УДК 340.1:342.7
DOI: 10.36979/1694-500X-2022-22-7-64-69

КЛАССИФИКАЦИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

М.У. Алияскарова

Аннотация. Исследованы различные варианты классификации угроз информационной безопасности личности, основанные как на научных исследованиях, так и на нормах отраслевого законодательства Кыргызской Республики. Автор уделяет особенное внимание изучению особенностей классификационного подхода, сформированного в научных источниках, при котором угрозы информационной безопасности личности разделяются на внешние и внутренние. И приходит к выводу, что в большинстве научных источников отсутствуют четкие классификационные критерии отнесения той или иной угрозы информационной безопасности личности к внутренней или внешней угрозе. По мнению автора, выделение внешних и внутренних угроз информационной безопасности личности следует производить по характеру расположения источника угрозы относительно самого объекта. При этом автор отмечает определенную сложность определения таких угроз в зависимости от использования VPN-технологий, которые затрудняют определение места нахождения источника угроз.

Ключевые слова: информационная безопасность; личность; безопасность государства; угроза информационной безопасности; внешние угрозы; внутренние угрозы; классификация; критерии классификации.

ЖЕКЕ АДАМДЫН МААЛЫМАТТЫК КООПСУЗДУГУНА КЕЛТИРИЛГЕН КОРКУНУЧТАРДЫН КЛАССИФИКАЦИЯСЫ

М.У. Алияскарова

Аннотация. Макалада илимий изилдөөлөрдүн негизинде, ошондой эле Кыргыз Республикасынын тармактык мыйзамдарынын ченемдеринин негизинде жеке адамдын маалыматтык коопсуздугуна келтирилген коркунучтарды классификациялоонун ар кандай варианттары изилденген. Автор илимий булактарда калыптанган классификациялык мамиленин өзгөчөлүктөрүн изилдөөгө өзгөчө көңүл бурат, мында жеке адамдын маалыматтык коопсуздугуна коркунучтар тышкы жана ички болуп бөлүнөт. Автордун пикирири боюнча, адамдын маалыматтык коопсуздугуна тышкы жана ички коркунучтарды бөлүштүрүү объекттин өзүнө карата коркунуч булагынын жайгашкан жеринин мүнөзүнө жараша жүргүзүлүүгө тийиш. Ошол эле учурда автор VPN технологияларын колдонууга жараша мындай коркунучтарды аныктоодо белгилүү бир кыйынчылыкты белгилейт, бул коркунучтардын булагын аныктоону кыйындатат.

Түйүндүү сөздөр: маалыматтык коопсуздук; жеке адам; мамлекеттик коопсуздук; маалыматтык коопсуздук коркунучу; тышкы коркунучтар; ички коркунучтар; классификациялоо; классификациялоонун критерийлери.

CLASSIFICATION OF THREATS TO PERSONAL INFORMATION SECURITY

M.U. Aliiaskarova

Abstract. The article explores various options for the classification of threats to the information security of an individual, based both on scientific research and on the norms of the sectoral legislation of the Kyrgyz Republic. The author pays special attention to the study of the features of the classification approach, formed in scientific sources, in which threats to the information security of an individual are divided into external and external threat. And comes to the conclusion, that in most scientific sources there are no clear classification criteria for attributing a particular threat to personal information security to an internal or external threat. According to the author, the identification of external and internal threats to personal information security should be made by the nature of the location of the threat source relative to the object itself. At the same time, the author notes a certain difficulty in determining such threats, depending on the use of VPN - technologies, which make it difficult to determine the location of the source of threats.

Keywords: information security; personality; state security; information security threat; external threats; internal threats; classification; classification criteria.

В современный период развития мироустройства важное значение придается информационной безопасности личности. В процессе ведения информационной геополитической войны именно человек становится главной мишенью. Поэтому для обеспечения информационной безопасности личности необходимо доскональное изучение вызовов и угроз информационной безопасности личности. Отечественный исследователь Х.М. Якубова дает следующее определение угрозы безопасности: «Угроза безопасности – совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государств» [1, с. 104]. Такое определение вполне относимо и к понятию информационной безопасности личности.

В настоящее время сформировано множество разнообразных подходов к выделению классификационных критериев вызовов и угроз информационной безопасности личности.

Так, по мнению Н.А. Северцева и А.В. Бецкова, среди угроз информационной безопасности выделяются внешние и внутренние угрозы [2]. При этом исследователи к источникам внешних угроз относят следующие: «деятельность иностранных политических, экономических, религиозных, военных, разведывательных структурных образований; деятельность международных террористических и преступных групп; подготовка и проведение недружественной политики, связанные с созданием средств воздействия на информационную структуру и информационные ресурсы; активизация духовно-культурных и идеологических экспансий, усиление зависимости молодого поколения от внешних информационных воздействий» [2]. К числу основных внутренних угроз, по мнению Н.А. Северцева и А.В. Бецкова, относятся: «олигархизация общества, разделяющая людей на супер богатых и бедных с предсказуемыми последствиями; рост организованной преступности и ее политизация; криминализация общества; снижение уровня образования, патриотического воспитания, рост социального невежества; недостаточная информация в сфере государственного управления; резкое снижение уровня фундаментальных прикладных научных исследований в различных сферах научной деятельности, издание непрофессионального подхода объединений, присоединений, разъединений, расформирование и тому подобное научных и образовательных структур (НИИ и вузов), различных по профессиональному содержанию. <…> Также к внутренним угрозам относятся компьютерные преступления различной направленности, отток молодых ученых (математиков и физиков) за границу в поисках уважительного отношения к своей профессиональной работе; отсутствие основ гражданского общества и правового государства; антинародная деятельность средств массовой информации, в частности телевидения – по оболваниванию населения путем непрерывного демонстрирование насилия, убийств, разврата, возвеличивание административных чиновников различного уровня, всякого рода шоуменов, никчемных артистов и тому подобное, в то же время отсутствует информации о современных ученых, педагогах, врачах, прославивших страну своим интеллектуальным трудом» [2].

Придерживается позиции о разделении угроз информационной безопасности на внутренние и внешние и Д.А. Тершуков [3]. Однако в исследовании данного автора четкие классификационные критерии относимости угроз информационной безопасности к той или иной группе не обозначены.

Внешние и внутренние угрозы информационной безопасности личности называет также Л.К. Бостанова. Как отмечает Л.К. Бостанова, «обеспечение информационной безопасности, под которой понимается состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз, представляется весьма важной задачей» [4]. При этом конкретный перечень внешних и внутренних угроз исследователем не приводится.

Перечень внешних и внутренних угроз информационной безопасности государства в целом закреплен в пунктах 31, 32 Концепции информационной безопасности Кыргызской Республики на 2019–2023 годы, утвержденной постановлением Правительства Кыргызской Республики от 3 мая 2019 года № 209 [5] (далее по тексту – Концепция информационной безопасности КР). Так, в соответствии с данным

нормативно-правовым актом, к внешним угрозам информационной безопасности относятся:

«1) рост транснациональной преступности в сфере компьютерных технологий и информации, нарушающей сохранность информационных ресурсов и штатное функционирование государственных информационных систем;

2) увеличение технологического отрыва других государств, усиливающее зависимость Кыргызской Республики от использования зарубежной техники и программного обеспечения для защиты критических информационных инфраструктур;

3) разработка рядом стран программ по ведению информационного воздействия и пропаганды, в целях достижения преимущества в информационной сфере;

4) деятельность международных экстремистских, террористических и других преступных сообществ, организаций и групп в информационной сфере Кыргызской Республики;

5) распространение в информационном пространстве противоправного контента, а также иной идеологии, нарушающих нравственные устои общества;

6) обострение международной конкуренции за обладание стратегически важной информацией, стремление ряда стран к доминированию в информационном пространстве Кыргызской Республики и получению доступа к информации с ограниченным доступом;

7) введение некоторыми государствами на своих информационных рынках всевозможных ограничений, ущемляющих интересы Кыргызской Республики» [5].

В числе внутренних угроз информационной безопасности в п. 32 Концепции информационной безопасности КР названы:

«1) эксплуатация устаревших технических устройств и оборудования, приобретение импортных технических и программно-аппаратных средств, а также средств защиты информации при создании и развитии информационной инфраструктуры Кыргызской Республики;

2) отставание Кыргызской Республики от многих стран мира по уровню информатизации деятельности органов государственной власти, местного самоуправления и хозяйствующих субъектов;

3) слабая координация деятельности органов власти и управления Кыргызской Республики по укреплению информационной безопасности и недостаточность финансового обеспечения мероприятий, нацеленных на защиту информационной сферы Кыргызской Республики;

4) несовершенство нормативной правовой базы, регулирующей межведомственные отношения и систему контроля в информационной сфере Кыргызской Республики, а также недостаточная правоприменительная практика в данной области;

5) несовершенство законодательства по своевременному ограничению доступа к материалам деструктивного характера в сети Интернет, а также отсутствие законодательной базы по вопросам регулирования взаимоотношений в сети Интернет, несовершенство правоприменительной практики в отношении распространения противоправной информации;

6) функционирование на приграничных территориях Кыргызской Республики теле- и радиоканалов сопредельных государств;

7) отсутствие государственной системы анализа и мониторинга информационного пространства Кыргызской Республики» [5]. При этом несмотря на то, что данные внешние и внутренние угрозы информационной безопасности выделяются в общегосударственном масштабе, считаем, что они имеют объектом своего негативного воздействия в числе прочего также и личность отдельного гражданина. Ведь личность, общество и государство в своем фундаментальном значении выступают структурными составляющими друг друга в приведенном иерархическом порядке.

Таким образом, множество исследователей в научных источниках, а также в нормах национального законодательства Кыргызской Республики в числе угроз информационной безопасности личности выделяют внешние и внутренние угрозы. Однако, по нашему мнению, при разделении угроз информационной безопасности личности на внешние и внутренние, изложенном в вышеприведенной классификации, нарушается главный принцип классификации – выделение

основных классификационных критериев. Если предположить, что в качестве такого критерия используются иностранный и внутригосударственный источник формирования угроз информационной безопасности, то большинство из вышеназванных внутренних угроз находятся в прямой корреляции от внешних угроз информационной безопасности. Они фактически неотделимы друг от друга. Также в условиях повсеместного распространения и использования сети Интернет, моментального распространения информации в сети, в том числе и информации пропагандистского характера (законной и незаконной), вредоносных компьютерных программ и т. д., осуществляемой в том числе с использованием VPN-технологий, значительно усложняет определение внешней или внутригосударственной принадлежности источника распространения информации, а следовательно, и отнесение такой вредоносной информации к внутренним или внешним угрозам информационной безопасности.

Поэтому подход к классификации вызовов и угроз информационной безопасности личности, при котором угрозы информационной безопасности подразделяются на внешние и внутренние, хотя и следует признать заслуживающим внимания, но четких классификационных критериев, по нашему мнению, в нем не использовано. Следовательно, разделение угроз информационной безопасности личности на внешние и внутренние носит больше условный характер, так как такие угрозы взаимообусловлены и взаимосвязаны.

В п. 33 Концепции информационной безопасности КР приводится классификация угроз информационной безопасности на основе такого критерия, как общая направленность. Так, в числе угроз информационной безопасности выделяются:

«1) угрозы правам и свободам личности в области информационной деятельности и духовной жизни, индивидуальному, групповому и общественному сознанию, обусловленные:

- сдерживанием процессов развития информационной сферы Кыргызской Республики;

- несоблюдением законных ограничений на создание и распространение в Кыргызской Республике информации, разжигающей расовую, этническую, национальную, религиозную и межрегиональную рознь, а также разрушающей нравственные устои общества;

- широкой пропагандой образцов так называемой массовой культуры, противоречащей исторически сложившимся менталитету и традициям народа Кыргызской Республики и ведущих к постепенному разрушению норм морали в обществе;

- противоправным применением специальных средств воздействия на индивидуальное, групповое и общественное сознание и, как следствие, усиление зависимости духовной, экономической и политической сфер в общественной жизни Кыргызской Республики от навязываемой извне информации;

- угроза подмены государственной идеологии и мировоззрения посредством навязывания идей через средства массовой коммуникации;

- угроза мобилизации граждан для участия в незаконных акциях, вербовки посредством материалов радикального характера;

2) угрозы информационной поддержке и информационному обеспечению внутренней и внешней политики, реализуемой руководством Кыргызской Республики, обусловленные:

- недостаточным вниманием со стороны государственных органов вопросам своевременной разработки проектов нормативных правовых актов;

- деятельностью в информационном пространстве Кыргызской Республики (включая сеть Интернет) информационных агентств, средств массовой информации и иных информационных структур, искажающих информацию о внутренней и внешней политике Кыргызской Республики;

- недостаточной эффективностью деятельности национальных информационных агентств и средств массовой информации по противодействию негативному информационному воздействию на население Кыргызской Республики;

- недостаточным финансово-техническим обеспечением государственных органов, уполномоченных вести работу в области информационной безопасности и информационной политики;

3) угрозы безопасности информационных и телекоммуникационных средств и систем, как

уже развернутых, так и создаваемых на территории Кыргызской Республики, такие как:

- противоправные сбор и использование информации, нарушения технологии обработки информации;

- несанкционированный доступ к информации, находящейся в банках и базах данных;

- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;

- уничтожение, повреждение, радиоэлектронное подавление, разрушение или хищение средств и систем обработки информации, телекоммуникации и связи, машинных и других носителей информации;

- воздействие или компрометация на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации, средств криптографической защиты информации;

- утечка информации по техническим каналам;

- внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;

- использование несертифицированных зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи;

- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;

- нарушение законных ограничений на распространение информации;

- увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности» [5].

Безусловно, каждая из названных в Концепции информационной безопасности КР угроз в определенной мере влечет те или иные негативные последствия для обеспечения интересов защищенности личности от вредного воздействия. Однако наиболее логически обоснованный подход к выделению классификационных критериев угроз информационной безопасности личности разработан А.А. Чеботаревой. В своем диссертационном исследовании А.А. Чеботарева предлагает в качестве критериев классификации угроз информационной безопасности личности использовать такие, как «цель, источник угрозы, характер воздействия» [6, с. 15].

При этом в числе целей, преследуемых источником той или иной угрозы, А.А. Чеботарева выделяет «воздействие на сознание личности, на ее психологическое состояние, овладение личной информацией, распространение идеологии терроризма, радикальных идей в сети Интернет, финансовое мошенничество» [6, с. 15]; в числе источников угрозы: «сам пользователь, националистические, религиозные, этнические и иные организации и структуры, использующие информационно-телекоммуникационные технологии для террористической деятельности, преступники, распространяющие в глобальном информационном пространстве различные формы сексуального насилия, и др.» [6, с. 15]; по характеру расположения источника угрозы относительно самого объекта (внутренние или внешние), а также по характеру воздействия «непреднамеренные, случайные, либо умышленные, целенаправленно создающие опасность, причиняющие вред, ведущие к неблагоприятным последствиям для личности» [6, с. 15].

Заключение. Учитывая изложенное, предлагаем собственный вариант классификации угроз информационной безопасности личности, основанный на следующих критериях:

1) по направленности на объект посягательства угрозы информационной безопасности личности следует разделять на: угрозы нравственно-интеллектуальной сфере личности, угрозы информации персонального характера и личной информации, угрозы сфере электронных финансов и ценных бумаг;
2) по источникам вредоносного посягательства следует выделять: физических лиц, иностранных агентов, экстремистские и террористические организации и др;

3) по характеру расположения источника угрозы относительно самого объекта: внутренние или внешние.

Поступила: 01.03.2022;
рецензирована: 16.03.2022; принята: 18.03.2022.

Литература

1. *Якубова Х.М.* Правовые основы информационной безопасности в Кыргызской Республике / Х.М. Якубова // Вестник КРСУ. 2011. Т. 11. № 10.
2. *Северцев Н.А.* Информационная безопасность и принципы ее обеспечения / Н.А. Северцев, А.В. Бецков // Труды Международного симпозиума «Надежность и качество». 2018. № 1. URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-i-printsipy-ee-obespecheniya (дата обращения: 28.12.2021).
3. *Тершуков Д.А.* Анализ современных угроз информационной безопасности / Д.А. Тершуков // NBI-technologies. 2018. № 3. URL: https://cyberleninka.ru/article/n/analiz-sovremennyh-ugroz-informatsionnoy-bezopasnosti (дата обращения: 28.12.2021).
4. *Бостанова Л.К.* Виды и особенности угроз информационной безопасности / Л.К. Бостанова // Международный научно-исследовательский журнал. 2012. № 6(6). URL: https://research-journal.org/technical/vidy-i-osobennosti-ugroz-informacionnoj-bezopasnosti/ (дата обращения: 28.12.2021).
5. Концепция информационной безопасности Кыргызской Республики на 2019–2023 годы, утверждена постановлением Правительства Кыргызской Республики от 3 мая 2019 года № 209. URL: http://cbd.minjust.gov.kg/act/view/ru-ru/13652?cl=ru-ru (дата обращения: 28.12.2021).
6. *Чеботарева А.А.* Правовое обеспечение информационной безопасности личности в глобальном информационном обществе: автореф. дис. … д-ра юрид. наук: 12.00.13 / А.А. Чеботарева. М., 2017.