ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ОСОБЕННОСТИ ПОСТРОЕНИЯ СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ В ЗАРУБЕЖНЫХ ГОСУДАРСТВАХ (НА ПРИМЕРЕ МОДЕЛИ ТУРЕЦКОЙ РЕСПУБЛИКИ)

ORGANIZATIONAL AND LEGAL FEATURES OF BUILDING A CYBERSECURITY SYSTEM IN FOREIGN COUNTRIES (ON THE EXAMPLE OF THE MODEL OF THE REPUBLIC OF TURKEY)

УДК 343. 9

Ковалев О. Г., доктор юридических наук, кандидат психологических наук, профессор, профессор кафедры организации режима и оперативно-розыскной деятельности в уголовно-исполнительной системе, Псковский филиал Академии ФСИН России г. Псков.

Скипидаров А. А., магистрант, ФГБОУ ВО Псковский государственный университет, г. Псков.

Kovalev O. G., okovalev66@gmail.com

Skipidarov A. A., temapskov@yandex.ru

Аннотация

В статье рассматриваются организационные и нормативно-правовые особенности построение системы кибебезопасности в Турецкой Республике (Турецкая модель). Проведенное теоретическое исследование показало, что данная модель кибербезопасности имеет комплексный, оборонно-наступательный характер, сочетает в себе как оборонительные, так и активные наступательные действия, проведение тактических кибератак на упреждение возможной киберугрозы. Изучение проблемы проказало, что Турецкая Республика больше других стран использовала при построении системы кибербезопасности опыт развитых государств в данном направлении с участием специалистов военного ведомства и гражданских экспертов. При

этом правительством Республики первостепенное внимание уделяется развитию и совершенствованию социального статуса и имиджа подразделений, участвующих в обеспечении кибербезопасности. Специальные подразделения объеденены в соответствующую структуру, состоящую из пяти основных департаментов: правоохранительного, военного, морского, космического и комплексной обороны. Перечисленные дапертаменты взаимодействуют с профильными министерствами и ведомствами в вопросах предупреждения и реагирования на возникающие киберугрозы, разрешения киберситуаций различной степени сложности. Проведенный сравнительный и контент анализ показал, что Турецкой Республике в последние годы удалось создать масштабную, системную и устойчивую структуру кибербезопасности, организационно отличную от других развитых зарубежных стран, использованием возможностей активно привлекаемых хакерских киберсообществ, а также хакеров-одиночек, принимающих участие в обеспечение национальной кибербезопасности Республики.Государственными структурами применяется эффективная, простая и мобильная система нормативно-правового регулирования кибербезопасности государства.

Annotation

The article discusses the organizational and regulatory features of building a cybersecurity system in the Republic of Turkey (Turkish model). The conducted theoretical research has shown that this model of cybersecurity has a complex, defensive-offensive character, combines both defensive and active offensive actions, conducting tactical cyberattacks to prevent a possible cyber threat. The study of the problem showed that the Republic of Turkey, more than other countries, used the experience of developed countries in this area with the participation of military specialists and civilian experts in building a cybersecurity system. At the same time, the Government of the Republic pays primary attention to the development and improvement of the social status and image of the units involved in ensuring cybersecurity. Special units are combined into a corresponding structure consisting

of five main departments: law enforcement, military, maritime, space, and integrated defense. These departments interact with relevant ministries and departments in the prevention and response to emerging cyber threats, and in the resolution of cyber situations of varying degrees of complexity. The comparative and content analysis conducted showed that in recent years, the Republic of Turkey has managed to create a large-scale, systematic and stable cybersecurity structure, organizationally different from other developed foreign countries, using the capabilities of actively involved hacker cyber communities, as well as lone hackers involved in ensuring the national cybersecurity of the Republic.Government agencies use an effective, simple and mobile system of regulatory and legal regulation of cybersecurity of the state.

Ключевые слова: киберезопасность, Турецкая Республика, Турецкая модель, оборонно-наступательный характер, кибератака, киберугроза, департаменты, правоохранительный, военный, морской, космический, комплексной обороны, хакерские киберсообщества, хакеры-одиночки.

Keywords: cybersecurity, Republic of Turkey, Turkish model, defense-offensive nature, cyber attack, cyber threat, departments, law enforcement, military, maritime, space, integrated defense, hacker cyber communities, lone hackers.

Проблема организации системы и стратегии кибербезопасности учреждений и органов государственного сектора, промышленных и оборонных предприятий, компаний и корпораций, бизнес структур, является приоритетной для многих технологичных государств, развивающихся в век современных информационных технологий, постоянно изменяющегося киберпространства, возникающих киберугроз и киберситуаций, осуществляемых кибератак и киберпреступлений.

Проводимое нами комплексное теоретико-эмпирическое исследование позволило определить и описать основные подходы различных зарубежных государств в организации кибербезопасности, выделить различные модели («Североамериканскую», «Европейскую», «Китайскую», «стран Юго-Восточной Азии», «Иранскую» и «Северокорейскую»).

Данные исследования представляют не только познавательный интерес, но и могут быть полезны при организации эффективной и современной национальной модели обеспечения кибербезопасности высокого уровня.

В рассматриваемом контексте заслуживает внимания опыт, накопленный в данной сфере в Турецкой Республике - «Турецкая модель обеспечения кибербезопасности».

Рассматриваемая стратегия кибербезопасности имеет комплексный, оборонно-наступательный характер, сочетает в себе как оборонительные, так и активные наступательные действия, проведение тактических кибератак на упреждение возможной киберугрозы.

Наиболее вероятными противниками Анкары в киберпространстве выступают государства (Египет, Эфиопия, Греция и Израиль), а также политические движения и радикальные, экстремистские группировки, к которым действующая власть относит движение Гюлена, рабочую партию Курдистана и другие.

Изучение и систематизация доступных публикаций по теме показали, что создание турецкой системы кибербезопасности было начато в 2011 году и активно осуществлялось в последующем, когда развитие и распространение киберугроз повлекло существенную коррекцию ранее намеченной стратегии развития кибербезопасности Республики. Был организован так называемый командный центр киберзащиты, статус которого был расширен до департамента командования киберзащиты вооруженных сил Турции.

В 2016 году была сформирована дополнительная организационная структура под названием “Центр электронной войны”, которая специализируется на предотвращении и реагировании на киберугрозы, ведении боевых действий в киберпространстве.

Таким образом, изначально кибербезопасность государства выстраивалась в направлении защиты военного и оборонного потенциала. Однако, начиная с 2017 года в Генеральном штабе вооруженных сил Республики начал также функционировать центр кибероборонысо

структурным подразделением по мониторингу киберугроз, ориентированный на противодействие внутренним киберугрозам, борьбе с терроризмом и экстремизмом в киберпространстве.

Неообходимо отметить, что Турецкая Республика больше других стран применила при построении системы кибербезопасности опыт развитых государств в данном направлении с участием специалистов военного ведомства и гражданских экспертов.

Четыре года назад министр транспорта и связи Турции объявил о планах создания спецподразделения для защиты киберпростаранства от несанкционированного вмешательства и кибератак, и уже в 2020 году так называемые турецкая киберармия, белые хакеры стали активно использоваться в этом направлении.[1]

При этом правительством Республики первостепенное внимание уделяется развитию и совершенствованию социального статуса и имиджа подразделений, участвующих в обеспечении кибербезопасности.

Этому посвящена Национальная стратегия в сфере кибербезопасности, в которой сформулированы основные задачи противодействия киберугрозам в киберпространстве, направления развития киберподразделений Республики, подразумевающее в частности гибкое активное реагирование на возникающие киберинциденты, с возможным навязыванием противнику собственной тактики кибервоздействия.

Данная стратегия строится на реализации специальной нормативно-правовой базы, основу которой составляет издаваемый Советом национальной безопасности Турции специальный документ, регламентирующий осуществление политики национальной безопасности. В нем, в частности, перечисляются основные внутренние и внешние угрозы государства, определяется место и значение кибербезопасности, которая в числе других элементов, отнесена к пятой составляющей национальной безопасности (наряду с сухопутными, морскими, воздушными и космическими войсками).

Также указанный документ нацеливает систему кибербезопасности на противодействие враждебной пропаганде, кибертерроризму, защиту государства и граждан, ключевых инфраструктур, государственных учреждений, промышленных объектов от киберинцидентов различной степени сложности.[2]

Возникающие частные вопросы, связанные с регулированием киберпространства и противодействию киберугрозам, регулируются с помощью регулируются специальными указами органов государственной власти, ведомственными нормативными правовыми актами, в числе которых особо выделяется Положение «О мерах по информационной и коммуникационной безопасности Турецкой Республики». [3]

Также значительное место в системе кибербезопасности государство занимает деятельность Совета по кибербезопасности и Центра кибероборонь Туркцкой Республики.

Государственные органы Турции на протяжении последних двух лет выражают растущую озабоченность количеством и характером криминальных атак на экономические объекты государства, материальным ущербом, причиняемым киберпреступлениями прежде всего в банковской сфере.

В связи с чем прогнозируемой рекцией со стороны государства стало отражение основ кибербезопасности в Стратегтческом плане развития Турецкой Республики на 2019-02023 годы. Использование киберподразделений для защиты экономики страны, предотвращения повторения крупнейшей в истории государства кибератаки на банковскую сферу, осуществленной криминальным киберсообществом в 2015 году.

По официальным данным (существенно заниженным по мнениям экспертов) подразделения кибербезопасности вооруженных сил Турецкой Республики состоят из 13 тыс. военных специалистов и гражданских экспертов, а также бывших хакеров, называемых “белыми”, добровольно перешедшими на работу в соответствующие государственные структуры. Подразделения кибербезопасности объеденены в соответствующую

структуру, состоящую из пяти основных департаментов: правоохранительного, военного, морского, космического и комплексной обороны. Перечисленные дапертаменты взаимодействуют с профильными министерствами и ведомствами в вопросах предупреждения и реагирования на возникающие гиберугрозы, разрешения киберситуаций различной степени сложности.

Правоохранительный департамент координирует деятельность по вопросам кибербезопасности директората национальной полиции Турецкой Республики и генерального командования жандармерии по выявлению и пресечению фактов кибератак на гражданские объекты, банки, страховые компание, другие финансовые организации, а также на профилактики мошенничества и созданию антиправительственных группировок в киберпространстве.

Военный департамент осуществляет кибербезопасность в интересах в первую очередь армейской разведки. Наиболее известная киберакция данного подразделения это преодоление системы безопасности комплексов противовоздушной обороны “Patriot”, расположенных на границе с Сирийской Республикой в 2018 году. Выявленные киберподразделениями технические и программные недостатки комплексов послужили дополнительным аргументом в пользу закупки российских систем ПВО С-400.[4]

Морской департамент специализируется на кибербезопасности судов и инфраструктуры военного и гражданского флота, объектов береговой охраны. Нибольшую актульность даннрое направление организации кибербезопасности приобрело при осуществлении геологической разведки шельфа Средиземного моря в прошлом году.

Космический департамент обеспечивает кибербезопасность космических объектов, в первую очередь телекоммуникационных спутников, а также осуществляет на постоянной основе мониторинг земной поверхности.

Департамент комплексной обороны осуществляет контрразведывательные мероприятия по обнаружению уязвимых мест в системе национальной кибербезопасности, разработки и реализации превентивных мер защиты.

Отличительной чертой организации системы кибербезопасности Турецкой модели является активное использование в этом процессе так называемых дружественных группировок-крупных хакерских киберсообществ, действующих автономно от государственных киберподразделений, “белых хакеров”, выполняющих отвлекающие маневры в киберпространстве, осуществляющих крупные демонстративные символические киберакции.

Также часто используются хакеры-одиночки, состоящие на связи с Национальной разведывательной организацией, привлекаемые для проведения разовых киберакций, создания и продвижения хакерских ячеек в зарубежных странах.

Таким образом, проведенный сравнительный и контент анализ литературы и информационных источников по теме показал, что Турецкой Ркспублике в последние годы удалось создать масштабную, системную и устойчивую структуру кибербезопасности, организационно отличную от других развитых зарубежных стран, использованием возможностей активно привлекаемых хакерских киберсообществ, а также хакеров-одиночек, принимающих участие в обеспечение национальной кибербезопасности Республики.

Также государственными структурами разработана и используется эффективная, достаточно простая и мобильная система нормативно-правового регулирования кибербезопасности государства.

Литература

1. www.news.day.az [сайт]. – URL: https://www.news.day.az/world/897937.html (дата обращения: 01.04.2021)

2. www.mgk.gov.tr [сайт]. – URL: https://www mgk.gov.tr. (дата обращения: 02.04.2021); www.cumhuriyet.com.tr [сайт]. – URL: https://www. www.cumhuriyet.com.tr/yazarlar/mehmet-ali-guller/guvenlik-stratejisi-nasil-olusturulmali-1754956 (дата обращения: 02.04.2021)

3. Ссылка: www.aa.com.tr/ru [сайт]. – URL: https:/ www.aa.com.tr/ru/1530730 (дата обращения: 03.04.2021)

4. Ссылка: www.securitylab.ru [сайт]. – URL: https:/ www.securitylab.ru/blog/personal/Business_without_danger/146799.php (дата обращения: 03.04.2021)

Literature

1. Link: www.news.day.az [site]. - URL: https://www.news.day.az/world/897937.html (accessed: 01.04.2021)

2. Link: www.mgk.gov.tr [site]. - URL: https://www mgk.gov.tr. (accessed: 02.04.2021); www.cumhuriyet.com.tr [site]. - URL: https://www. www.cumhuriyet.com.tr/yazarlar/mehmet-ali-guller/guvenlik-stratejisi-nasil-olusturulmali-1754956 (accessed: 02.04.2021)

3. Link: www.aa.com.tr/ru [site]. – URL: https:/ www.aa.com.tr/ru/1530730 (accessed: 03.04.2021)

4. Link: www.securitylab.ru [site]. - URL: https:/ www.securitylab.ru/blog/personal/Business_without_danger/146799.php (accessed: 03.04.2021)