УДК : 340

ЗАКОНОДАТЕЛЬНОЕ РАЗГРАНИЧЕНИЕ ПОНЯТИЙ «КИБЕРБЕЗОПАСНОСТЬ» И «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Кулжабаева Жанат Орынбековна
Кандидат юридических наук, доцент, Ученый секретарь Института законодательства и правовой информации РК; г. Астана, Республика Казахстан; e-mail: kulzhabai@mail.ru

Аннотация. *В современных условиях развития общества система информационного взаимодействия активно использует различные технические средства, телекоммуникационные системы. Уровень распространения, получения, использования необходимых знаний и информации затрагивает различные сферы общественной жизни. При этом, рост объемов информации настолько велик, что для продуктивного его использования необходимо внедрять компьютеры, современные элементы информационно-коммуникационной инфраструктуры, включая глобальную сеть Интернет. Нарастающий масштаб использования современных информационных технологий, широко используемых во всех сферах государственной и общественной деятельности определяет особую актуальность задачи постоянного совершенствования системы защиты общих информационных ресурсов. При этом очевидными стали факторы, повышающие необходимость законодательного разграничения понятий «кибербезопасность» и «информационная безопасность». В данной статье обозначены авторские позиции по дефинициям «информационная безопасность», «информационная безопасность в сфере информатизации», «кибербезопасность»; анализ действующих редакций правовых норм об информационной безопасности и кибербезопасности; зарубежная практика обеспечения безопасности информации/данных. Значимость защиты информации обусловлена обменом электронных документов и оказания электронных услуг. Проблема обеспечения информационной безопасности, кибербезопасности имеет комплексный характер и связана с необходимостью сочетания законодательных, организационных мер, дальнейшим объединением научно-технического и экономического потенциала заинтересованных субъектов права, использованием имеющихся и разработкой новых наиболее эффективных подходов, способов и средств защиты информации. Принимая во внимание положения действующего законодательства, передовую зарубежную практику, мнение экспертного сообщества Казахстана, рекомендуется разграничить на законодательном уровне понятия «информационная безопасность» и «обеспечение кибербезопасности» применительно для сферы информатизации. Кроме того, целях введения в законодательство РК и единообразного толкования понятийно-категориального аппарата в обеспечении кибербезопасности предлагается ввести такие дефиниции как угроза кибербезопасности, инцидент кибербезопасности. Предлагается расширить обязанности владельца критически важных объектов инфраструктуры.*

Ключевые слова: *информация, национальная безопасность, информационная безопасность, кибербезопасность, киберзащита, информационно-коммуникационные технологии.*

КИБЕРҚАУІПСІЗДІК» ЖӘНЕ «АҚПАРАТТЫҚ ҚАУІПСІЗДІК» ҰҒЫМДАРЫНЫҢ ЗАҢНАМАЛЫҚ АЙЫРМАШЫЛЫҒЫ

Жанат Орынбекқызы Құлжабаева
Заң ғылымдарының кандидаты, доцент, ҚР заңнама және құқықтық ақпарат институтының Ғылыми хатшысы; Астана қ., Қазақстан Республикасы; e-mail: kulzhabai@mail.ru

Аннотация. *Қоғамның қазіргі даму жағдайында ақпараттық өзара әрекеттесу жүйесі әртүрлі техникалық құралдарды, телекоммуникациялық жүйелерді белсенді қолданады. Қажетті білім мен ақпаратты тарату, алу, пайдалану деңгейі қоғамдық өмірдің әртүрлі салаларына әсер етеді. Сонымен қатар ақпарат көлемінің өсуі соншалық, оны тиімді пайдалану үшін компьютерлерді, ғаламдық Интернет желісін қоса алғанда, ақпа-*

раттық-коммуникациялық инфрақұрылымның заманауи элементтерін енгізу қажет. Мемлекеттік және қоғамдық қызметтің барлық салаларында кеңінен қолданылатын заманауи ақпараттық технологияларды қолданудың өсіп келе жатқан ауқымы жалпы ақпараттық ресурстарды қорғау жүйесін үнемі жетілдіру міндетінің ерекше өзектілігін анықтайды. Сонымен қатар «киберқауіпсіздік» және «ақпараттық қауіпсіздік» ұғымдарын заңнамалық саралау қажеттілігін арттыратын факторлар айқын болды. Бұл мақалада «ақпараттық қауіпсіздік», «ақпараттандыру саласындағы ақпараттық қауіпсіздік», «киберқауіпсіздік» дефиницялары бойынша авторлық позициялар; ақпараттық қауіпсіздік және киберқауіпсіздік туралы құқықтық нормалардың қолданыстағы редакцияларын талдау; ақпарат/деректер қауіпсіздігін қамтамасыз етудің шетелдік тәжірибесі көрсетілген. Ақпаратты қорғаудың маңыздылығы электрондық құжаттар алмасуға және электрондық қызметтер көрсетуге байланысты. Ақпараттық қауіпсіздікті, киберқауіпсіздікті қамтамасыз ету проблемасы кешенді сипатқа ие және заңнамалық, ұйымдастырушылық шараларды үйлестіру, мүдделі құқық субъектілерінің ғылыми-техникалық және экономикалық әлеуетін одан әрі біріктіру, қолда бар және жаңа неғұрлым тиімді тәсілдерді, тәсілдер мен ақпаратты қорғау құралдарын әзірлеу қажеттілігімен байланысты. Қолданыстағы заңнаманың ережелерін, озық шетелдік тәжірибені, Қазақстанның сараптамалық қоғамдастығының пікірін назарға ала отырып, ақпараттандыру саласына қатысты «ақпараттық қауіпсіздік» және «киберқауіпсіздікті қамтамасыз ету» ұғымдарын заңнамалық деңгейде ажырату ұсынылады. Бұдан басқа, ҚР заңнамасына енгізу және киберқауіпсіздікті қамтамасыз етуде тұжырымдамалық-категориялық аппаратты бірқелкі түсіндіру мақсатында киберқауіпсіздік қатері, киберқауіпсіздік оқиғасы сияқты дефинициялар енгізу ұсынылады. Инфрақұрылымның маңызды объектілері иесінің міндеттерін кеңейту ұсынылады.

Түйінді сөздер: *ақпарат, ұлттық қауіпсіздік, ақпараттық қауіпсіздік, киберқауіпсіздік, киберқорғаныс, ақпараттық-коммуникациялық технологиялар.*

LEGISLATIVE DISTINCTION BETWEEN THE CONCEPTS OF «CYBERSECURITY» AND «INFORMATION SECURITY»

Kulzhabayeva Zhanat Orynbekovna
Candidate of Legal Sciences, Associate Professor, Academic Secretary of the Institute of Legislation and Legal Information of the Republic of Kazakhstan; Astana c., Republic of Kazakhstan; e-mail: kulzhabai@mail.ru

Abstract. *In modern conditions of development of society, the system of information interaction actively uses various technical means, telecommunication systems. The level of distribution, receipt, use of necessary knowledge and information affects various spheres of public life. At the same time, the growth of information volumes is so great that for its productive use it is necessary to introduce computers, modern elements of information and communication infrastructure, including the global Internet. The growing scale of use of modern information technologies, widely used in all spheres of state and public activity determines the special relevance of the task of constant improvement of the system of protection of common information resources. At the same time, the factors increasing the need for legislative differentiation between the concepts of "cybersecurity" and "information security" have become obvious. This article outlines the author's positions on the definitions of "information security", "information security in the field of informatization", "cybersecurity"; an analysis of the current versions of legal norms on information security and cybersecurity; foreign practice of ensuring the security of information / data. The importance of information protection is due to the exchange of electronic documents and the provision of electronic services. The problem of ensuring information security, cybersecurity is complex and is associated with the need to combine legislative, organizational measures, further unification of the scientific, technical and economic potential of interested legal entities, the use of existing and the development of new, most effective approaches, methods and means of information protection. Taking into account the provisions of the current legislation, advanced foreign practice, the opinion of the expert community of Kazakhstan, it is recommended to distinguish at the legislative level the concepts of "information security" and "ensuring cybersecurity" as*

applied to the field of informatization. In addition, in order to introduce into the legislation of the Republic of Kazakhstan and a uniform interpretation of the conceptual and categorical apparatus in ensuring cybersecurity, it is proposed to introduce such definitions as a threat to cybersecurity, a cybersecurity incident. It is proposed to expand the responsibilities of the owner of critical infrastructure facilities.

Keywords: *information, national security, information security, cybersecurity, cyber defense, information and communication technologies.*

Информация о финансировании

Данное исследование осуществлено при финансовой поддержке Комитета по науке Министерства науки и высшего образования Республики Казахстан (ИРН BR24993082 «Комплексное изучение гуманитарных аспектов информационной безопасности Казахстана и компонентов «мягкой силы» в обеспечении устойчивого развития и консолидации казахстанского общества»).

DOI: 10.52026/2788-5291_2024_79_4_178

Введение

Трендом современного общественного развития является использование высоко информационных технологий, телекоммуникационных систем и соответствующих технических средств. Все это должно сопровождаться совершенствованием правового регулирования общественных отношений в сфере внедрения инновационных информационно-коммуникационных технологий.

Процесс усовершенствования информационного законодательства обеспечивает и гарантирует соблюдение конституционных прав и свобод человека, способствует формированию соответствующей концепции информационной безопасности *(далее - ИБ).* При этом, при реализации конституционных прав обеспечения каждому гражданину возможности ознакомиться с затрагивающими его права и интересы документами, решениями и источниками информации (п.3 статьи 18 Конституции РК), право каждого гражданина свободно получать и распространять информацию любым, не запрещенным законом способом (п.2 статьи 20 Конституции РК) формируется соответствующее информационное пространство, расширяются сферы международного сотрудничества в сфере.

В содержании и развитии информационной составляющей любого государства заметен возрастающий объем информации любого вида, используемый и широко распространенный в различных областях политики, экономики. При этом приоритетными становятся использование информационных и компьютерных технологий. Их интенсивное развитие, объемная распространенность во всех областях государственной и общественной деятельности повышает особую значимость тенденций укрепления и совершенствования системы защиты общих информационных ресурсов всех государств.

Материалы и методы

В Стратегии сотрудничества государств – участников СНГ в построении и развитии информационного общества на период до 2025 года и Плане действий по ее реализации, утвержденной Решением Совета глав правительств СНГ от 28 октября 2016 года[1] были обозначены принципы, которым должна соответствовать ИБ. Смысл обозначенных девяти принципов, в конечном итоге, сводится к конфиденциальности, целостности, доступности информации. С 2016 года государства – участники СНГ гармонизируют законодательство и нормативно-техническую базу в области информационно-коммуникационных технологий *(далее-ИКТ).*

Как известно, государства – участники СНГ разработали и внедрили современные приложения ИКТ, такие как электронное правительство; электронная торговля; электронная наука; электронное здравоохранение; электронное обучение; электронная культура; электронная занятость; электронное сельское хозяйство; электронная охрана окружающей среды; электронный регион; электронный нотариат; применение информационных и биометрических технологий в системах паспортно-визовых и иных идентификационных документов нового поколе-

[1] *Стратегия сотрудничества государств – участников СНГ в построении и развитии информационного общества на период до 2025 года и Плане действий по ее реализации, утвержденная Решением Совета глав правительств СНГ от 28 октября 2016 года // Единый реестр правовых актов и других документов Содружества Независимых Государств. https://cis.minsk.by/reestrv2/doc/5490#text (Дата обращения: 15.06.2024 года)*

ния. Все это способствует необходимости совершенствования механизма защиты любого рода информации, учета большого объема информационных ресурсов. Кроме того, каждое государство, каждый государственный орган заинтересован в создании технологических информационных ресурсов, их дальнейшего эффективного, совместного использования. Учитывая требования действующего законодательства, лучшую зарубежную практику необходимо сформировать эффективную, неуязвимую правовую политику защиты интересов личности и государства в информационной сфере.

В Республике Казахстан утверждена Информационная доктрина[2] и План действий[3] по её реализации. Данные акты являются стратегическими документами нашего государства для формирования государственной политики в информационно-коммуникационной сфере. В доктрине указано, что обеспечение информационной безопасности страны и ее граждан, своевременное реагирование на информационные вызовы и риски являются «ключевым направлением» реализации доктрины. Представляется необходимым отметить, что рассматриваемом документе, определяющим систему воззрений, совокупность политических принципов, видения и подходов к развитию по вопросам информации, кроме устоявшихся словосочетаний «информационная безопасность», «информационная сфера», «информационная политика», информационное пространство» появились неологизмы, такие как «информационная экосистема», «информационный контент», «информационный тренд», «информационный хаб», «информационный суверенитет».

Результаты

В настоящее время в научном сообществе и среди практикующих специалистов выделяется проблема отсутствия законодательного разграничения понятий «кибербезопасность» и «информационная безопасность» в Казахстане.

Например, Л.Ф. Татаринова отмечает, что «проводя соотношение исследуемых терминов в законодательстве Республики Казахстан, мы можем ориентироваться только на имеющиеся в законодательстве Казахстана термины «информационная безопасность» и «защита информации», и отсутствующие в том же законодательстве, но имеющиеся в специальной литературе термины «кибербезопасность» и «киберзащита»» [1, с.61]. В диссертационной работе Исабаевой С.Б. обосновывается тезис о том, что в концепции кибербезопасности Казахстана дано определение термину «кибербезопасность» и Законе РК «Об информатизации» понятию «Информационная безопасность в сфере информатизации». Однако, по мнению соискателя, представленные формулировки нетривиальны и существенно разнятся [2, с.9].

Наличие большого количество публикаций по соотношению рассматриваемых правовых категорий, по-прежнему, остается дискуссионным. «Между этими терминами не существует четкой границы, что приводит к размыванию исследуемой области и возникновению различных сложностей среди коммуницирующих сторон. В связи с этим имеет смысл уточнить содержание терминов кибербезопасность и информационная безопасность, информационные и кибернетические системы, охарактеризовать уровни киберпространства, а также выделить проблемы безопасности на каждом из этих уровней» [3, с.315-316].

Кубышкин А.В., рассматривая международно-правовой аспект обеспечения информационной безопасности, считает необходимым принятие согласованных признаков составов преступлений, связанных с компьютерами и информационными сетями в рамках конвенции об обеспечении информационной безопасности [4, с.6]. Аналогичный подход предлагает Талимончик В.П. в вопросах обеспечения информационной безопасности в вопросах борьбы с правонарушениями в сфере информации [5, с.203].

В целях единообразного толкования указанных правовых дефиниций, представляется целесообразным проанализировать действующее законодательство, где встречаются вышеуказанные понятия.

Как отмечают аналитические издания, главной схожей чертой в понятиях «кибербезопасность» и «информационная безопасность» является применение метода триады

[2] *Указ Президента Республики Казахстан от 20 марта 2023 года № 145 «Об утверждении Информационной доктрины Республики Казахстан»// https://adilet.zan.kz/rus/docs/U2300000145(Дата обращения: 15.06.2024 года)*

[3] *Постановление Правительства Республики Казахстан от 24 августа 2023 года № 723 «Об утверждении Плана действий по реализации информационной доктрины Республики Казахстан (I этап: 2023 – 2025 годы)» https://adilet.zan.kz/rus/docs/U2300000145(Дата обращения: 15.06.2024 года)*

CIA для разработки политик безопасности[4].

1) Конфиденциальность (Confidentiality) – действие по защите данных от просмотра посторонними лицами. Примером защиты конфиденциальности может быть действие по предотвращению кражи паролей или кражи компьютера сотрудника.

2) Целостность (Integrity) – акт поддержания и обеспечения точности и полноты данных на протяжении всего их жизненного цикла. По сути, это означает, что данные не могут и не должны быть изменены посторонними лицами. Нарушение целостности будет включать что-то вроде внедрения вредоносного ПО, скрытого в другой программе.

3) Доступность (Availability) - возможность доступа и использования данных при необходимости.

В соответствии с Законом о национальной безопасности[5] в подпункте 1) статьи 1 используется понятие «информационная инфраструктура» как совокупность технических средств и систем формирования, создания, преобразования, обработки, передачи, использования и хранения информации; в подпункте 2) этой же статьи обозначается понятие «информационное пространство» как сфера деятельности, связанная с формированием, созданием, преобразованием, обработкой, передачей, использованием, хранением информации, оказывающая воздействие в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию. ИБ отнесена к одному из видов национальной безопасности согласно подпункту 5) статьи 4 «Виды национальной безопасности» и определена как состояние защищенности информационного пространства Республики Казахстан, а также прав и интересов человека и гражданина, общества и государства в информационной сфере от реальных и потенциальных угроз, при котором обеспечивается устойчивое развитие и информационная независимость страны.

При этом стремительный рост и увеличение объема ИКТ с одной стороны и существующая ситуация в мире с другой, обозначает необходимость включения кибербезопасности в сферу национальной безопасности. Всеобъемлющий, опасный характер кибер- или компьютерной преступности настолько очевиден в связи с совершенствованием новых технологий.

Также действующее законодательство РК выделяет «ИБ в сфере информатизации» - состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз (ст. 1 Закона об информатизации).[6] Данное определение относится к правовой норме технического характера и связано с защищенностью исключительно инструментария («железа»).

Концепция кибербезопасности[7] *(далее -КБ)* «Киберщит Казахстана» под КБ понимает состояние защищенности информации в электронной форме и среды ее обработки, хранения, передачи (электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры) от внешних и внутренних угроз, то есть ИБ в сфере информатизации. Иными словами, Концепция расширяет понятие «ИБ в сфере информатизации», включая в него элемент касательно защищенности информации в электронной форме.

Таким образом, информационная безопасность - относительно широкое понятие, включающее в себя обеспечение безопасности информации с целью защиты человека, общества и государства. Кибербезопасность подразумевает под собой безопасность информации в электронной форме и инфраструктуры, на которой такая информация содержится.

Обсуждение

Понятие информационная безопасность в Законе об информатизации используется применительно к сфере информатизации и соответствует по своему содержанию понятию кибербезопасности. Государственный контроль распространяется на сферу информатизации (п.п. 52 ст. 138 Предпринимательского кодекса)[8]. В связи с этим, государственный контроль за деятельностью по обеспечению

[4] *Cybersecurity vs. Information Security: Is There A Difference?: https://www.bitsight.com/blog/cybersecurity-vs-information-security (Дата обращения: 15.06.2024 года)*

[5] *Закон Республики Казахстан от 6 января 2012 года № 527-IV «О национальной безопасности Республики Казахстан» // https://adilet.zan.kz/rus/docs/Z1200000527 (Дата обращения: 15.06.2024 года)*

[6] *Закон «Об информатизации» от 24 ноября 2015 года // https://adilet.zan.kz/rus/docs/Z1500000418 (Дата обращения: 15.08.2024 года)*

[7] *Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 «Об утверждении Концепции кибербезопасности ("Киберщит Казахстана"): https://adilet.zan.kz/rus/docs/P1700000407 (Дата обращения: 15.08.2024 года)*

[8] *Предпринимательский кодекс Республики Казахстан от 29 октября 2015 года // https://adilet.zan.kz/rus/docs/*

кибербезопасности может осуществляться при условии уточнения термина кибербезопасность – «в сфере информатизации».

На наш взгляд, принимая во внимание передовую зарубежную практику, необходимо выработать новый подход к законодательному разграничению понятий «кибербезопасность» и «информационная безопасность».

Основополагающей правовой базой в обеспечении КБ в Казахстане являются Закон об информатизации, Единые требования, а также ряд подзаконных актов, посвященных вопросам мониторинга, обмена информацией, аудита информационных систем.

Закон об информатизации регламентирует нормы касательно прав и обязанностей субъектов в сфере обеспечения кибербезопасности, включая обмен информацией касательно киберинцидентов, защиты объектов информатизации, испытания и аудита информационных систем.

Круг субъектов в сфере обеспечения кибербезопасности в РК достаточно обширный. Он включает в себя нижеследующих акторов:

1. Национальный координационный центр информационной безопасности (НКЦИБ) осуществляет сбор, анализ и обобщение информации отраслевых центров информационной безопасности и оперативных центров ИБ об инцидентах информационной безопасности на объектах ИКИ ЭП и других критически важных объектов инфраструктуры (далее – КВОИКИ);

2. Оперативные центры информационной безопасности (ОЦИБ) создаются при организации и обнаруживают, оценивают, прогнозируют, локализуют, нейтрализуют и осуществляют профилактику угроз ИБ.

3. Государственный оперативный центр информационной безопасности осуществляет мониторинг обеспечения ИБ объектов информатизации «электронного правительства», а также мониторинг событий информационной безопасности объектов информатизации государственных органов;

4. Национальная служба реагирования на компьютерные инциденты информационной безопасности осуществляет межотраслевую координацию по вопросам мониторинга обеспечения ИБ, казахстанского сегмента Интернета, а также КВОИКИ, реагирования на инциденты ИБ;

5. Служба реагирования на инциденты информационной безопасности (KZ-CERT) занимается координацией действий подразделений компьютерной безопасности государственных органов, операторов связи.

6. Отраслевой центр информационной безопасности организовывает и координирует обеспечение информационной безопасности субъектами информатизации соответствующей отрасли (сферы) государственного регулирования.

В свою очередь, Государственная техническая служба проводит испытания объектов информатизации «электронного правительства» на соответствие требованиям ИБ. Согласно действующему законодательству, выдача акта по результатам испытания входит в компетенцию уполномоченного органа в сфере обеспечения информационной безопасности. В рамках исполнения Указа Главы государства[9] в части «сокращения срока создания и (или) развития государственных объектов информатизации до шести месяцев» будет упразднена государственная услуга «Выдача акта по результатам испытаний на соответствие требований информационной безопасности». При этом, процедура выдачи протоколов испытаний по ИБ для информационных систем, собственником/владельцем и (или) заказчиком которых является государственный орган, передается в государственную техническую службу (GtoG), а для всех остальных информационных систем в аккредитованные испытательные лаборатории (BtoB).

Вместе с тем необходимо отметить, что, согласно Закону о техническом регулировании[10] «акт» не относится к документам об оценке соответствия (ст. 24 Закона). В связи с этим, принимая во внимание разграничение понятий КБ и ИБ, а также перечень документов по оценке соответствия, необходимо законодательно регламентировать понятие «протокол по результатам испытаний на соответствие требованиям кибербезопасности», а также полномочия компетентного органа в сфере обеспечения кибербезопасности касательно пересмотра результатов подобного протокола.

Анализ Закона об информатизации показал отсутствие норм, регламентирующих правовой статус собственника КВОИКИ.

K1500000375 (Дата обращения: 15.08.2024 года)

[9] Указ Президента Республики Казахстан от 13 апреля 2022 года № 872 «О мерах по дебюрократизации деятельности государственного аппарата»: https://adilet.zan.kz/rus/docs/U2200000872 (Дата обращения: 15.08.2024)

[10] Закон Республики Казахстан от 30 декабря 2020 года № 396-VI ЗРК «О техническом регулировании»// https://adilet.zan.kz/rus/docs/Z2000000396#564 (Дата обращения: 15.08.2024)

В нем регламентируются лишь обязанности владельца КВОИКИ (п. 2-1 ст. 17). В этой связи, на законодательном уровне имеется необходимость закрепить нормы касательно правового статуса собственника КВОИКИ.

Помимо этого, владелец КВОИКИ по Закону об информатизации не наделен следующими обязанностями:

1) собирать, анализировать и обобщать информацию об инцидентах кибербезопасности на объектах информационно-коммуникационной инфраструктуры;

2) обеспечивать кибербезопасность, защиту и безопасное функционирование КВОИКИ, реагирования на инциденты кибербезопасности с проведением совместных мероприятий по обеспечению кибербезопасности в порядке, установленном законодательством Республики Казахстан.

Также в рамках Закона об информатизации и подзаконных нормативных правовых актов используются термин «угроза информационной безопасности».

Практически во всех современных государствах информационная безопасность (она же компьютерная или кибербезопасность) является составной частью концепции национальной безопасности.

В зарубежной практике для обеспечения безопасности информации/данных используются два термина «информационная безопасность» и «кибербезопасность». По мнению различных аналитических изданий, информационную безопасность и кибербезопасность легко спутать, поскольку эти две области во многом пересекаются.[11] Необходимо рассмотреть понятия вышеуказанных терминов и определить их различия и схожие черты.

Под дефиницией «информационная безопасность» (InfoSec/Information Security) понимается «защита информации и информационных систем от несанкционированного доступа, использования, раскрытия, нарушения, модификации или уничтожения с целью обеспечения конфиденциальности, целостности и доступности».[12] Данное определение содержится в Глоссарии Национального института стандартов и технологий США (NIST).

Также согласно Глоссарию Национального института стандартов и технологий США (NIST), под «кибербезопасностью» (cybersecurity) понимается «предотвращение повреждения, защита и восстановление компьютеров, систем электронной связи, услуг электронной связи, проводной связи, включая содержащуюся в них информацию, для обеспечения ее доступности, целостности, конфиденциальности и неподдельности».[13]

Согласно Оксфордскому словарю, информационная безопасность - «состояние защищенности от несанкционированного использования информации, особенно электронных данных, или меры, принимаемые для достижения этого».[14] Понятие «кибербезопасность» в данном словаре отсутствует.

В соответствии с определением Кембриджского словаря:

1) «информационная безопасность» - состояние защищенности электронных данных от преступного или несанкционированного использования;

2) «кибербезопасность» - способы защиты компьютерных систем от таких угроз, как вирусы[15].

На практике встречается более расширенное понятие «информационная безопасность», связанное с обеспечением безопасности личности, в первую очередь. Так, к примеру, Доктрина информационной безопасности Российской Федерации, под термином «информационная безопасность Российской Федерации» понимает состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.[16] В Кыргызстане, согласно Концепции информационной

---

[11] *Information Security Vs. Cybersecurity: What's The Difference?: https://www.forbes.com/advisor/education/information-security-vs-cyber-security/ Difference Between Cybersecurity & Information Security: https://analyticsindiamag.com/difference-between-cybersecurity-information-security/ Cybersecurity vs. Information Security: Is There A Difference?: https://www.bitsight.com/blog/cybersecurity-vs-information-security (Дата обращения: 15.08.2024)*

[12] *Information security: https://csrc.nist.gov/glossary/term/information_security (Дата обращения: 15.08.2024)*

[13] *Cybersecurity: https://csrc.nist.gov/glossary/term/cybersecurity (Дата обращения: 28.09.2024)*

[14] *https://www.oxfordlearnersdictionaries.com/definition/english/translate (Дата обращения: 28.09.2024)*

[15] *Cambridge Dictionary: https://dictionary.cambridge.org/dictionary/english/information-security (Дата обращения: 28.09.2024)*

[16] *Доктрина информационной безопасности Российской Федерации: https://rg.ru/documents/2016/12/06/doktrina-infobezobasnost-site-dok.html (Дата обращения: 28.09.2024 года)*

безопасности Кыргызской Республики на 2019-2023 годы, информационная безопасность Кыргызской Республики - состояние защищенности личности, общества и государства от информационных угроз.[17]

Таким образом, в большинстве случаев, если информационная безопасность — это общий термин для создания и обслуживания систем и политик для защиты любой информации - электронной или физической, то кибербезопасность направлена на защиту систем и содержащихся в них данных, хранящихся исключительно в электронном виде, в киберпространстве. Следует подчеркнуть, что в некоторых странах подход к термину «информационная безопасность» имеет расширенное понятие и включает состояние защищенности личности, общества и государства.

Заключение

Принимая во внимание положения действующего законодательства, передовую зарубежную практику, мнение экспертного сообщества Казахстана, рекомендуется разграничить на законодательном уровне понятия «информационная безопасность» и «обеспечение кибербезопасности» применительно для сферы информатизации.

В целях введения в законодательство РК и единообразного толкования понятийно-категориального аппарата в обеспечении кибербезопасности предлагается закрепить определить понятия «угроза кибербезопасности», «инцидент кибербезопасности».

Анализ национального законодательства и зарубежного опыта показал необходимость расширения объема полномочий владельца КВОИКИ в вопросах обработки информации об инцидентах кибербезопасности на объектах информационно-коммуникационной инфраструктуры; активизации проведения совместных мероприятий по обеспечению кибербезопасности в порядке, установленном законодательством Республики Казахстан; необходимость направления КВОИКИ на повторное испытание на соответствие требованиям кибербезопасности; систематизировать процедуру передачи резервных копий электронных информационных ресурсов на единую национальную резервную платформу хранения электронных информационных ресурсов.

ЛИТЕРАТУРА

1. Татаринова Л.А. Соотношение понятий «информационная безопасность», «защита информации» и «кибербезопасность», «киберзащита» по законодательству Республики Казахстан // Вестник КазНУ. Серия юридическая. – 2019. – Т. 67. – №. 3. – С. 60-64.

2. Исабаева С.Б. Диссертация «Обеспечение кибербезопасности Казахстана в условиях глобальной цифровизации»: https://repository.apa.kz/bitstream/handle/123456789/732/746.pdf?sequence=1&isAllowed=y. (Дата обращения: 28.09.2024.)

3. Архипова Е.А. Современное понимание терминов «кибернетическая безопасность» и «информационная безопасность»// «Young Scientist» - № 12 (76) - December, 2019. – С.315-320. //file:///C:/Users/zh.kulzhabaeva/Desktop/Sovremennoe_ponimanie_terminov_kiberneticeskaa_bez.pdf (Дата обращения: 28.09.2024.)

4. Кубышкин А.В. Международно-правовые проблемы обеспечения информационной безопасности государства / Диссертация / Москва. 2002 г. // https://lawbook.online/pravovoe-regulirovaniemejdunarodnoe/informatsiyaf-bezopasnost-informatsionnaya-15097.html. (Дата обращения: 28.09.2024.)

5. Талимончик В.П. Международно-правовое регулирование отношений в сфере информации: дисс. ... докт.юрид. наук: 12.00.10 / Талимончик В.П.; [Место защиты: С.-Петерб. гос. ун-т].- Санкт-Петербург, 2013.- 400 с.: ил. РГБ ОД, 71 15-12/21// http:// www.dslib.net/pravo-evropy/mezhdunarodno-pravovoe-regulirovanie-otnoshenij-v-sfere-informacii.html. (Дата обращения: 28.09.2024.)

REFERENCES

1. Tatarinova L.A. Sootnoshenie ponjatij «informacionnaja bezopasnost'», «zashhita informacii» i «kiberbezopasnost'», «kiberzashhita» po zakonodatel'stvu Respubliki Kazahstan // Vestnik KazNU. Serija juridicheskaja. – 2019. – T. 67. – №. 3. – S. 60-64.

[17] *Концепция информационной безопасности Кыргызской Республики на 2019-2023 годыhttp://cbd.minjust.gov.kg/act/view/ru-ru/13652 (Дата обращения: 28.09.2024 года)*

2. Isabaeva S.B. Dissertacija «Obespechenie kiberbezopasnosti Kazahstana v uslovijah global'noj cifrovizacii»:https://repository.apa.kz/bitstream/handle/123456789/732/746.pdf?sequence=1&isAllowed=y. (Data obrashhenija: 28.09.2024.)

3. Arhipova E. A. Sovremennoe ponimanie terminov «kiberneticheskaja bezopasnost'» i «informacionnaja bezopasnost'»// «Young Scientist» - № 12 (76) - December, 2019. – S.315-320. //file:///C:/Users/zh.kulzhabaeva/Desktop/Sovremennoe_ponimanie_terminov_kiberneticeskaa_bez.pdf (Data obrashhenija: 28.09.2024.)

4. Kubyshkin A.V. Mezhdunarodno-pravovye problemy obespechenija informacionnoj bezopasnosti gosudarstva / Dissertacija / Moskva. 2002 g. // https://lawbook.online/pravovoe-regulirovaniemejdunarodnoe/informatsiyaf-bezopasnost-informatsionnaya-15097.html. (Data obrashhenija: 28.09.2024.)

5. Talimonchik V.P. Mezhdunarodno-pravovoe regulirovanie otnoshenij v sfere informacii: diss. ... dokt.jurid. nauk: 12.00.10 / Talimonchik V.P. [Mesto zashhity: S.-Peterb. gos. un-t].- Sankt-Peterburg, 2013.- 400 s.: il. RGB OD, 71 15-12/21// http:// www.dslib.net/pravo-evropy/mezhdunarodno-pravovoe-regulirovanie-otnoshenij-v-sfere-informacii.html. (Data obrashhenija: 28.09.2024.)