Секция «Государственное управление и политический процесс в современной России»

Информационная безопасность в сфере государственного управления

Научный руководитель – Морозов Илья Леонидович

Винников Артем Игоревич
Студент (магистр)
Волгоградский филиал Российской академии народного хозяйства и государственной службы, Волгоград, Россия
E-mail: artem-vinn@mail.ru

В наше время получение информации является одной из составляющих развития нашего общества. Получая новую информацию начиная обрабатывать ее и использовать, в своих целях. Можно заметить, что в процессе обработки информации приходим к новому обществу от индустриального к информационному.[1]

Под термином информационная безопасность автор работы предлагает понимать режим, обеспечивающий гарантированную защиту информации от несанкционированного доступа к ней, разрушения или искажения, а так же контроль и сохранение инструментов, осуществляющих передачу данной информации.

Особое явление, на котором стоит сконцентрировать внимание — это осуществление обмена информацией между государствами. При этом вопрос о сохранении достоверной информации стоит более серьёзней чем, казалось бы. Основной проблемой является намеренное искажение достоверной информации через зарубежные средства массовой информации, связано это прежде всего из политических и экономических интересов соперничающих государств. Контролировать интернет-пространство на территории России является одной из приоритетных задач, а за пределами ее территорий вообще является задачей не выполнимой.

Способы решения данной проблемы рассмотрим на уровне IT-технологий. Используя такой метод как шифр, можно обеспечить безопасность данной информации. Понимая, что, не использовав методы для сохранения информации возможна утечка через интернет и другие источники, в следствии так же приходится прибегать к таким методам как блокировка не официальных сайтов, контроль запрещённых серверов.

При массовой цифровизации производственных и управленческих процессов значительно упростилась задача в работе в многих сферах деятельности, но с появлением такого ресурса в отдельно взятом государстве возникает опасение, является ли это оправданной частью и стоит рисковать конфиденциальностью данной информации? Затрагивая такую проблему как приватность на государственном уровне стоит отметить возможные риски и последствия при вмешательстве постороннего в эту сферу. Основным и самым секретным пунктом является государственная тайна.

Одним из ярких вмешательств государства в осуществлении слежки и сбора информации - после серии терактов в 2001 году государственными служащими США был проведен комплекс мер для неправомерного, на тот момент, сбора информации. Информация снималась буквально со всех слабозащищённых коммуникационных государственных линий и организаций, частных лиц или просто иностранцев, посетивших Америку. Агентство Национальной Безопасности, которое занималась данной процедурой, утверждало, что действия совершались исключительно ради безопасности и пресечения повторного террористического акта. Рассматривая проблему на много масштабнее, можно понять, что полученная информация, которая находилась в обработке Агентства могла быть использована против личности в любой момент. Использование программы PRISM позволило

поставить под частичный контроль и зарубежные информационные ресурсы, что нарушило суверенитет других государств.[2]

В настоящее время проблематика информационной безопасности находится в фокусе внимания российского руководства, идет эволюция законодательной базы.[3] Для решения проблемы в России используются как общие меры безопасности, так и осуществление профилактики и контроля за внешними рисками. В соответствии Федерального закона от 20 февраля 1995 г. N 24-ФЗ "Об информации, информатизации и защите информации", на территории Российской Федерации регулируются права конфиденциальной информации.[4]

Российские эксперты отмечают безусловное преобладание принципов «запретительного подхода» в государственной информационной политике, который несет в себе как определённые плюсы, так и соответствующие риски.[5] Анализ нормативной правовой базы России в сфере обеспечения информационной безопасности, позволил выявить следующие закономерности: основной упор делается на оборонную промышленость с применением усовершенствованных информационных технологий, сохраняя территориальную целостность страны, устранение внешних и внутренних военных конфликтов, предотвращение нарушение стабильности государства. Обеспечение информационной безопасности в политической и социальной сфере гарантирует сохранение суверенитета государства, основных прав и свобод человека. [6]

[1] Голицын Г. А. Информатизация. Поведение. Товрчество. / Г. А. Голицын, В.М. Петров. М. Наука. 1991.

[2] Гринвальд Г. Негде спрятаться. Эдвард Сноуден и зоркий глаз Дядюшки Сэма. Питер. 2014.

[3] Morozov I.L. Legal Basis of State Management Decisions in the Field of Russia's Information Security: Politological Analysis // Political Science Issues. 2020. Т. 10. № 3 (42-44). С. 331-338.

[4] Федеральный закон от 20 февраля 1995 г. N 24-ФЗ "Об информации, информатизации и защите информации" Российской Федерации на период до 2025 года и дальнейшую перспективу" [Электронный ресурс] // Справочно-правовая система «Гарант» - Режим доступа: http://www.garant.ru, свободный. - Загл. с экрана.

[5] Морозов И.Л. Государственная политика в сфере информационной безопасности по легитимации политического порядка современной России - тенденции, проблемы, решения // Общество: политика, экономика, право. 2020. № 9 (86). С. 12-15.

[6] Доктрина информационной безопасности Российской Федерации. 2016. №646. С. 5.