Секция «Проблемы социального и политического развития современного Востока»

Проблема кибербезопасности в Южной Кореи

Научный руководитель – Валиахметова Гульнара Ниловна

Муратова Алена Анатольевна
Студент (магистр)
Уральский федеральный университет имени первого Президента России Б.Н.Ельцина,
Институт социальных и политических наук, Екатеринбург, Россия
E-mail: Alen4ka1810@list.ru

Проблема кибербезопасности в Южной Корее

Муратова А.А
Студент
Уральский федеральный университет имени первого Президента России Б. Н. Ельцина. Гуманитарный институт. Екатеринбург, Россия.
E-mail: Alen4ka1810@list.ru

Конец XX века можно охарактеризовать, как начало новой информационной эпохи. Сейчас уже можно говорить о том, что четвертая промышленная революция наступила и мы являемся свидетелями данного этапа. Статичность нашего мира была утеряна, с тех пор как у человечества появился компьютер, а затем и мировая информационная сеть-интернет. С появлением интернета появились чипы и датчики, которые встроены в ваш ПК или телефон, благодаря им мир интернета стал еще более удобным. Географические и временные границы стерлись, расстояние уже не является проблемой для обмена информацией.

С технологичсекой точки зрения «кибербезопасность» означает «поиск и применение административных и технических средств для предотвращения каких-либо повреждений, изменений или утечки информации при сборе, обработке, хранении, поиске, передаче или получении информации». С другой стороны, «кибербезопасность» означает защиту информационной и коммуникационной сети и систем от различных рисков, которые могут иметь место в киберпространстве. А информационная среда, в свою очередь - это совокупность информационных ресурсов, система формирования, распространения, использования информационной инфраструктуры. Помимо концепции защиты информации, кибербезопаснгсть включает в себя ряд мероприятий по обнаружению и реагированию на различные угрозы [3].

Проблема кибербезопаности и киберпреступности поднимается на мировом уровне. Кибератаки совершаются ежеминутно, в связи с этим мы можем разделить кибератаки, совершаемые на информационную систему на случайные: сбои в работе аппаратуры, человеческий фактор, аварийные ситуации из-за стихийных бедствий или отключения электропитания и т.п) и преднамеренные.

Южная Корея, страна с одним из высочайших показателей уровня проникновения Интернета, сталкивается с серьезной угрозой внешних кибератак, что вынуждает ее концентрировать все усилия на защите своего киберпространства.

Корея лидер в электронной индустрии и родина таких транснациональных компаний как Samsung, LG, поэтому и уровень проникновения мобильного Интернета составляет 84.8%. Мобильные социальные сети и приложения для онлайн общения необычайно популярны в стране - местное приложение KakaoTalk используется более чем 48 млн. человек. Наиболее же популярными социальными сетями являются Facebook, Twitter, а также местные - M2Day, NateConnect.

Однако, все положительные аспекты использования Интернета в Корее резко контрастируют с подавляющим числом киберпреступлений и инцидентов в сфере обеспечения информационной безопасности по сравнению с другими странами региона. Существует мнение, что непомерно высокий уровень киберпреступности относится к неизбежным издержкам ускоренного развития информационного общества [1]. Другие соотносят эти нежелательные явления с отсутствием социального и правового контроля онлайн-активности в Корее, а также парадоксальным невниманием властей.

По данным Корейского агентства интернет-развития, ежегодные экономические потери, связанные с киберпреступностью, оцениваются примерно в 452 трлн вон. Это 0,8% мирового ВВП [3].

Согласно статистическим данным Symantec Corporation, известному своей антивирусной продукцией Norton, в мире каждый 12 человек становится жертвой киберпреступности. Сумма ущерба составляет целых 113 миллиардов долларов, что в 10 раз больше, чем в Олимпийских играх в Лондоне[3].

Законодательная база Южной Кореи в сфере борьбы с киберпреступностью и обеспечением информационной безопасности весьма обширна. Меры наказания за совершение киберпреступлений предусмотрены уголовным кодексом, речь в котором идет о традиционных преступлениях, главным средством совершения которых является компьютер и сеть Интернет, а также другими законами [2].

Южная Корея стремиться занять позицию как регионального, так и глобального лидера в международном диалоге по вопросам обеспечения кибербезопасности. Наиболее конструктивный диалог государство поддерживает с Японией и Китаем. Взаимодействие со странами региона ведется через форумы АСЕАН, АТЕС, APCERT. Однако крайне напряженные отношения с Северной Кореей являются существенной помехой на пути к достижению статуса регионального лидера.

Источники и литература

1) 1. Cho KyonSeok. The Current Situation of Measures for Crime Victims in the Korean Criminal Justice System. [Электронный ресурс] // unafei.or URL: http://www.unafei.or.jp/english/pdf/RS_No81/No81_10VE_Seok.pdf (дата обращения 15.01.2018)
2) 2. Junsik Jang. Best Practices in Cybercrime Investigation in the Republic of Korea. [Электронный ресурс] // unafei.or http://www.unafei.or.jp/english/pdf/RS_No79/No79_09VE_Jang2.pdf (дата обращения 15.01.2018)
3) 3. 4[U+CC28] [U+C0B0][U+C5C5][U+D601][U+BA85] [U+C2DC][U+B300][U+C5D0] [U+B354] [U+C911][U+C694][U+D574][U+C9C4] [U+C0AC][U+C774][U+BC84] [U+BCF4][U+C548][Электронный ресурс] // .naver.com. URL: https://m.blog.naver.com/PostView.nhn?blogId=mocienews&logNo=221130150270&proxyReferer=https%3A%2F%2Fm.search.naver.com (дата обращения 20.01.2018)