УДК 342 **DOI: 10.34670/AR.2021.40.90.021**

К вопросу об обеспечении защиты государственной тайны на современном этапе

Смирнова Карина Сергеевна

Кандидат юридических наук,
начальник кафедры специальных дисциплин,
Новороссийский филиал,
Краснодарский университет МВД России,
353911, Российская Федерация, Новороссийск, ш. Сухумийское, 12 км;
e-mail: mail2smirnova@mail.ru

Кривошеин Александр Александрович

Старший преподаватель кафедры тактико-специальной подготовки,
Волгодонский филиал,
Ростовский юридический институт МВД России,
347360, Российская Федерация, Волгодонск, ул. Степная, 40;
e-mail: mail2smirnova@mail.ru

Плешивцев Алексей Юрьевич

Кандидат педагогических наук,
старший преподаватель кафедры физической подготовки,
Волгоградская академия МВД России,
400089, Российская Федерация, Волгоград, ул. Историческая, 130;
e-mail: mail2smirnova@mail.ru

Челпух Эдем Айдерович

Курсант,
Новороссийский филиал,
Краснодарский университет МВД России,
353911, Российская Федерация, Новороссийск, ш. Сухумийское, 12 км;
e-mail: mail2smirnova@mail.ru

Аннотация

Данная статья посвящена актуальной проблеме, связанной со сложностями обеспечения защиты государственной тайны на современном этапе развития государств и научно-технического прогресса. В статье рассматриваются потенциальные угрозы вопросов защиты государственной тайны в Российской Федерации. Сегодня большинство органов, ведомств и служб, работающих со сведениями, составляющими государственную тайну и обеспечивающих ее защиту используют многоуровневые системы обработки информации – компьютеры, облачные хранилища, корпоративные сети и так далее. Все

эти системы не только передают информацию, но и являются средой ее возможной утечки по техническим каналам. Утечка информации – это несанкционированный доступ к закрытым данным и неконтролируемое распространение секретных сведений в результате их разглашения. В статье рассматриваются виды реализации угроз информационной безопасности, представлены возможности условий утечки секретной информации, проанализированы проблемные вопросы защиты государственной тайны от технической утечки, а также внутренние угрозы, которые берут свое начало в несовершенстве законодательства по этому вопросу к которым добавляются возможности, созданные развитием научно- технического процесса. Представлены варианты путей решения проблемных вопросов защиты государственных секретов от утечки по техническим каналам на современном этапе развития Российской Федерации.

Для цитирования в научных исследованиях

Смирнова К.С., Кривошеин А.А., Плешивцев А.Ю., Челпух Э.А. К вопросу об обеспечении защиты государственной тайны на современном этапе // Вопросы российского и международного права. 2021. Том 11. № 6А. С. 156-162. DOI: 10.34670/AR.2021.40.90.021

Ключевые слова

Государственная тайна, государство, закон, законодательство, угроза, безопасность, хакер, утечка, научно-технический прогресс, защита информации, интернет, государственные секреты, безопасность государства.

Введение

События последних нескольких лет однозначно говорят о значимости проблемы безопасности информации, вопросы охраны государственной тайны со временем не теряют своей актуальности, так как государственная тайна любой страны является частью ее суверенитета и, несомненно, должна охраняться как можно тщательнее. При этом одной из важнейших составляющих национальных интересов Российской Федерации в информационной сфере является защита информационных ресурсов, содержащих сведения, относящиеся к государственной тайне, от несанкционированного доступа.

Однако, с каждым годом осуществлять данную защиту становится сложнее ввиду множества факторов. К тому же защита государственной тайны на данном этапе привлекает к себе внимание не только со стороны государства, но и со стороны граждан. Подтверждается данный интерес повышенным числом возбужденных уголовных дел, связанных с утечкой государственной тайны по различным каналам, в том числе техническим. Сегодня большинство организаций, работающих со сведениями, составляющими государственную тайну и обеспечивающих ее защиту используют многоуровневые системы обработки информации – компьютеры, облачные хранилища, корпоративные сети и т. д. Все эти системы не только передают данные, но и являются средой возможной утечки информации.

Основное содержание

Утечка информации – это несанкционированный доступ к закрытым данным и неконтролируемое распространение секретных сведений в результате их разглашения. Выделяют три вида утечки информации: разглашение, несанкционированный доступ к

информации, получение секретной информацией разведками.

Под разглашением информации понимается запрещённая передача служебной или секретной информации до людей, не имеющих на неё права. Под несанкционированным доступом понимается получение запрещённой информации ложным или обманным путём лицом, не имеющим на неё права. Получение секретной информации разведками может осуществляться с помощью технических средств или агентурными методами.

Большую опасность для государственной тайны, как бы это не звучало странно, представляет научно-технический прогресс, развитие коммуникационных возможностей людей. К примеру, это выражается в появлении большого количества различных мессенджеров, позволяющих людям общаться на большом расстоянии, передавать фото, видео, звуковые материалы без особых усилий, а также глобализация сети «Интернет».

Изначально заложенная цель в создание сети «Интернет» и мессенджеров выражалась в облегчении коммуникаций между людьми. И как оказалось, из благородной цели вытекает менее благородное последствие.

Способы, которые избирают преступники при совершении преступлений в сети «Интернет», нестандартные, сложные, многообразные и постоянно обновляются и модернизируются. Один человек при наличии слабых компьютерных мощностей способен реализовать самые сложные сценарии преступлений. Кроме того, лица совершающие преступления используют сеть «Интернет» для обмена новыми способами и результатами применения данных способов. [Чернецкий, Говорун, Картавцев, 2021]

Но чтобы более подробно рассмотреть данную проблему, во-первых, стоит обратить внимание на несовершенство существующей системы правового регулирования защиты государственной тайны.

Как известно, главным нормативно-правовым актом, регулирующим деятельность, связанную с защитой государственной тайны в интересах обеспечения безопасности Российской Федерации является Закон РФ «О государственной тайне» от 21 июля 1993 № 5485-1, который можно рассматривать как основу деятельности всех, работающих с государственной тайной, органов, ведомств и служб. Однако, в данный момент времени, «Законы» уже не актуальны в иерархии нормативно-правовых актов Российской Федерации, но, исходя из того, что они не были признаны утратившими силу, а актов заменяющих их не было разработано, Закон РФ «О государственной тайне» от 21 июля 1993 № 5485-1 является действующим, но сейчас он перестал отвечать всем требованиям такого закона, неактуальность выражается уже в его названии и несоответствии текста закона современным реалиям, неактуальности иных основополагающих нормативно-правовых актов в области защиты государственной тайны, на которые имеется ссылка в данном законе. [Смирнова, Литвяк, Челпух, 2019, 301-303]. Исходя из данной позиции можно сделать вывод, что проблемные вопросы защиты государственной тайны от утечки, внутренние угрозы, берут свое начало в несовершенстве законодательства по этому вопросу к которому добавляются возможности, созданные развитием научно- технического процесса.

Если говорить о внешних угрозах защите государственной тайны Российской Федерации и любой другой страны, опираясь на достижения государств в научно-техническом и коммуникационном прогрессе, достаточно вспомнить нашумевшее дело 2013 года, главным фигурантом которого является Эдвард Сноуден. Э. Сноуден, будучи сотрудником Агентства национальной безопасности (АНБ) США, передал газетам The Guardian и The Washington Post секретную информацию, принадлежащую АНБ, касающуюся тотальной слежки американских спецслужб за информационными коммуникациями между гражданами многих государств по всему миру при помощи существующих информационных сетей и сетей связи

[https://ru.wikipedia.org/wiki/Сноуден,_Эдвард].

Итак, развитие коммуникационных способностей стран и граждан является не только удобством, но и угрозой. Иначе говоря, данный прогресс можно назвать «непреодолимой силой» поскольку остановить его невозможно, а, следовательно, невозможно обезопасить информационные данные граждан и государств. Преступления, совершаемые в отношении «секретов», обеспечиваются за счёт многоуровневой и сложной сетевой инфраструктуры, а также полной анонимности действий. Трансграничный характер преступлений позволяет преступнику находиться в одном государстве, а потерпевшему в другом, и оба лица находятся под юрисдикцией своих государств. [Чернецкий, Говорун, Картавцев, 2021]

Государству необходимо разрабатывать различные варианты защиты своих секретов от утечки по различным каналам, так как Э. Сноуден является не первым человеком придавшем огласке факт шпионажа и похищения государственной тайны одним государством у других. Например, в 1960 году произошёл побег в СССР сотрудников АНБ Уильяма Мартина и Бернона Митчелла. Перебежчики АНБ сообщили в КГБ, что американская спецслужба перехватывает секретные правительственные сообщения не только потенциальных противников, но также и ближайших союзников, прежде всего Великобритании [Нехорошев URL: http://www.sovsekretno.ru/articles/shpion-netraditsionnoy-orientatsii].

Российская Федерация создает условия предотвращению утечки своих государственных секретов по различным каналам всеми имеющимися способами и методами. На законодательном уровне выносятся нормативные акты и различного рода предложения по увеличению уровня защиты информации. Для обеспечения технической защиты в части ограничения или ограждения коммуникаций внутри государства от внешних воздействий и зависимостей.

К концу 2021 года в России планируется создать полностью автономную глобальную сеть «Интернет», работающую на серверах и доменах, принадлежащих государству. Относительно «Интернета» как источника потенциальной угрозы для утечки различных «секретов» также отмечал Президент РФ Владимир Путин, он подчеркивал, что интернет – это изобретение ЦРУ и западные спецслужбы используют его для прослушивания россиян и сбора оборонной информации [https://www.vesti.ru/article/1796534].

Мы не можем не согласиться в этом плане с главой государства, так как уже приводили пример сбора информации со стороны спецслужб США.

Автономный интернет позволит пропускать весь трафик внутри Российской Федерации через точки обмена, тем самым будет минимизирована передача данных за рубеж и, к тому же, весь трафик будет дополнительно контролироваться.

В 2019 году уже была сформирована правовая база для реализации автономного интернета, а именно был принят Федеральный Закон от 01 мая 2019 года № 90 -ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации», иначе говоря, закон о «суверенном интернете», который и предусматривает создание национальной системы маршрутизации интернет-трафика и инструментов централизованного управления.

Принятие данного закона также обосновывают необходимостью обеспечения безопасности России в случае отключения ее от глобальной сети «Интернет» международной некоммерческой организацией ICANN, расположенной в США.

Заключение

Таким образом, большую угрозу безопасности и обеспечению защиты государственной

тайны Российской Федерации от утечки по техническим каналам, несет в себе сеть «Интернет» и иные коммуникационные приложения. Поэтому мы можем лишь поддержать реализацию автономного интернета в государстве, так как отечественный интернет –действенная мера обеспечения государственной безопасности.

Библиография

1. Конституция Российской Федерации" (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // URL: http://www.consultant.ru/document/cons_doc_LAW_28399/2573feee1caecac37c442734e00215bbf1c85248/.
2. Аникин И.В., Глова В.И., Нигматуллина А.Н. Методы и средства защиты компьютерной информации: Учебное пособие. Казань: КГТУ 2008.
3. Горбатенков, О. Е. Кибертерроризм как преступление международного характера / О. Е. Горбатенков// Молодой ученый. — 2018. — № 18 (204). — С. 217-218. — URL: https://moluch.ru/archive/204/49961/.
4. Ищейнов В. Я., Мецатунян М. В. Защита конфиденциальной информации: Учеб. пособие. М.: ФОРУМ, 2009. 256 с.
5. Касъяненко М.А. Правовые проблемы при использовании Интернета в транснациональном терроризме // Информационное право. М., 2012. № 1.
6. Невская А.И., Петрова Е.П. Возможные причины утечки информации при нарушении персоналом правил работы с конфиденциальной информацией//Современные научные исследования и инновации. 2016. № 12 [Электронный ресурс]. URL: https://web.snauka.ru/issues/2016/12/75791 (дата обращения: 18.06.2021).
7. Нехорошев, Григорий. Шпион нетрадиционной ориентации. Совершенно секретно (8 декабря 2016) // URL: http://www.sovsekretno.ru/articles/shpion-netraditsionnoy-orientatsii/
8. Смирнова К.С., Литвяк Л.Г., Челпух Э.А. К вопросу о государственной тайне//Гуманитарные, социально-экономические и общественные науки. 2019. № 12. С. 301-303.
9. Чернецкий В.А., Говорун А.Ю., Картавцев Д.А. Некоторые особенности совершения преступления, а так же способы установления лиц, совершающих преступления в сети «интернет»//«Вопросы российского и международного права». 2021. №6.
10. Ищейнов В. Я., Мецатунян М. В. Защита конфиденциальной информации: Учеб. пособие. М.: ФОРУМ, 2009. 256 с.

Matter of protecting state secrets at the present stage

Karina S. Smirnova

PhD in Law
Chief of chair of the special disciplines of Novorossiysk branch,
Krasnodar University of the Ministry of Internal Affairs of the Russian Federation,
353911, 12 km Sukhumiiskoe hwy, Novorossiysk, Russian Federation;
e-mail: mail2smirnova@mail.ru

Aleksandr A. Krivoshein

Senior Lecturer
Department of Tactical and Special Training
Volgodonsk branch,
Rostov Law Institute of the Ministry of Internal Affairs of the Russian Federation,
347360, 40 Stepnaya st., Volgodonsk, Russian Federation;
e-mail: mail2smirnova@mail.ru

Aleksei Yu. Pleshivtsev

PhD in Pedagogy
Senior lecturer of the Department of Physical Training
Volgograd Academy of the Ministry of Internal Affairs of the Russian Federation,
400089, 130 Istoricheskaya st., Volgograd, Russian Federation;
e-mail: mail2smirnova@mail.ru

Edem A. Chelpukh

Cadet
Novorossiysk branch,
Krasnodar University of the Ministry of Internal Affairs of the Russian Federation,
353911, 12 km Sukhumiiskoe hwy, Novorossiysk, Russian Federation;
e-mail: mail2smirnova@mail.ru

Abstract

This article is devoted to an urgent problem associated with the difficulties of ensuring the protection of state secrets at the present stage of development of states and scientific and technological progress. The article examines the potential threats to the protection of state secrets in the Russian Federation. Today, most of the bodies, departments and services working with information constituting state secrets and ensuring its protection use multi-level information processing systems - computers, cloud storage, corporate networks, and so on. All these systems not only transmit information, but are also an environment for its possible leakage through technical channels. Information leakage is unauthorized access to classified data and uncontrolled distribution of classified information as a result of its disclosure. The article examines the types of implementation of threats to information security, presents the possibilities of conditions for the leakage of classified information, analyzes the problematic issues of protecting state secrets from technical leaks, as well as internal threats that originate in the imperfection of legislation on this issue, to which are added the opportunities created by the development of scientific technical process. Variants of ways of solving problematic issues of protecting state secrets from leakage through technical channels at the present stage of development of the Russian Federation are presented.

For citation

Smirnova K.S., Krivoshein A.A., Pleshivtsev A.Yu., Chelpukh E.A. (2021) K voprosu ob obespechenii zashchity gosudarstvennoi tainy na sovremennom etape [Matter of protecting state secrets at the present stage]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 11 (6A), pp. 156-162. DOI: 10.34670/AR.2021.40.90.021

Keywords

State secret, state, law, legislation, threat, security, hacker, leak, scientific and technological progress, information protection, Internet, state secrets, state security.

References

1. The Constitution of the Russian Federation" (adopted by popular vote on 12.12.1993 with amendments approved during the all-Russian vote on 01.07.2020) // URL: http://www.consultant.ru/document/cons_doc_LAW_28399/2573feee1caecac37c442734e00215bbf1c85248
2. Anikin I. V., Glova V. I., Nigmatullina A. N. Methods and means of protecting computer information: A textbook. Kazan: KSTU 2008.
3. Gorbatenkov, O. E. Cyberterrorism as an international crime / O. E. Gorbatenkov// A young scientist. — 2018. — № 18 (204). — Pp. 217-218. - URL: https://moluch.ru/archive/204/49961/.
4. Ishcheinov V. Ya., Metsatunyan M. V. Protection of confidential information: Textbook. Moscow: FORUM, 2009. 256 p.
5. Kasyanenko M. A. Legal problems when using the Internet in transnational terrorism // Information Law. Moscow, 2012. No. 1.
6. Nevskaya A. I., Petrova E. P. Possible reasons for information leakage when the staff violates the rules for working with confidential information//Modern scientific research and innovation. 2016. No. 12 [Electronic resource]. URL: https://web.snauka.ru/issues/2016/12/75791 (accessed: 18.06.2021).
7. Nekhoroshev, Grigory. A spy of an unconventional orientation. Top Secret (December 8, 2016) // URL: http://www.sovsekretno.ru/articles/shpion-netraditsionnoy-orientatsii/
8. Smirnova K. S., Litvyak L. G., Chelpukh E. A. On the issue of state secrets // Humanities, socio-economic and social sciences. 2019. No. 12. pp. 301-303.
9. Chernetsky V. A., Govorun A. Yu., Kartavtsev D. A. Some features of committing a crime, as well as ways to identify persons committing crimes on the Internet // "Issues of Russian and international law". 2021. №6.
10. Ishcheinov V. Ya., Metsatunyan M. V. Protection of confidential information: Textbook. Moscow: FORUM, 2009. 256 p.