стратегическом уровне, в то время как понятие информационной безопасности имеет более тактическое значение.

Литература

1. Baykara M., Daş R. ve İ. Kardoğan. Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi, 1st International Symposium on Digital Forensics and Security, Elazığ, s:231-239. s. 233.
2. Canbek G., Sağiroğlu Ş. Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme, Gazi Üniversitesi Politeknik Dergisi, 2006, Cilt: 9 Sayı: 3 ss. 165-174, s. 168.
3. Clarke G. CompTIA Security+ Certification Study Guide (Exam SY0-301). s.l.: McGraw Osborne Media (2011) 806 p., p. 257.
4. Daniel M. White. The Federal Information Security Management Act of 2002: A Potemkin Village 79 Fordham L. Rev. (2011) p. 370-405, p. 394.
5. Dulaney E. Chuck E. CompTIA Security+ Study Guide: Exam SY0-201. Fourth Edition dü. s.l.: John Wiley & Sons, 2017, 528 p. p. 173.

6. Graves, K. CEH Certified Ethical Hacker Study Guide. s.l.: John Wiley & Sons. Grutzmacher, 2010, p. 393, p. 189.

7. Thomas H. Davenport. Big Data at Work: Dispelling the Myths, Uncovering the Opportunities, Harvard Business Review Press, 2014, 240 p., p. 175.

8. <http://ina.bnu.edu.cn/docs/20140520102905252150.pdf>. 17.10.2019.

УДК 342.565 + 342.571(043.2)

Guoqiang Fu,
Legal Specialist, Singapore

ОСОБЕННОСТИ УЧАСТИЯ ГРАЖДАН В ОТПРАВЛЕНИИ ПРАВОСУДИЯ В ГОНКОНГЕ

Особенности участия граждан в отправлении правосудия является важной характеристикой конституционного устройства государства [1, 2]. Данная работа посвящена изучению особенностей участия граждан в отправлении правосудия в Гонконге [2, с. 263-265].

В Гонконге граждане принимают участие в отправлении правосудия в качестве присяжных заседателей (jurors) в Высоком суде (High Court), являющемся судом общей юрисдикции по гражданским и уголовным делам и выступающим как суд первой инстанции. С участием присяжных в Высоком суде предусмотрено рассмотрение гражданских и уголовных дел, а также дел по установлению невменяемости. Граждан также могут вызывать для участия в коронерском расследовании (coroner's inquest) в составе коронерского жюри (coroner's jury). Лица в возрасте от 21 года до 65 лет, постоянно проживающие в Гонконге, имеют право быть присяжными заседателями или участвовать в коронерском расследовании. Коллегии присяжных заседателей, участвующие в рассмотрении всех гражданских дел, уголовных дел и дел по установлению невменяемости формируются в составе 7 человек, за исключением случаев, когда по постановлению судьи они могут быть сформированы в составе 9 человек. Освобождаются от исполнения обязанностей присяжных заседателей члены Исполнительного совета и Законодательного собрания Гонконга, мировые судьи, судьи и их помощники, регистраторы судов, служащие судов, коронеры, работники министерства юстиции, полицейские, работники иммиграционной службы, таможенники, пожарные, работники исправительных учреждений, лица, осуществляющие надзор за условно осужденными, консулы, вице-консулы и лица аналогичного ранга, барристеры по закону и практикующие солиситоры, зарегистрированные врачи, дантисты, ветеринары, редакторы ежедневных газет, фармацевты и аптекари, священнослужители христианской, иудейской, мусульманской, индусской религиозных конгрегаций, монахини, студенты учебных