УДК 343

Некоторые вопросы обеспечения кибербезопасности в Республике Казахстан

Темиржанова Ляззат Ахметжановна – кандидат юридических наук, адвокат коллегии адвокатов г. Нур-Султан.

Сагымбеков Бахытжан Жасамуратович – магистр права, ведущий научный сотрудник Академии правоохранительных органов при Генеральной прокуратуре Республике Казахстан.

Аннотация: В статье авторами рассмотрены правовые и организационные проблемы обеспечения кибербезопасности в Республике Казахстан. Авторами отмечается, что среди наиболее распространенных проблем обеспечения кибербезопасности является отсутствие в стране единого механизма взаимодействия между правоохранительными органами зарубежных государств, недостаточный уровень подготовки сотрудников органов, осуществляющих противодействие киберугрозам, нехватка IT-специалистов, а также низкий уровень их оплаты в государственных органах.

Ключевые слова: Кибербзопасность, правоохранительных органы информационные технологии, киберпреступления.

Использование IT-технологий во всех сферах жизнедеятельности граждан, организаций напрямую связано с вопросами повышения уровня кибербезопасности серверов всех государственных и правоохранительных структур, а также непрерывного его совершенствования.

С 2010 года плотность пользователей сети интернет в Казахстане увеличилась с 36,1% до 75%, а количество пользователей мобильного Интернета - с 3 миллионов 694 тысяч практически утроилось и достигло 10 миллионов 567 тысяч в нашей стране на ежедневной основе фиксируется и отражается более 100 тыс. атак различного уровня

воздействия на электронные информационные ресурсы государственных органов.[1]

В этой связи взлом электронных систем любого учреждения обоснованно вызывает вопросы и тревогу по поводу эффективности усилий органов, отвечающих за обеспечение кибербезопасности государства.

В целях обеспечения информационной безопасности государственных органов, физических и юридических лиц, а также выработки механизмов предупреждения и оперативного реагирования на инциденты информационной безопасности в 2017 году в Республике Казахстан была принята Концепции кибербезопасности «Киберщит Казахстана».

Концепцией «Киберщит Казахстана» на данном этапе предусматривается создание Национального оперативного органа нацеленного на обработку данных о состоянии защищенности наиболее важных компонентов национальной информационной инфраструктуры. Соответственно уже сейчас назрела объективная необходимость совместной и слаженной работы правоохранительных органов по противодействию киберугрозам.

Согласно последнему отчету Межународного сюза электросвязи в Глобальном индексе кибербезопасности за 2018-2019 гг. лидирующие позиции заняли Великобритания (1 место) и США (2 место).

Среди стран СНГ лидирующую позицию заняла Россия (26 место). Казахстан на сегодня находится на 40 месте, Узбекистан 52 место, Азербайджан 55 место. Далее следуют Беларусь (69), Армения (79), Таджикистан (107), Киргизстан (111) и Туркменистан (143).[2]

В Казахстане среди правоохранительных органов вопросами кибербезопасности непосредственно занимается МВД РК. В этих целях ее структуре создано специальное управление «К» – подразделение по борьбе с высокотехнологичной преступностью.

Наряду с МВД в Казахстане существует Служба реагирования на компьютерные инциденты KZ-CERT, целью которой является выявление атак на объекты информационные инфраструктуры, обеспечение взаимодействия между экспертами и разработка технических рекомендаций и законодательства по борьбе с киберпреступностью.[3]

Таким образом, контроль динамики киберпреступности и ее распространения зависят не только от органов власти, но и от культуры кибербезопасности каждого пользователя.

Изучение материалов СМИ, деятельности государственных и правоохранительных органов позволяет выделить ряд проблем в сфере кибербзопансоти. К их числу можно отнести такие проблемы, как безграничность интернета и несовершенство правовой базы, трудности идентификации преступника из-за отсутствия единого механизма взаимодействия между правоохранительными органами зарубежных государств, недостаточный уровень подготовки сотрудников органов, осуществляющих противодействие киберпреступлениям, нехватка IT-специалистов, а также низкий уровень их оплаты в государственных органах.

Кроме того, в ходе расследования уголовных правонарушений данной категории, следователи органов внутренних дел сталкиваются с проблемами, связанными с получением информации о принадлежности зарубежных IP-адресов, принадлежности мобильных телефонов и номеров электронных кошельков, а также квалифицированным осмотром техники, так как даже при удалении электронной информации на цифровом носителе могут оставаться определенные данные.

Многие зарубежные государства серьезно подходят к проблемам кибербезопасности, в том числе к организации расследования правонарушений, совершаемых с использованием информационных систем.

Интересным на наш взгляд представляет опыт Республики Корея, где в 2012 году создан Центр кибербезопасности при Генеральной прокуратуре Республики Корея (Prosecutor’s Cybersecurity Center). Способ организации данной службы на деле доказал свою эффективность, так как с момента ее создания отмечено снижение инцидентов связанных с киберугрозами.

Центр кибербезопасности Кореи представляет собой центр мониторинга информационных систем и систем кибербезопасности, анализ электронных журналов и корреляция событий, анализ вирусной активности, средств предотвращения утечек информации и других источников событий.

Подобные национальные центры кибербезопасности имеются в других странах, например, в Германии (NCAZ), США (NCSC), Великобритании (NISCC).

В этой связи знакомство с передовым мировым опытом противодействия кибератакам, киберпреступлениям, компьютерной криминалистики полезно и необходимо для сотрудников правоохранительных органов.

На сегодня международный опыт по противодействию киберугрозам активно изучается Генеральной прокуратурой РК, в связи с чем на постоянно основе направляет своих сотрудников в командировки для обучения и участия в зарубежных семинарах.

Вместе с тем в Генеральной прокуратуре РК имеется потребность в кадрах для организации круглосуточно функционирующего центра кибербезопасности Генеральной прокуратуры, в штате которого необходимы квалифицированные специалисты по сбору и анализу цифровых улик.

В качестве объективных обстоятельств, препятствующих кадровому обеспечению государственных органов квалифицированными специалистами по кибербезопасности, является значительная разница в размере заработной платы специалиста по кибербезопасности. Более того, сложные процедуры приема на государственную службу еще более усугубляет положение.

На сегодня в структуре Генеральной прокуратуры имеется управление информационной безопасности, которое обеспечивает информационную безопасность ее органов, однако надзорными функциями данное управление не обладает.

По сведениям Управления, ежемесячно Государственная техническая служба,

находящаяся в структуре КНБ РК, фиксирует и направляет им отчет об имеющихся как минимум 100 000 событий, в том числе критических угрозах. В управление изучает и принимает соответствующие меры по устранению данных угроз.

В 2017 г. при Генеральной прокуратуре также создан консультативно-совещательный орган – IT-Комитет органов прокуратуры, целью которого является осуществление работы по совершенствованию, автоматизации и оптимизации, действующих/новых бизнес-процессов органов, ведомств и учреждений прокуратуры Республики Казахстан, а также рассмотрение, предварительное утверждение новых решений и продуктов.

Соответственно IT-Комитет не занимается предупреждением кибератак, он прорабатывает вопросы информационной технологии и бизнес-процессов.

Наряду с названными подразделениями в Комитете правовой статистики и специальных учетов Генеральной прокуратуры создана группа по информационной безопасности, которая обеспечивает информационную безопасность КПСиСУ.[4]

Необходимо отметить Комитетом по правовой статистике на сегодня реализован ряд успешных проектов – Единый реестр досудебных расследований; аналитические информационные системы «Торелик», «Зандылык», интернет-портал «Карта уголовных правонарушений», «Карта ДТП», Е-штрафы, единый шлюз «Система информационного обмена правоохранительных и специальных органов», информационный сервис «Централизованный банк данных должников «Шектеу», «Единый реестр субъектов и объектов проверок», проект «Е-уголовное дело».[5]

Данные проекты показали обширный информационный потенциал КПСиСУ, который может быть использован в обеспечении кибербезопасности электронных систем не только КПСиСУ, а также и всех правоохранительных органов.

Таким образом, несмотря на достигнутые результаты Казахстана в области обеспечения кибербезопасности нами сделанные следующие выводы и рекомендации:

1. В структуре всех государственных органов, а также их ведомствах необходимо

создание специализированного подразделения киберзащите.

2. Нужно повышать качество подготовки высококвалифицированных IT-специалистов для нужд государственных органов, а также компьютерно-информационную грамотность населения, т.к. низкая квалификация сотрудников влияет на количество регистрации преступлений в сфере информационных технологий и качество их выявления и расследования.

3. Требуется консолидация всех государственных и правоохранительных органов в сфере кибербезопасности. К примеру, со стороны Генеральной прокуратуры имеется объективная возможность использовать информационный потенциал КПСиСУ и создать базу мониторинга и отслеживания состояния имеющихся киберугроз.

4. Необходимо создание надежной правовой базы, определяющей понятие, порядок и движение криптовалют, так как неуклонно растет количество киберпрступлений связанных цифровыми видами валют.

Список литературы

1. Концепция кибербезопасности «Киберщит Казахстана», утверждена постановлением Правительства Республики Казахстан от 30 июня 2017г .No30. Режим доступа: URL https://tengrinews.kz/zakon /pravitelstvo_respubliki_kazahstan_premer_ministr_rk/hozyaystvennaya_deyatelnost/id-P1700000407/(дата обращения 01.03.2020)

2. Глобальный индекс кибербезопасности 2018-2019. Режим доступа: URL https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx (дата обращения 01.03.2020)

3. О Службе реагирования на компьютерные инциденты KZ-CERT. Режим доступа: URL https://cert.gov.kz/about/kz_cert (дата обращения 01.04.2020)

4. Комитет по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан. Режим доступа: URL http://pravstat.prokuror.gov.kz/rus/

5. Развитие органов правовой статистики и специальных учетов //Закон и время – 2017. – No4/196 – С.54-55.

{social}