УДК 334.021:35

ИНИЦИАТИВЫ КАЗАХСТАНА В ОБЛАСТИ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Оралов Асылхан Раздыкович
asylhan_pvl_95@mail.ru
Евразийский национальный университет им. Л.Н. Гумилева,
г.Нурсултан, Республика Казахстан

Аннотация. В данной статье представлен обзор инициатив Казахстана по обеспечению кибербезопасности на международном уровне. Обозначены актуальные на сегодняшний день угрозы в сфере обеспечения кибербезопасности. Автор указывает на причины, по которым необходимо развивать международное сотрудничество в области обеспечения информационной безопасности. Среди них автор особенно делает акцент на интегрированном характере информационного пространства, что позволяет киберпреступникам совершать атаки физически находясь на территории другой страны. Также автор выделил такие угрозы, как эволюционирующий характер киберугроз и несовершенство существующих правовых систем по вопросам обеспечению информационной безопасности. Отдельно отмечены риски, связанные с уязвимостью программных приложений, которые приобретают актуальность в связи

широкомасштабной цифровизацией предоставления государственных услуг. Автор отмечает, что борьба с киберугрозами – это задача не одного государства, а всего международного сообщества. И в данном контексте инициативы Казахстана по обеспечению кибербезопасности на международном уровне представляют особую важность.
Ключевые слова: кибербезопасность, информационная безопасность, глобальные инициативы Казахстана

Аннотация. Бұл мақалада Қазақстанның халықаралық деңгейдегі киберқауіпсіздік бастамаларына шолу жасалады. Киберқауіпсіздік саласындағы қазіргі қауіп-қатерлер анықталды. Автор ақпараттық қауіпсіздік саласындағы халықаралық ынтымақтастықты дамыту қажеттілігінің себептерін көрсетеді. Олардың ішінде автор әсіресе киберқылмыскерлерге басқа елдің аумағында болған кезде шабуылдар жасауға мүмкіндік беретін ақпараттық кеңістіктің интеграцияланған сипатына ерекше назар аударады. Сондай-ақ, автор киберқауіптердің дамып келе жатқан сипаты және ақпараттық қауіпсіздік бойынша қолданыстағы құқықтық жүйелердің жетілмегендігі сияқты қауіп-қатерлерге тоқталды. Мемлекеттік қызметтерді көрсетудің ауқымды цифрландыруына байланысты өзекті болып отырған бағдарламалық қосымшалардың осалдығымен байланысты тәуекелдер бөлек атап өтілді. Автор киберқауіп-қатерлермен күресу бір мемлекеттің емес, бүкіл халықаралық қауымдастықтың міндеті екенін атап өтті. Осы тұрғыда халықаралық деңгейдегі киберқауіпсіздікті қамтамасыз ету жөніндегі Қазақстанның бастамалары ерекше маңызға ие.
Түйінді сөздер: киберқауіпсіздік, ақпараттық қауіпсіздік, Қазақстанның ғаламдық бастамалары

Abstract. This article provides an overview of Kazakhstan's cybersecurity initiatives at the international level. The current threats in the field of cybersecurity are identified. The author points out the reasons why it is necessary to develop international cooperation in the field of information security. The author especially focuses among them on the integrated nature of the information space, which allows cybercriminals to carry out attacks while physically they are located on the territory of another country. The author also highlighted such threats as the evolving nature of cyber threats and the imperfection of existing legal systems on information security. The risks associated with the vulnerability of software applications, which are becoming relevant in connection with the large-scale digitalization of the provision of public services, are separately noted. The author notes that the fight against cyber threats is not the task of one state, but of the entire international community. And in this context, Kazakhstan's initiatives to ensure cybersecurity at the international level are of particular importance.
Keywords: cybersecurity, information security, global initiatives of Kazakhstan

Обеспечение кибербезопасности является актуальным вопросом для всего международного пространства ввиду нарастающих угроз вместе с дальнейшим развитием информационно-коммуникативных технологий. Кроме того, государства мира активными темпами внедряют в процесс государственного управления информационно-коммуникационные технологии, многие государственные услуги сегодня можно получить в электронном формате. Цифровизации подлежат многие сферы жизнедеятельности людей, включая систему образования, здравоохранения, малого и среднего бизнеса и так далее.

Кибербезопасность определяется как «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 информационная безопасность в сфере информатизации» [1].

3 февраля 2021 года на заседании Совета Безопасности Республики Казахстан Первый Президент, Елбасы Н.А.Назарбаев отметил в качестве ключевых вызовов угрозы в области кибербезопасности. Ранее, во время заседания Совета Безопасности в 2019 году он также уделил особое внимание необходимости усиления кибербезопасности. На заседании Совета безопасности по кибербезопасности в 2017 году Елбасы отметил, что развитие цифровых технологий и их внедрение призвано принести пользу, но в то же время подвержено угрозам, к которым страна должна быть готова.

По оценкам экспертов, угрозы кибербезопасности на сегодняшний день имеют тенденцию к росту. Согласно некоторым данным, в январе 2021 года в Казахстане было совершено чуть более 3 тыс. кибератак — в 2,8 раза больше по сравнению с январем прошлого года. Из более чем 3 тыс. кибератак в январе 2021 года 2,7 тыс. приходится на ботнеты — заражение компьютеров через вредоносное ПО для дальнейшего их использования злоумышленниками без ведома их владельцев. Количество инцидентов-ботнетов за год выросло в 3,2 раза. Инцидентов, при которых фиксировалось отсутствие доступа к интернет-ресурсам, было зафиксировано 176 — на 69,2% больше, чем годом ранее [2].

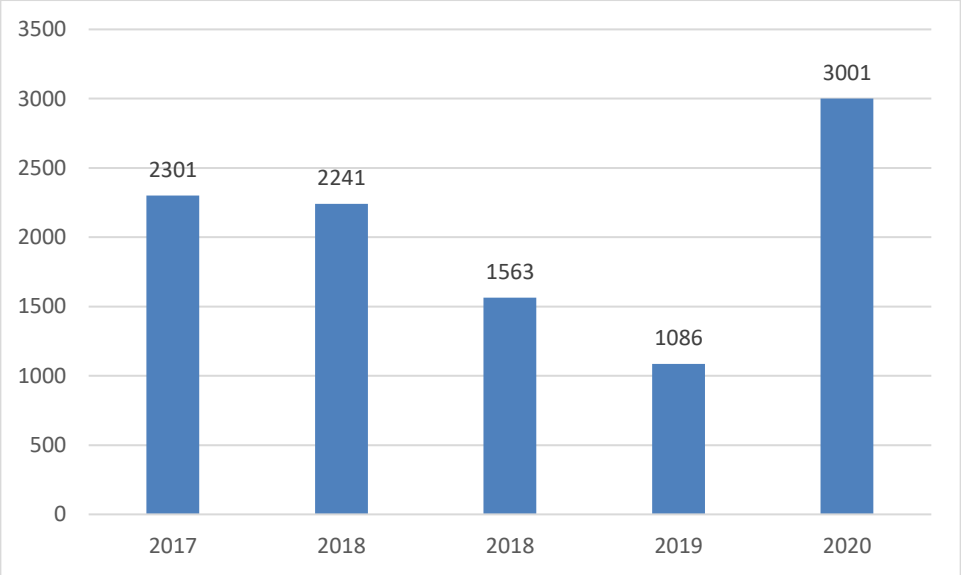

Рисунок 1. Количество инцидентов кибератак в Казахстане с 2017 по 2020 гг. [2]

При этом важно отметить, что обеспечение кибербезопасности затрудняется высокой степенью интегрированности информационного пространства стран, практически размываются границы виртуального пространства в международном контексте. Например, эксперты обеспокоены такими рисками, как ***постоянно эволюционирующий характер киберугроз***, изменение стратегии и «переход от модели центрального командного управления бот-сетями к одноранговой модели с распределенной структурой управления, способной охватывать находящиеся в различных странах компьютеры с раскрытой системой безопасности» [3]. Это явление представляет собой особый риск, так как затрудняется определение точного местонахождения какого-либо отдельного географического объекта как места происхождения кибератак с использованием бот-сетей, соответственно, их обнаружения и подавления. Также при такой стратегии может быть не только произведено распространение спама и вредоносных программ, а также запрещенного контента, при этом владельцы атакованных компьютеров могут не знать о том, что их устройство используется при кибератаке.

Также эксперты отмечают такие угрозы, как ***ослабление заградительных барьеров и совершенствование технических способов совершения киберпреступлений***.

Несанкционированный доступ к информационно-коммуникационным системам с целью их разрушения либо манипулирования ими становится доступнее из-за слабого финансовых и интеллектуальных заградительных барьеров для приобретения инструментария, то есть, набора технических средств и приложений для рассылки спама, создания вредоносных программных средств.

Кроме тоже, экспертами отмечается такая проблема, как ***несовершенство существующих правовых систем*** по вопросам обеспечению информационной безопасности. Так, киберпреступники переносят свои операции в страны, которые не приняли соответствующие меры для пресечения деятельности киберпреступников. При этом из-за интеграции информационного пространства они могут атаковать своих жертв из стран с принятыми законодательными мерами и будучи на территории другой страны. По оценкам экспертов, многие страны мира приняли соответствующее законодательство в области обеспечения кибербезопасности. Однако эти законы применимы в определенных национальных или региональных масштабах. В случае, если все страны введут соответствующее законодательство, киберпреступники не могут быть легко экстрадированы из страны, в которой данное киберпреступление было инспирировано, в страну, в которой оно было совершено, если эти правовые системы не обеспечивают возможность взаимодействия. В данном контексте важно выработать меры взаимопонимания и взаимодействия по вопросам обеспечения кибербезопасности между странами мира.

Также важной угрозой является ***уязвимость программных приложений.*** Так, вредоносные программные средства получают распространение, в том числе, из-за наличия уязвимых мест в программных приложениях, которые используются для получения несанкционированного доступа к информационно-коммуникационным системам. Таким образом, облегчается доступ к уязвимым программным приложениям и системам. Это особенно важный вопрос ввиду масштабной цифровизации государств, внедряющих электронный формат предоставления государственных услуг. В случае наличия слабых мест в программном обеспечении может быть получен несанкционированный доступ к информационным системам и установлен контроля над ними. Это может привести к потере личных данных, а также к финансовым потерям.

Также отдельной угрозой является отсутствие организационных структур в области обеспечения кибербезопасности. Безусловно, некоторые страны и региональные объединения создали собственные структуры, занимающиеся системами наблюдения и оповещения и реагированием на инциденты, а также организационные структуры для координации деятельности по реагированию на кибератаки. Однако необходимо дальнейшее развитие сотрудничества, формирование и совершенствование деятельности организаций по вопросам обеспечению кибербезопасности. Если кибератака совершается в одной стране, ее разрушительные последствия могут в течение короткого времени достичь своих жертв в странах, между которыми имеются соединения. Эксперты считают, что свободный поток информации, совместная работа и сотрудничество между национальными организационными структурами имеют жизненно важное значение для эффективного устранения таких инцидентов и реагирования на них

Таким образом, угрозы, связанные с киберпространством, носят глобальный характер. Географические факторы не являются препятствием для места и времени совершения кибератак. Все попытки решить эти проблемы на национальном и региональном уровнях оказались недостаточными. Юридические и технические меры на национальном и региональном уровнях необходимы, однако их недостаточно, для того чтобы преодолеть эти глобальные угрозы.

Киберугрозы являются проблемой не одной отдельно взятой страны, и обеспечение информационной безопасности возможным только при тесном сотрудничестве государств и требует выработки совместных мер по противодействию обозначенным угрозам.

Казахстан в целях усиления кибербезопасности на международном уровне, а также предотвращению угроз терроризма с использованием информационно-коммуникационных технологий, выдвигает свои инициативы. Так, в 2019 году на Саммите Шанхайской организации сотрудничества Президент Республики Казахстан К.К. Токаев выступил **с инициативой создания Центра информационной безопасности** на разе Региональной антитеррористической структуры ШОС. Глава государства акцентировал внимание на том, что перевод многих сфер общественной и экономической жизни в онлайн-пространство актуализирует тематику кибербезопасности [4].

Данная инициатива является важным шагом по укреплению международной и региональной безопасности. Ее реализация будет способствовать усилению мер по обеспечению кибербезопасности в регионе, а также защищать информационное пространство ШОС.

Список литературы

1. Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 «Об утверждении Концепции Кибербезопасности («Киберщит Казахстана»)». http://adilet.zan.kz/rus/docs/P1700000407

2. Количество кибератак в Казахстане увеличилось почти в 3 раза. 01.03.2021. https://kapital.kz/tehnology/93798/kolichestvo-kiberatak-v-kazakhstane-uvelichilos-pochti-v-3-raza.html

3. Глобальная программа кибербезопасности МСЭ. Международный союз электросвязи. 2007 г. https://ifap.ru/pr/2008/080908aa.pdf

4. Выступление Президента Казахстана Касым-Жомарта Токаева на заседании Совета глав государств-членов ШОС. https://www.akorda.kz/ru/speeches/external_political_affairs/ext_speeches_and_addresses/vystuplenie-prezidenta-kazahstana-kasym-zhomarta-tokaeva-na-zasedanii-soveta-glav-gosudarstv-chlenov-shos