НЕКОТОРЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ
В РЕСПУБЛИКЕ КАЗАХСТАН

Н. А. БИЕКЕНОВ,
заведующий сектором Отдела правоохранительной системы Администрации Президента Республики Казахстан,
д. ю. н.

В статье рассматриваются концептуальные аспекты организации и развития национальной системы киберзащиты с учетом зарубежного опыта. Определены сферы экономики и безопасности, которые могут стать главными жертвами хакерских атак. Предложены приоритетные направления стратегии защиты информационного пространства.

Ключевые слова: киберзащита, киберпреступность, национальная безопасность, информационное пространство,защита информации.

Высокие темпы развития в Казахстане информационно-коммуникационных технологий актуализируют вопросы защиты соответствующей инфраструктуры. Поскольку ее повреждение или разрушение может иметь значительные последствия для безопасности страны.

По оценкам экспертов Казахстан занимает 18-е место в мире по количеству получаемого спама и 7-е по опасности веб-серфинга. Почти половина пользователей Интернета в 2010 г., становились объектами атак со стороны хакеров, и эта цифра в 2011 г. увеличилась на 47%[1]. По данным Kaspersky Security Network, Казахстан стал объектом 85% интернет-атак в Центральной Азии[2]. При этом за последние три года наблюдается тенденция их роста пропорционально развитию цифровой инфраструктуры.

Кроме того, увеличение числа пользователей Интернета и расширение предоставляемых онлайн услуг привели к росту киберпреступности, в основном в финансовой сфере.

К их наиболее существенным особенностям обычно относят особую сложность раскрытия и расследования, чрезвычайно высокую латентность, прозрачность национальных границ для преступников и отсутствие единой правовой базы для борьбы с ними, нередко особо крупные размеры ущерба, высокопрофессиональный состав лиц, совершающих подобные преступления.

В наше время по всему миру насчитывается более тридцати тысяч сайтов, которые ориентированы на взлом и обучение этим приемам. За небольшие деньги любой подросток может позволить себе такую книгу, которая обучит его элементарным методам атаки на информационные системы. Это лишний раз подтверждает актуальность исследуемой проблемы и необходимость серьезного подхода к ее решению.

Имеются факты нападения на сайты правительственных учреждений. В частности, летом 2011 г., сотни компьютеров в государственных органах, главным образом, в дипломатических представительствах за рубежом, были заражены вирусом, который позволял хакерам получить контроль над компьютером и конфиденциальные данные.

До настоящего времени государственные информационные сети не подвергались политически мотивированным кибератакам, сходным с теми, что происходили в Эстонии в 2007 г. или в Грузии в 2008 г. Хотя такие атаки остаются возможной угрозой, но актуальность приобретают проблемы связанные с информационной безопасностью в стратегически важных секторах экономики – энергетике и транспорте, которые могут стать главными жертвами кибератак.

Так, национальные компании «Қазақстан темір жолы» поэтапно переводит в цифровой формат свои сложные операции, «KEGOC» нуждается в фазовой информации от своих сетей, чтобы лучше управлять потоками энергии.

Реализуется космическая программа, где большое значение играет контроль за спутниками связи. Вооруженные силы планируют развивать массовые электронные решения в аэрокосмической отрасли. Аналогичные технологии используются для мониторинга морских месторождений, судоходных путей нефтяных танкеров, экологических рисков и контрабанды на Каспии[3].

Наряду с этим оцифровывается сфера внутренней безопасности: документы удостоверяющие личность, камеры видеонаблюдения, электронные запросы по уголовным делам, перехват сообщений сотовой связи, системы мониторинга и сбора информации и т. д.

[1]На долю Казахстана приходится 95,19% спама Центральной Азии," Kursiv.kz, 26 августа 2011 г., http://www.kursiv.kz/novosti/v-kazakhstane/1195213705-na-dolyu-kazaxstana-prixoditsya-9519-spama-ca.html; "Казахстан занял 18 место в мировом рейтинге стран-распространителей спама," Kursiv.kz, 19 июля 2011г., http://www.kursiv.kz/novosti/v-kazakhstane/1195212413-kazaxstan-zanyal-18-e-mesto-v-mirovom-rejtinge-stran-rasprostranitelej-spama.html/.

[2]Екатерина Исакова, "Хакеры выбирают Казахстан," Kursiv.kz, 21 октября 2010 г, http://www.kursiv.kz/hi-tech/hitech- weekly/1195205432-xakery-vybirayut- kazaxstan.html.

[3]Аналитический обзор по Центральной Азии.//www.centralasiaprogram.org/images/Policy_Brief_2-RUS.pdf.

Все это не только актуализирует проблему защиты информации, но и делает возможным использование IT-коммуникаций в организации общественных протестов или террористических актов, а также управлении возможными конфликтами.

Именно поэтому общество нуждается в твердых гарантиях его устойчивости к кибератакам и другим критическим ситуациям. Независимо от того, направлены ли такие атаки против коммерческих предприятий или государственных органов.

Для организации киберзащиты создан ряд структур *(Управление «К» Комитета криминальной полиции МВД, аналогичное специализированное подразделение в КНБ, государственная служба технической защиты информации Министерства транспорта и коммуникаций)*, принимающих участие в обеспечении информационной безопасности государства. Они занимаются совершенствованием законодательства, изучением и сертификацией технических средств, обеспечением информационной защиты систем органов государственной власти, расследованием преступлений и обнаруженных кибератак, а также принятием мер по их пресечению.

Анализ работы указанных структур показал, что она зачастую не сбалансирована и не синхронизирована. Реализуемая защита киберпространства не одинаково эффективна во всех направлениях.

При этом в методологическом плане принимаемые меры ориентированы на сдерживание объективно развивающихся процессов, поэтому баланс безопасности может быть нарушен при относительно скромных ресурсах.

Изучение зарубежного опыта *(в том числе с выездом в США, Эстонию, Китай и Южную Корею)* организации кибербезопасности свидетельствует о значительной диспропорции уровня готовности к противодействию киберугрозам на национальном уровне, а также возможности использования передовых наработок в Казахстане.

В ОБЛАСТИ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ

На сегодня только 10 из 27 стран ЕС отработали стратегии кибербезопасности. *Наиболее защищенными странами являются Дания, Великобритания, Финляндия, Швеция и Нидерланды.* С целью устранения указанных недостатков 7 февраля 2013 г. Европейская комиссия представила «Стратегию кибербезопасности ЕС».

Основные положения проекта документа предусматривают:

- разработку всеми странами-членами Евросоюза национальных стратегий кибербезопасности;
- обязательную ратификацию всеми участниками политической организации «Конвенции Совета Европы о киберпреступности» от 2001 г., как основного международного правового инструмента противодействия преступности в киберпространстве. *Справочно: в мире действуют «Европейская Конвенция по киберпреступлениям» (подписана 43 странами, 39 из которых входят в Совет Европы, а оставшиеся – Япония, США, Канада и Южная Африка). В ней указаны определения терминов, связанных с проблемой, классификации и необходимые санкции по борьбе с кибертерроризмом. «Окинавская хартия глобального информационного общества» рассматривает аналогичную проблему, но распространяется только на США, Великобританию, Канаду, Германию, Францию, Италию, Японию и Россию.*
- введение единого перечня стандартов готовности стран к противодействию киберугрозам;
- обязательное информирование европейскими компаниями определенного национального органа о выявленных кибериндидентах;
- улучшение синергии между гражданским и оборонным секторами в сфере кибербезопасности и т.д.

С 1 января 2013 г. в составе Европола начал функционировать «Европейский центр по киберпреступности», основная цель которого состоит в увеличении защищенности граждан стран-членов ЕС от растущего уровня киберпреступности.

Аналогичные акты на политическом уровне приняты в России *(Указ Президента РФ от 15.01.2013 г. №31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации)*[4], Республике Корея *(июль 2013 г.)*, США (*февраль 2013 г.)*[5] и Украине *(Доктрина информационной безопасности, 2009 г.)*[6].

Поэтому представляется необходимым разработать и принять государственную программу (концепцию, стратегию) киберзащиты информационного пространства, предусматривающей:

- создание системы постоянного мониторинга киберугроз;
- развитие национальных систем оперативного обнаружения кибератак и противодействия им;
- совершенствование системы взаимодействия государственных силовых структур, отвечающих за кибербезопасность, и общественных организаций, работающих в области информационной безопасности;
- организацию программы научно-технических работ по проблемам кибербезопасности.

В ОБЛАСТИ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Казахстан становится частью более широкого киберпространства, в котором два главных соседа – Россия и Китай – особенно известны своим высоким уровнем киберпреступности. *В 2011 г. более трети мировых киберпреступлений, причинивших ущерб на $12,5 млрд., осуществлялись выходцами из русско-говорящего мира. Группы, вовлеченные в эту деятельность, все больше контролируются организованными преступными элементами. Китай также является убежищем для киберпреступников, особенно для тех, кто участвует в экономических преступлениях. Доклад США раскритиковал обе страны за использование высокотехнологичного шпионажа для своего собственного развития, а Китай назвал местом, где проживают «наиболее активные и стойкие преступники экономического шпионажа»*[7].

Поэтому развитие мер по укреплению кибербезопасности должно осуществляться на отличной от соседей базе, а в идеале следует формировать собственную программную платформу. Поскольку в стране используется импортное сетевое оборудование, которое возможно обслуживается зарубежными вендорами дистанционно и может быть в нужный момент отключено. Весь серьёзный софт по информационной безопасности иностранных производителей, в частности, вся информация смартфонов, планшетников и компьютеров Apple посредством специальных программ доступна разведывательным службам США.

[4]http://www.consultant.ru/document/cons_doc_LAW_140909/.

[5]http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity).

[6]Азаров одобрил законопроект о кибербезопасности http://inukr.net/economy/158871-azarov-odobril-zakonoproekt-o-kiberbezopasnosti.html.

[7]Пентагон обвиняет Китай в кибератаках http://www.golos-ameriki.ru/content/us-china-cyber/1655652.html.

В 2009 г. в Южной Корее были задержаны трое киберпреступников, которые промышляли сбытом не подлежащих огласке сведений более 20 миллионов соотечественников. Это является крупнейшей утечкой персональных данных в истории страны.

Используя решения иностранных разработчиков, государство получило, по сути, чёрный ящик, готовое техническое решение, выполняющее заложенные функции, но контролируемое иностранной компанией.

Государственные органы и электронное правительство пользуются иностранными антивирусными продуктами, что также не способствует обеспечению безопасности. Кроме того, следует разрабатывать собственные криптографические программы.

Партнёрские же отношения с местными разработчиками дали бы государству непосредственно технологии, знания, специалистов, возможность создания собственных, контролируемых решений. Во всех развитых странах существуют компании по разработке антивирусных программ и других решений в области защиты информации.

В плане организации защиты интересен опыт Китая, где действует программа «Золотой щит» которая фильтрует содержание интернет-сайтов. Программа получила неофициальное название «Великий китайский фаервол». Так, данные от интернет-провайдера в этой стране передаются не напрямую к пользователю, а на специальный «сервер защиты», который, в свою очередь, решает, что именно можно показать потребителю. Так в Китае в разное время попадали под запрет Google, Wikipedia и Youtube[8].

Создание средств защиты в стране на уровне государства неизбежно ведёт к изучению средств нападения. Совершенствование защиты – это постоянно растущая квалификация кадров, изучение существующего кибероружия, отработка технологии атак для тестирования собственной защиты.

Кибероружие уже существует в мире как отдельный класс вооружения. Ведущие IT-державы открыто заявляют о создании собственного кибервооружения и подразделений для ведения кибервойн. В нынешнее время практически каждый политический или военный конфликт сопровождается противоборством в сети Интернет.

Согласно открытой информации технологиями для проведения кибератак сейчас обладают единицы государств (между которыми уже возникают открытые противостояния в киберпространстве), но исследования в этой отрасли ведутся множеством стран.

Создание кибероружия в Казахстане является лишь вопросом времени. Формировать отрасль кибервооружения необходимо уже сейчас или в ближайшем будущем, как одну из задач государственной программы киберзащиты.

В ОБЛАСТИ ВЗАИМОДЕЙСТВИЯ С ЧАСТНЫМ СЕКТОРОМ

Развитие информационных технологий – многообещающий бизнес. К примеру, в Корее объем системы E-learning *(обучение с помощью Интернет и мультимедиа. Работают 18 виртуальных университетов)* ежегодно растет на 8,2%.

Вместе с тем, существует очень мало систематизированной информации о безопасности в киберпространстве, поданной в доступной форме. Есть острая необходимость запуска программы обучения населения. Она должна быть рассчитана не только на узкоспециализированные структуры, но и на изучение основ кибербезопасности в школах и институтах, а также обучение людей, вышедших из школьного и студенческого возраста.

Для информирования и обучения необходимо, в том числе, создать информационно-консультационный центр, где пользователи смогут получать ответы на вопросы, связанные с киберугрозами и киберзащитой.

В Украине уже создана такая информационная площадка *(Antivirus.ua)*, миссией которого является создание условий для обмена квалифицированной информацией между рядовыми пользователями, экспертами, представителями правоохранительных структур, СМИ, учебных заведений.

Таким образом, быстрая информатизация, масштабы потенциальных последствий преступлений в киберпространстве требуют от государства серьезного внимания к развитию национальной системы кибербезопасности. Первоочередные шаги в этом направлении должны предусматривать разработку необходимой нормативно-правовой базы и повышение эффективности работы соответствующих институциональных структур с учетом зарубежного опыта в этой сфере.

[8]Путин «загрузил» ФСБ интернетом. http://digest.subscribe.ru/inet/protection/n985077559. html

Н. А. Биекенов: Қазақстан Республикасында киберқауіпсіздікті қамтамасыз етудің бірқатар проблемалары.

Мақалада шетелдік тәжірибені ескере отырып, киберқорғаныстың ұлттық жүйесін ұйымдастыру мен дамытудың концептуалды аспектілері қарастырылады. Экономика мен қауіпсіздіктің хакерлік шабуылдардың басты құрбандары болуы мүмкін салалары анықталған. Ақпараттық кеңістікті қорғайтын стратегияның басым бағыттары ұсынылған.

Түйінді сөздер: киберқорғаныс, киберқылмыстық, ұлттық қауіпсіздік, киберқауіптер, ақпараттық кеңістік, ақпаратты қорғау, хакерлік шабуыл, қорғаныс стратегиясы, киберкеңістік, ғаламтор.

N. Biyekenov: Some problems of cyber security in the Republic of Kazakhstan.

The article discusses conceptual aspects of organisation and development of the national cyber security system based on international experience. The sectors of economy and security, that could be the main victims of hacker attacks are defined. Priority directions of the strategy of information space security are proposed.

Keywords: cyber security, cyber crime, national security, information space, information protection, hacker attack, defense strategy, cyberspace, internet.