УДК:343.34:004.77 **DOI: 10.34670/AR.2020.91.10.062**

Некоторые проблемы обеспечения кибербезопасности в Кыргызской Республике

Казанбаева Зарема Равильевна

Кандидат юридических наук,
доцент кафедры предпринимательского
и процессуального права,
Кыргызский национальный
университет им. Ж. Баласагына,
720033, Кыргызская Республика, Бишкек, улица Киевская, 132;
e-mail: zarema_k76@mail.ru

Аннотация

В статье рассмотрены актуальные вопросы обеспечения кибербезопасности в современных условиях, затрагивающих широкий круг не только частных и корпоративных, но и государственных интересов, которые имеют широкое распространение и приобретают угрожающий характер. Обозначены главные тенденции развития киберугроз в современном глобальном информационном пространстве и меры, необходимые для их нейтрализации. Приведен правовой аспект вопросов, лежащих в основе зарождающейся тематики обеспечения кибербезопасности в Кыргызской Республике. Дан краткий обзор проекта Стратегии кибербезопасности КР, а также Плана мероприятий по реализации данной стратегии, содержащую единую концепцию информационной и кибербезопасности в качестве комплексного рамочного документа, определяющего государственную политику в этой сфере. Проведен анализ потенциальных путей развития соответствующей нормативной базы. Особо отмечена необходимость развития международного взаимодействия и сотрудничества в данной сфере.

Для цитирования в научных исследованиях

Казанбаева З.Р. Некоторые проблемы обеспечения кибербезопасности в Кыргызской Республике // Вопросы российского и международного права. 2019. Том 9. № 10А С. 493-500. DOI: 10.34670/AR.2020.91.10.062

Ключевые слова

Кибербезопасность, информационная безопасность, руководящие принципы, стандарты, нормативный документ.

Введение

В современных условиях развития общества и технологий невозможно отрицать тот факт, что роль информационной среды неуклонно возрастает. Киберпространство – это новый канал для создания и распространения всевозможной информации, оно стало новым двигателем роста экономики, новой платформой социального управления, новым способом международного сотрудничества, к тому же и совершенно новой областью государственного суверенитета. Информационно-Коммуникационные Технологии (ИКТ) являются неотъемлемой составной частью экономического и социального развития страны на пути к информационному обществу. Сегодняшний мир живет в эпоху глобальной конвергенции цифровых, физических и биологических технологий, изменяя мир вокруг и понимание качества жизни. Информационные технологии фундаментально изменили образ нашей повседневной жизни, способы работы и коммуникаций между людьми. Расширение областей применения информационных технологий, представляя собой фактор развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно является побудителем новых вызовов и угроз.

Согласно рейтингу Internet Live Stats, составленному в 2016 году, в Кыргызстане насчитывается 2,76 миллиона пользователей Всемирной паутины, что составляет 34.4 процента населения страны.[1] Для большинства пользователей Интернет стал повседневным, привычным явлением. Три четверти выходящих в сеть делают это ежедневно. У 94 процентов пользователей есть выход в сеть из дома. Интернет-аудитория по-прежнему растет.

Основное содержание

Активное развитие информационно-коммуникационных технологий и растущее использование сети Интернет с особой остротой определяет необходимость обеспечения безопасности в информационной среде, составной частью которой является киберпространство, и защиты информационной инфраструктуры, требующей широкого диапазона мер в области сетей связи и их информационной безопасности, борьбы с киберпреступностью.

По данным Norton Cybercrime Report 2018 каждый пятый человек старше 18 лет становился жертвой кибератаки либо в социальных сетях, либо через мобильные устройства.[2] Большинство пользователей Интернета предпринимают лишь базовые действия по защите информации (удаляют подозрительные электронные письма, с осторожностью раскрывают личные данные), однако не обращают внимания на такую важную меру, как создание сложных паролей и их регулярное изменение.

Неосторожность пользователей порождает новые виды компьютерных преступлений. В настоящий момент среди основных угроз кибербезопасности можно выделить внедрение компьютерного вируса, несанкционированный доступ к информации, ее подделку,

[1] «Число пользователей Интернета в КР превысило два миллиона – рейтинг…» // новостной портал «Sputnik.kg». [Электронный ресурс]. – Режим доступа: https://ru.sputnik.kg/Kyrgyzstan/20160728/1028236996.html

[2] «Тенденции киберугроз: обзор киберугроз 2018» // Центр безопасности Norton by Symantec. [Электронный ресурс]. – Режим доступа: https://us.norton.com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review.html

уничтожение, блокирование, копирование и т.д. На практике компьютерные преступления чаще всего являются лишь одним из этапов совершения кражи или мошенничества. Получив неправомерный доступ к персональному компьютеру преступник, как правило, не ограничивается лишь копированием информации о пароле и логине доступа в личном кабинете потерпевшего, который является пользователем услуг интернет-банкинга. Конечной и главной целью злоумышленника является тайное изъятие чужих денежных средств с банковского счета потерпевшего, что квалифицируется как кража**.**

Увеличение числа пользователей Интернета повышает критичность и делает более ощутимыми последствия в случае отказов техники, ведет к увеличению количества атак на абонентские устройства. Пренебрежение требованиями безопасности при использовании интернет-ресурсов и социальных сетей, игнорирование мер «цифровой гигиены» повышает риск неприкосновенности частной жизни, модификации или уничтожению персональных данных. Низкий уровень компьютерной грамотности конечных пользователей при отсутствии базовых знаний по общим методам компьютерных атак приводит к росту фактов кибер-мошенничества, противоправного использования ИКТ.

Меры, связанные с автоматизацией оказания государственных услуг, начавшаяся цифровизация государственных и муниципальных услуг, доступа к информации о деятельности государственных органов, создание государственных информационных ресурсов и систем, аккумулирование в них большого количества данных, в том числе критически важных (биометрика, данные, необходимые для выполнения государственных функций) также несут в себе определенные риски. Объем данных, обрабатываемых в государственном секторе, постоянно растет, что приводит к необходимости выработки новых форм их хранения и обеспечения их безопасности. Защита и безопасность данных, особенно критически важных, имеет сегодня решающее значение.

Критичной для Кыргызстана является ситуация с отсутствием обязательных для госорганов требований в сфере информационной и кибербезопасности для государственных информационных систем, включая обучение руководителей подразделений и всего задействованного в оказании электронных государственных и муниципальных услуг персонала принципам и технологиям защиты конфиденциальной информации.

В правовом поле, несмотря на обилие нормативных правовых актов в сфере информатизации, отсутствует единая терминология в части базовых терминов информационной и кибербезопасности. В действующем уголовном законодательстве отсутствуют многие составы совершаемых сегодня киберпреступлений, в процессуальном законодательстве – методы фиксации и оценки цифровых доказательств.

Ситуация усугубляется дефицитом доверия общественности к принимаемым государством мерам, направленным на защиту государственных информационных систем, обеспечение кибербезопасности.

При этом частный и финансовый сектор вынужден полагаться исключительно на собственные силы. Недооценена важность совместных усилий по формированию безопасного киберпространства внутри страны.

Недостаточная обеспеченность бизнес-сектора в технологиях защиты информации, зачастую не желание признавать потребности в защите информации и сетевой безопасности, приводит к большому количеству остающихся латентными инцидентов информационной и

кибербезопасности.[3]

Остро ощущается общая нехватка экспертов по информационной и кибербезопасности, особенно в государственном секторе. Программы обучения и подготовки специалистов в этой сфере, не в полной мере отвечают сегодняшним тенденциям и реалиям.

В целом анализ действующего законодательства в сфере информационной и кибербезопасности позволяет делать выводы о том, что оно:

- представляет собой устаревшую нормативную базу, большинство законов были сформированы в принципиально иной технологической и социальной среде, и в силу этого не учитывают современных трендов в сфере кибербезопасности;

- не содержит терминов и определений информационной безопасности, кибербезопасности, киберпространства, кибергигиены, нет понятий критической информационной инфраструктуры и т.п.;

- в определенной степени остается противоречивым, не подкреплено реальными ресурсами;

- не обеспечивает эффективный контроль обеспечения прав субъектов правовых отношений в сере информационной и кибербезопасности.

Одним из первых шагов в разрешении существующей ситуации является принятие Стратегии кибербезопасности Кыргызской Республики на 2019-2023 годы, утвержденной постановлением Правительства КР от 24 июля 2019 года № 369 и утверждения Плана мероприятий по реализации данной стратегии, содержащую единую концепцию информационной и кибербезопасности в качестве комплексного рамочного документа, определяющего государственную политику в этой сфере. [4]

Данная Стратегия кибербезопасности обеспечит единство подходов к формированию и реализации общенациональной политики обеспечения безопасности защищаемых законом видов информации, защиты электронных информационных ресурсов и систем, информационно-коммуникационной инфраструктуры, а также методологической базы и нормативных правовых актов, регулирующих сферу безопасного использования ИКТ.

Необходимой мерой в рамках реализации плана мероприятий по реализации Стратегии является и создание организационных киберструктур, специальных подразделений в правоохранительных органах, развитие сети центров реагирования на компьютерные инциденты (CERT) для определения киберугроз, управления операциями и реагирования на них, а также участия в механизмах сотрудничества на внутригосударственном, региональном и международном уровнях, привлечение технического и экспертного сообщества по вопросам потенциальных решений в сфере кибербезопасности. [5]

Общая цель таких мер состоит в создании и постоянном поддержании системы управления кибербезопасностью, обеспечивающей устойчивое развитие Кыргызской Республики при

[3] Фред Шрайер, Барбара Викс, Теодор Х. Винклер «Кибербезопасность: дорога, которую стоит пройти». Женева, 2013. Женевский центр демократического контроля над вооруженными силами.

[4] Стратегия киберезопасности Кыргызской Республики на 2019-2023 годы, утвержденной постановлением правительства КР от 24 июля 2019 года № 369; План мероприятий по реализации Концепции информационной безопасности КР на 2019-2023 годы, утвержденный постановлением правительства КР от 24 июля 2019 года № 369. [Электронный ресурс]. – Режим доступа: http://cbd.minjust.gov.kg/act/view/ru-ru/15479?cl=ru-ru

[5] Обзор потенциала в области кибербезопасности. Кыргызская Республика. Сентябрь 2017 года// Портал повышения компетенций в сфере кибербезопасности. [Электронный ресурс]. – Режим доступа: www.sbs.ox.ac.uk/cybersecuritycapacity

использовании информационно-коммуникационных технологий.

Необходимо развитие национального потенциала в области кибербезопасности, обмен информацией о передовом опыте, привлечение всего сообщества в целом. Формирование культуры кибербезопасности путем распространения передового опыта, повышение уровня осведомленности по вопросам кибербезопасности, создании необходимого потенциала, совершенствования средств кибербезопасности, укрепление и поддержание согласованности усилий в сфере кибербезопасности;

Вопросы кибербезопасности должны включать состояние защищенности средств телекоммуникаций (средств связи), цифровых (электронных) информационных ресурсов информационных систем, информационно-коммуникационной инфраструктуры от внешних и внутренних угроз.

Основными направлениями обеспечения кибербезопасности должны стать:

- правовое обеспечение (принятие и применение правовых норм в сфере кибербезопасности);
- организационное обеспечение (регламентация деятельности, исключающая нанесение ущерба, наличие соответствующих служб);
- инженерно-техническое обеспечение (использование технических средств, препятствующих нанесению ущерба, физические, аппаратные, программные и криптографические средства защиты).

Принятие данного документа будет означает значимый шаг в признании проблемы уязвимого киберпространства, выстраивании адекватных сегодняшнему дню методов и способов его защиты.

В Плане мероприятий четко определены органы/организации, ответственные за осуществление мер, сроки выполнения мероприятий. Все это должно быть подкреплено прописанными финансовыми ресурсами с четким распределением на каждое конкретное мероприятие.

В стране не выстроена четким образом и нормативно не закреплена иерархия государственных структур, задействованных в сфере обеспечения кибербезопасности с четким распределением задач и функций в данной сфере. Не создан уполномоченный государственный орган по реагированию на возникающие угрозы и киберинциденты (CERT).

Заключение

Результаты проведенного правового анализа позволяют сформулировать следующие общие **выводы и рекомендации**:

1) привести в соответствие с принятой Стратегией кибербезопасности КР нормативно-правовую базу с целью внедрения основ использования электронной аутентификации и электронной подписи на принципах технологической нейтральности, универсальности, соответствия требований к шифрованию признанным современным международным принципам; выстроить надлежащую систему сертификации средств шифрования, в соответствии с которыми требования к цифровой подписи и устройствам электронной подписи соответствуют надлежащим требованиям к безопасности;
2) выстроить на национальном уроне систему органов государственного управления, задействованных в определении политики кибербезопасности и ее реализации на

организационном (управление), нормативно-правовом (доктринальном), инженерно-техническом уровне;

3) создать уполномоченный государственный орган по реагированию на возникающие угрозы и киберинциденты (CERT); ежегодно публиковать отчеты о киберугрозах и рисках, информировать общественность в целях повышения осведомленности, в том числе через веб-сайт такого уполномоченного органа (CERT); указанный уполномоченный CERT должен нести ответственность за предотвращение, реагирование и прогнозирование киберугроз;
4) законодательно закрепить необходимость обязательного извещения об инцидентах и факта попыток нарушения кибербезопасности всеми субъектами государственного и частного сектора, а также обязательного взаимодействия указанных субъектов в обмене соответствующей информацией о киберугрозах и киберинцидентах.
5) рассмотреть вопрос о создании в вооруженных силах страны отделов, ответственных за защиту национального киберпространства.
6) создать независимый государственный надзорный орган, который отвечает за защиту персональных данных.
7) в уголовном законодательстве принять меры по криминализации следующих составов уголовных киберпреступлений (в соответствии с международными подходами, в том числе Конвенцией Совета Европы о киберпреступности [6]):

- незаконный доступ к информации, данным, сетям;
- незаконный перехват информации, данных;
- незаконное вмешательство в целостность информации, данных;
- незаконное вмешательство в работу информационных систем;
- ненадлежащее использование компьютерных устройств;

8) на уровне процессуального законодательства закрепить методы и средства цифровой криминалистики (компьютерной форензики), внедрить соответствующие методы и способы фиксации цифровых доказательств в целях расследования и исследования их в суде.
9) рассмотреть вопрос об усилении международного сотрудничества, заключению соглашений по вопросам кибербезопасности с другими странами и/или международными организациями.

Библиография

1. «Число пользователей Интернета в КР превысило два миллиона – рейтинг…» // новостной портал «Sputnik.kg». [Электронный ресурс]. – Режим доступа: https://ru.sputnik.kg/Kyrgyzstan/20160728/1028236996.html
2. «Тенденции киберугроз: обзор киберугроз 2018» // Центр безопасности Norton by Symantec. [Электронный ресурс]. – Режим доступа: https://us.norton.com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review.html
3. Фред Шрайер, Барбара Викс, Теодор Х. Винклер «Кибербезопасность: дорога, которую стоит пройти». Женева, 2013. Женевский центр демократического контроля над вооруженными силами.
4. Стратегия кибербезопасности Кыргызской Республики на 2019-2023 годы, утвержденной постановлением правительства КР от 24 июля 2019 года № 369; План мероприятий по реализации Концепции информационной безопасности КР на 2019-2023 годы, утвержденный постановлением правительства КР от 24 июля 2019 года №

[6] Конвенция о компьютерных преступлениях. Будапешт, 23 ноября 2001 года. [Электронный ресурс]. – Режим доступа: https://rm.coe.int/1680081580

369. [Электронный ресурс]. – Режим доступа: http://cbd.minjust.gov.kg/act/view/ru-ru/15479?cl=ru-ru/
5. Обзор потенциала в области кибербезопасности. Кыргызская Республика. Сентябрь 2017 года// Портал повышения компетенций в сфере кибербезопасности. [Электронный ресурс]. – Режим доступа: www.sbs.ox.ac.uk/cybersecuritycapacity/
6. Конвенция о компьютерных преступлениях. Будапешт, 23 ноября 2001 года. [Электронный ресурс]. – Режим доступа: https://rm.coe.int/1680081580/

Some cybersecurity issues in the Kyrgyz Republic

Zarema R. Kazanbaeva

PhD in Law, Associate Professor,
associate professor of enterprise
and procedural law
Kyrgyz national university,
720033, 132, Kievskaya st., Bishkek, Kyrgyz Republic;
e-mail: zarema_k76@mail.ru

Abstract

The article deals with topical issues of cybersecurity in modern conditions, affecting not only a wide range of private and corporate interests, but also public interests, which are widespread and are becoming threatening. The main trends in the development of cyber threats in the modern global information space and the measures necessary to neutralize them are identified. The legal aspect of issues underlying the emerging topic of cybersecurity in the Kyrgyz Republic is presented. A brief overview of the draft Cybersecurity Strategy of the Kyrgyz Republic, as well as the Action Plan for the implementation of this strategy, containing a unified concept of information and cybersecurity as a comprehensive framework document defining the state policy in this field, has been given. An analysis of the potential development of the relevant regulatory framework has been carried out. The need to develop international cooperation and cooperation in this field was emphasized.

For citation

Kazanbaeva Z.R. (2019) Nekotorye problemy obespecheniya kiberbezopasnosti v Kyrgyzskoi Respublike [Some cybersecurity issues in the Kyrgyz Republic]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 9 (10A), pp. 493-500. DOI: 10.34670/AR.2020.91.10.062

Keywords

Cybersecurity, information security, guidelines, standards, regulatory document.

References

1. Computer Crime Convention. Budapest, 23 November 2001. [Electronic Resource] - Access Mode: https://rm.coe.int/1680081580/
2. "Cyber Threat Trends: Cyber Threat Overview 2018"//Norton by Symantec Security Center. [Electronic Resource] - Access Mode: https://us.norton.com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review.html
3. Fred Schreyer, Barbara Wicks, Theodore H. Winkler "Cybersecurity: A Road Worth Passing." Geneva, 2013. Geneva Centre for the Democratic Control of Armed Forces.

4. Review of cybersecurity potential. Kyrgyz Republic. September 2017//Portal of competency enhancement in the field of cybersecurity. [Electronic Resource] - Access Mode: www.sbs.ox.ac.uk/cybersecuritycapacity/
5. Strategy of cybersecurity of the Kyrgyz Republic for 2019-2023, approved by the resolution of the Government of the Kyrgyz Republic of July 24, 2019 № 369; Plan of measures for the implementation of the Concept of Information Security of the Kyrgyz Republic for 2019-2023, approved by Government Decision No. 369 of 24 July 2019. [Electronic resource]. - Access mode: http://cbd.minjust.gov.kg/act/view/ru-en/15479? cl = ru-en/
6. "The number of Internet users in the Kyrgyz Republic exceeded two million - rating..."//news portal "Sputnik.kg." [Electronic Resource] - Access Mode: https://ru.sputnik.kg/Kyrgyzstan/20160728/1028236996.html