(cc) BY

Галикберов Олег Владимирович
магистрант
ФГКОУ ВО «Университет прокуратуры РФ»
г. Москва

СРАВНИТЕЛЬНО-ПРАВОВОЕ ИССЛЕДОВАНИЕ В ОБЛАСТИ ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННЫМ УГРОЗАМ НА ПРИМЕРЕ РОССИИ, США И ГЕРМАНИИ

Аннотация: *в статье анализируются положения документов стратегического планирования США и Германии в сфере информационной безопасности с использованием сравнительно-правового метода научного исследования. Автором проводится сравнение с положениями отечественных правовых актов, посвященных информационной безопасности, а также рассматриваются некоторые проблемы, выявленные в ходе проведенного исследования.*

Ключевые слова*: документ стратегического планирования, информационная безопасность, информационная угроза, культура личной информационной безопасности, стратегия кибербезопасности.*

В настоящее время вопрос противодействия информационным угрозам стоит наиболее остро. Связано это в первую очередь с активизацией деятельности недружественных стран, направленной на манипулирование общественным сознанием в целях дестабилизации общественно-политической ситуации внутри страны. Как справедливо отмечала М.А. Евремова: «Основная задача государства с развитым информационным обществом – обеспечение информационной безопасности» [11, с. 3].

На данную проблематику не раз указывал Президент в своих выступлениях. Так, в послании Федеральному собранию, подчеркнул тенденцию увеличения числа агрессивных информационных атак, с целью исказить представления жителей нашей страны, в особенности молодого поколения о традиционных российских культурных и нравственных ценностях [15]. Не обошёл данную проблематику и И.В. Краснов, выступая на расширенном заседании коллегии

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

Генеральной прокуратуры. В выступлении он сделал акцент на возникновении различных рисков в условиях стремительного развития цифровых технологий. С этой целью, им было принято решение о создание специализированного надзорного подразделения, основной деятельностью которого является обеспечение информационной безопасности. И всего лишь за первый год своей работы, данное подразделение показало достойные результаты: «пресечено почти 90 тысяч нарушений, связанных с использованием на официальных интернет-ресурсах иностранных программных кодов, несертифицированных продуктов, размещением закрытых сведений в социальных сетях» [16].

Учитывая вышесказанное, актуальность вопросов обеспечения информационной безопасности не вызывает сомнения. В связи с этим необходимо используя научный метод сравнительно-правового исследования определить, каким образом обеспечивается информационная безопасность, какие приоритеты устанавливаются при её реализации в иностранных государствах на примере США и Германии и какие полезные идеи для нашей страны можно оттуда почерпнуть.

В Российской Федерации (далее-Россия) в сфере информационной безопасности выделяются два ключевых документа стратегического планирования: Стратегия национальной безопасности 2021 года [4] (далее Стратегия) и Доктрина информационной безопасности 2016 года [5] (далее Доктрина).

В свою очередь США также разрабатывают и принимают стратегию национальной безопасности (national security strategy) [8]. Данный документ стратегического планирования в США разрабатывается раз в 5 лет, что соответствует президентскому сроку. Иными словами, администрация нового президента заново формирует стратегию, определяя какие приоритеты будут реализовываться на данном этапе. В нашей стране, учитывая шестилетний президентский срок, стратегия обновляется раз в шесть лет. На основе стратегии, разрабатывается Доктрина в России и национальная стратегия кибербезопасности в США (national cybersecurity strategy), которая также действует в течение президентского срока. Последняя стратегия кибербезопасности в США была принята 1 марта 2023 года [9]. При схожем механизме разработки и принятия данных документов стратегического

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

планирования, наша Доктрина не обновлялась с 2016 года. Такая ситуация носит негативный характер, так как она разрабатывалась на основе положений стратегии национальной безопасности 2015, с тех пор национальные интересы и определяемые в соответствии с ними приоритеты и угрозы в информационной сфере, несколько изменились. В качестве одного из примеров, можно привести положение Стратегии, указывающее на то, что вооруженные силы недружественных государств, проводят мероприятия по выведению из строя объектов критической информационной инфраструктуры. Однако в Доктрине дается указание лишь на наращивание рядом стран возможностей для реализации такого рода действий. По мнению автора, ситуация, когда угрозы, определенные в Доктрине, не в полной мере согласуются с текущей обстановкой в мире, носит негативный характер, так как документ стратегического планирования, это в первую очередь руководство для всей системы органов публичной власти. От того какие задачи, приоритеты и угрозы в нём закреплены, зависит и направление деятельности этих органов, то, чему они будут противодействовать. Очевидно, что без определения актуальных угроз, невозможно полноценное, эффективное и своевременное обеспечение национальной безопасности в данной сфере.

В этой связи нельзя, не согласится с мнением Н.А. Молчанова, который указывал, что актуализация правовых основ информационной безопасности общества является объективной потребностью [12, с. 160]. Более того, видится возможным дополнить высказанную им позицию, отметив необходимость развития и актуализации правовых основ всей триады «личность, общество, государство». При этом основываясь на конституционных положениях, провозглашающих человека, его права и свободы высшей ценностью, защита личности должна иметь первоочередное значение [1].

Учитывая вышесказанное, интересна позиция Германии по вопросу обновления стратегии кибербезопасности. Обычный период обновления так же, как и в США, составляет 5 лет, однако в тексте самой стратегии кибербезопасности предусмотрена возможность обновления по истечению 4–6 лет после принятия, а в случаях существования значительных потребностях в изменении они могут

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

быть реализованы и раньше, то есть по необходимости [7]. Такой механизм видится крайне удачным решением по ряду причин.

Во-первых, чётко установлен срок, по истечении которого документ должен подвергнуться изменениям, и это вполне обосновано, учитывая стремительное развитие информационных технологий в настоящее время. В качестве примера можно обратиться к статистическим данным по использованию интернета населением нашей страны. За период с 2010 года по 2023 год количество граждан, использующих интернет на постоянной основе, увеличилось на 55% [10, с. 22]. Видна закономерность увеличения числа пользователей интернета, а вместе с этим всё большая часть деятельности общества перемещается в цифровую сферу, как следствие, увеличивающееся число потребителей способствует ускорению развития информационных технологий. Вполне возможно допустить, что в скором времени обновление стратегий кибербезопасности необходимо будет проводить с большей частотой.

Отсюда вытекает вторая причина, почему проводимая Германией политика в информационной сфере является удачной: возможность внесения изменения при существенной необходимости, о которой было сказано ранее, является дальновидной. Это позволит государству своевременно и эффективно реагировать на любые изменения, которые могут представлять опасность и потребовать формулирования новых задач и приоритетов для органов публичной власти. Так, В.М. Редкоус обращает внимание на несоответствие документов стратегического планирования в области обеспечения национальной безопасности текущим реалиям, предлагая досрочно разработать новую стратегию национальной безопасности [14, с. 21] Соглашаясь с приведенным мнением, необходимо отметить, что при существующих механизмах сделать это не представляется возможным, так как Федеральный закон «О стратегическом планировании», устанавливает конкретный срок корректировки стратегии: раз в шесть лет [3]. Механизма позволяющего внести досрочные изменения, как это реализовано в Германии, не предусмотрено. Видится возможным, в связи с этим, внести изменения, предусматривающие возможность Президента решать вопрос о досрочных изменениях документов стратегического планирования в сфере национальной безопасности.

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

В результате сравнительно-правового анализа также была выявлена тенденция, которая представляет угрозу для информационной безопасности, а именно: увеличивающиеся с каждым годом устройства «Интернета вещей». Данный термин в самом общем виде означает девайсы, которые могут подключаться к Интернету и имеют функциональное программное обеспечение с интегрированной технологией возможности удаленного управления. К ним могут относиться часы, холодильники, динамики, смарт-браслеты, медицинские устройства и т. п.

США и Германия полностью солидарны в том, что такие устройства представляют опасность для кибербезопасности. Производители, ввиду огромного спроса на такие устройства пренебрегают мерами защиты. Это значительно увеличивает возможности злоумышленников в информационном пространстве. Учитывая, что такие устройства могут использоваться не только гражданами для личного пользования, но и на производствах и объектах критической инфраструктуры, ущерб от использования уязвимостей этих устройств, вполне может представлять угрозу национальной безопасности в информационной сфере. Между тем, в нашей Доктрине нет ни одного упоминания данной проблематики и соответственно возможного порядка. В связи с этим видится возможным проработка данного вопроса и закрепление полученных результатов в профильных документах стратегического планирования в виде определения целей и направлений деятельности, которые должны запустить механизм противодействия данной угрозе.

Ещё одним аспектом, который позволяет обеспечить защищенность граждан в информационной сфере, является формирование «культуры личной информационной безопасности» (далее культура). Данный термин фигурирует в Доктрине, однако закрепленное определение для него, как и разъяснения, какие мероприятия необходимо проводить для развития культуры отсутствуют. Более того, отсылка на формирование культуры составителями Доктрины дается с использованием конструкции «в том числе», что не позволяет говорить о нём, как об одном из ключевых способах защиты.

Между тем, в германской стратегии вопросу повышения цифровой грамотности населения выделен целый параграф. Отмечается, что осведомленность о

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

безопасности в киберпространстве среди всех пользователей является фундаментальным требованием защит от цифровых рисков. При этом к пользователям относятся не только рядовые граждане, но и представители малого и среднего бизнеса. Для этих целей Германия активно реализует программы поддержки населения и бизнеса в вопросах информационной безопасности. Обучение цифровой грамотности повсеместно проводится в школах, университетах и рабочих местах. На постоянной основе происходит информирование населения о возможных киберугрозах. До граждан в доступной форме доводятся сведения о подведомственности возникающих ситуаций, что позволяет им незамедлительно обратиться в орган, который имеет возможность оказать помощь [7]. Такая политика, по мнению автора, является очередным удачным примером реализацией государством своих функций по обеспечению информационной безопасности. Плюсы проведения таких мероприятий заключаются в превентивном характере защиты, который позволяет избежать наступления опасных последствий или минимизировать их. Граждане, имеющие базовые знания о механизме реализации государством политики информационной безопасности, об основных угрозах и действиях, которые необходимо предпринять при возникновении той или иной ситуации, значительно повышают защищенность личности, общества и государства в целом. Как справедливо отметил А.А. Малюк: «Эффективность политики обеспечения информационной безопасности на 80% зависит от мер организационно-правового и гуманитарного характера» [13, с. 8]

Вопрос развития информационной культуры стоит на повестке дня в нашем государстве. Подтверждение этому является утвержденная Правительством в 2023 году концепция информационной безопасности детей. В данной концепции в качестве одной из основных задач ставится проведение мероприятий, направленных на повышение грамотности детей по вопросам информационной безопасности, формирование навыков законопослушного и ответственного поведения в цифровой среде [6]. Данная тенденция не может не радовать, однако следует учесть, что не только несовершеннолетние нуждаются в поддержке со стороны государства. Как уже отмечалось выше, все члены общества должны иметь

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

представление об информационной безопасности и её составляющих. В связи с этим видится возможным определения в Доктрине понятия «культура личной информационной безопасности», закрепление задач и приоритетов, направленных на реализацию данного института.

Подводя итоги, хотелось бы привести цитату из положения стратегии кибербезопасности США: “A resilient and flourishing digital future tomorrow begins with investments made today”. – «Устойчивое и процветающее цифровое будущее завтра начинается с инвестиций, сделанных сегодня».

Основываясь на результатах, полученных с использованием сравнительно-правового метода научного исследования, можно сказать о следующем: проблематика информационной безопасности является одним из приоритетных направлений для большинства развитых государств. Связано это со стремительным развитием информационных технологий, которое несёт в себе как положительные тенденции, так и новые опасности, которые требуют от государства принятия быстрых и решительных мер по их устранению. Наша Доктрина имеет существенный недостаток в виде морального устаревания. Особенно это заметно на фоне положений стратегий кибербезопасности США и Германии, которые в полной мере учитывают особенности не только текущей геополитической обстановки, но и тенденций развития информационных технологий, а также положительные и отрицательные результаты, которые были достигнуты за период действия предыдущих стратегий.

Сравнительное исследование также выявило некоторые удачные решения проводимой политики в информационной сфере, которые видится возможным использовать в нашей стране, что благотворно бы повлияло на степень защищенности личности, общества и государства.

Список литературы

1. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г., с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 №6-ФКЗ, от 30.12.2008 №7-ФКЗ, от 05.02.2014 №2-ФКЗ, от 21.07.2014 №11-ФКЗ, с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Российская газета. – 2020. – №144.

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

2. Федеральный закон «О безопасности» от 28.12.2010 №390-ФЗ // Собрание законодательства РФ. – 2011. – №1. – Ст. 2.

3. Федеральный закон «О стратегическом планировании в Российской Федерации» от 28.06.2014 №172-ФЗ // Собрание законодательства РФ. – 2014. – №26. Ч. 1. – Ст. 3378.

4. Указ Президента Российской Федерации «О Стратегии национальной безопасности Российской Федерации» от 02.07.2021 №400 // Собрание законодательства РФ. – 2021. – №27. Ч. 2. – Ст. 5351.

5. Указ Президента РФ «Об утверждении Доктрины информационной безопасности Российской Федерации» от 05.12.2016 №646.

6. Распоряжение Правительства РФ «Об утверждении Концепции информационной безопасности детей в Российской Федерации» от 28.04.2023 №1105-р // Официальный портал правовой информации [Электронный ресурс]. – Режим доступа: http://pravo.gov.ru/proxy/ips/?docbody=&link_id=18&nd=605444126&bpa=cd00000&bpas=cd00000&intelsearch=%EA%E0%F1++.

7. Стратегия кибербезопасности Германии 2021 года // Официальный сайт Федерального министерства внутренних дел и по делам общества [Электронный ресурс]. – Режим доступа: https://www.bmi.bund.de/EN/topics/it-internet-policy/cyber-security-strategy/cyber-security-strategy-node.html (дата обращения 17.03.2024).

8. Стратегия национальной безопасности США // Официальный сайт Белого дома [Электронный ресурс]. – Режим доступа: https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf (дата обращения: 17.03.2024).

9. Стратегия национальной кибербезопасности США // Официальный сайт Белого дома [Электронный ресурс]. – Режим доступа: https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/ (дата обращения 17.03.2024).

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

10. Абдрахманова Г.И. Цифровая экономика: 2023: краткий статистический сборник / Г.И. Абдрахманова, С.А. Васильковский, К.О. Вишневский [и др.]. – М.: НИУ ВШЭ, 2023. – 120 с.

11. Ефремова М.А. Уголовно-правовая охрана информационной безопасности: монография / М.А. Ефремова. – М.: Юрлитинформ, 2018. – 306 с. – EDN ZIHCGL

12. Молчанов Н.А. Доктрина информационной безопасности Российской Федерации (новелла законодательства) / Н.А. Молчанов, Е.К. Матевосова // Актуальные проблемы российского права. – 2017. – №2. – С. 159–163. – DOI 10.17803/1994-1471.2017.75.2.159-165. – EDN YKGDBZ

13. Малюк А.А. Актуальные вопросы создания системы массового обучения культуре информационной безопасности / А.А. Малюк, З.П. Малюк // Безопасность информационных технологий. – 2021. – Т. 28. №4. – С. 6–21. DOI 10.26583/bit.2021.4.01. EDN XHPGMY

14. Правовое обеспечение национальной безопасности. Тридцать лет законодательству о безопасности Российской Федерации: сборник материалов Всероссийской научно-практической конференции (Москва, 22 апреля 2022 г.). – М.: Проспект, 2023. – 272 с.

15. Послание Президента Федеральному собранию // Официальный сетевой ресурс Президента Российской Федерации [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/events/president/transcripts/statements/70565 (дата обращения 17.03.2024).

16. Расширенное заседание коллегии Генеральной прокуратуры // Официальный сетевой ресурс Президента Российской Федерации [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/events/president/transcripts/70678 (дата обращения 17.03.2024).

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)