ЕВРАЗИЙСКОЕ НАУЧНОЕ ОБЪЕДИНЕНИЕ
EURASIAN SCIENTIFIC ASSOCIATION
www.esa-conference.ru

УДК 004.056.2(575.2)

Анализ обеспечения кибербезопасности в Кыргызской Республике

Зимин Игорь Викторович, кандидат технических наук, доцент
Айтбекова Аида Айтбековна, аспирант
Институт электроники и телекоммуникаций
при Кыргызском государственном техническом университете им. И. Раззакова
Султанова Фируза Рустамовна, кандидат физико-математических наук, и.о. доцента
Кыргызская государственная медицинская академия им. И.К. Ахунбаева

DOI: 10.5281/zenodo.3271164

Информационная сфера является ключевой сферой жизни Кыргызской Республики, как государства и как целостного в своем разнообразии общества. В настоящее время самым актуальным вопросом считается кибербезопасность. Основу кибербезопасности составляют три процесса: предотвращение угрозы; обнаружение угрозы; реагирование. [1,3]

В последнее время вопрос информационной безопасности Кыргызстана очень часто становится предметом дискуссий и споров.

На ранних стадиях развития сетей связи вопросы безопасности не были главными из-за небольшого количества пользователей и наличия в основном локальных сетей, в которых подразумевается доверие всех пользователей друг другу. В данное время кибербезопасность приобретает все большее значение в связи с растущим влиянием компьютерных систем и Интернета на все сферы жизни, развитием беспроводных сетей, а также ростом «умных» устройств, смартфонов, телевизоров как части Интернета вещей. [1,3]

Кибербезопасность ставит своей целью организацию безопасности киберсреды, системы, в которую могут входить акционеры, относящиеся ко многим общественным и частным организациям, использующим разнообразные компоненты и разные подходы к вопросу безопасности.

Конкретные меры обеспечения кибербезопасности могут быть определены по результатам оценки рисков и в рамках планирования действий по повышению безопасности активов.

Концепции обеспечения информационной безопасности. Геополитическая карта Евразии перекрасилась, появились новые суверенные государства, в том числе и государства Центральной Азии: Кыргызская Республика, Республика Таджикистан, Туркменистан, Республика Узбекистан и Республика Казахстан. Получив независимость, эти государства стали разрабатывать свои национальные модели развития. С появлением информационно-коммуникационные технологии ИКТ одной из главных задач молодых государств Центральной Азии стало обеспечение информационной безопасности.

Одним из важных компонентов кибербезопасности является наличие в стране групп по реагированию на компьютерные инциденты (CERT). Развитие системы таких организаций в Центральной Азии находится пока на начальной стадии. Национальные Службы реагирования на компьютерные инциденты действуют в Республике Казахстан с 2011 г., Республике Узбекистан с 2013 г., а в Кыргызской Республике с 2015г.

В целом, актуальность развития таких структур для государств Центральной Азии велика, но вопрос их формирования, выведения на постоянный и комплексный формат деятельности и впоследствии, отраслевой специализации будет упираться в техническую готовность, организационные, финансовые и человеческие ресурсы.

Как обстоит ситуация с межгосударственным взаимодействием центрально-азиатских стран помимо наличия регионального CERT?

На сегодня Центральная Азия не охвачена каким-либо единым международным форматом борьбы с киберпреступностью. Инструменты и механизмы, предлагаемые региональными форматами, отрывочны и не образуют комплексной системы противодействия этим вызовам. В частности, страны региона не участвуют в механизме Конвенции о компьютерных преступлениях Совета Европы от 2001 г. Проблемы предотвращения и борьбы с ежедневными вызовами киберпреступности пока в большинстве случаев решаются самими операторами связи. [6] Каждая республика формирует собственные концепции обеспечения информационной безопасности, которые находят отражение в национальных законодательствах. Практически во всех государствах региона есть специальные комиссии по проблемам кибербезопасности, принимаются межправительственные соглашения по защите информационного пространства.

Меры, которые предпринимает Кыргызская Республика для обеспечения кибербезопасности, и каковы современные проблемы данной отрасли? В этой связи в Кыргызской Республике приняты государственные программы обеспечения информационной безопасности, обеспечения защиты государственной тайны, концепция обеспечения информационной безопасности, а также ряд других организационных и практических мер, которые реализуются государственными органами во взаимодействии с Государственным комитетом национальной безопасности ГКНБ, во взаимодействии с соответствующими госструктурами участвует в разработке ряда нормативных правовых актов по созданию и развитию единой информационной телекоммуникационной системы государственных органов. Правительству поручено обеспечить создание Комитета по информационной безопасности, который фактически будет выполнять функции уполномоченного органа (регулятора) по разработке государственной политики в сфере национальной информационной безопасности. [7]

ЕВРАЗИЙСКОЕ НАУЧНОЕ ОБЪЕДИНЕНИЕ
EURASIAN SCIENTIFIC ASSOCIATION
www.esa-conference.ru

В условиях стремительного развития информационно-телекоммуникационных технологий и их активного проникновения в повседневную жизнь граждан и систему государственного управления, а также полноценной реализации национального проекта "Таза Коом" важное значение приобретает вопрос обеспечения кибербезопасности.

Вопросы политики безопасности в Кыргызской Республике. Вопросы кибербезопасности будут решены: через формирование рамочной основы для единой системы государственной политики Кыргызской Республики; в области обеспечения кибербезопасности; в модернизации системы национальных стандартов в области кибербезопасности и защиты информации; в повышении уровня человеческих ресурсов и кадрового потенциала; формировании Национального Совета по кибербезопасности Кыргызской Республики; в обеспечении безопасности критической информационной инфраструктуры Кыргызской Республики, включая резервирование объектов инфраструктуры и данных.

В Кыргызской Республике был создан «Исследовательский аналитической центр ИКТ и информационной безопасности » на базе Института электроники и телекоммуникаций под руководством Секретариата Совета обороны Кыргызской Республики.

Основная цель центра – анализ и исследования, имеющихся ИКТ-угроз. Одной из самых важных тем, связанных с регулированием цифрового пространства, является обеспечение кибербезопасности. На фоне растущего экстремизма эта проблема особенно актуальна для стран Центральной Азии, где вместе с числом пользователей интернета растет и активность террористических организаций, которые вербуют новых адептов в свои ряды в режиме онлайн. Юное поколение остается незащищенным от киберугроз, последствия которых уже дают о себе знать. И это только малая доля возможных рисков, которые таятся в цифровом пространстве. Поэтому Кыргызская Республика перешла к решительным мерам по обеспечению кибербезопасности страны. [3,6]

Отдельное внимание будет уделено совершенствованию законодательства в области борьбы с компьютерной преступностью, расследованию компьютерных преступлений и активизации международного сотрудничества в этой области. Будет обеспечено закрепление в Уголовно-процессуальном кодексе Кыргызской Республики, методов и средств компьютерной криминалистики.

В рамках обновления Уголовного кодекса Кыргызской Республики будет обеспечена криминализация таких уголовных киберпреступлений, как: 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. [7]

Разработка нормативных правовых актов Кыргызской Республики.

Совместно с Советом Безопасности Аппарата Президента Кыргызской Республики разработан проект «Стратегии кибербезопасности Кыргызской Республики 2017-2023гг». Целью настоящей Стратегии является обеспечение уровня кибербезопасности граждан, бизнеса и государства, позволяющего защитить их жизненно важные интересы в области использования ИКТ и обеспечить устойчивое социально-экономическое развитие Кыргызской Республики, включая цифровую трансформацию национальной экономики.

Определены основные задачи:

- Формирование единой системы мер обеспечения кибербезопасности;
- Противодействие компьютерной преступности;
- Формирование единого понятийного и методологического аппарата в области кибербезопасности и информационной безопасности;
- Обеспечение безопасности критической информационной инфраструктуры;
- Формирование национальной системы предупреждения, реагирования и управления компьютерными инцидентами;
- Повышение уровня человеческих ресурсов и кадрового потенциала и т.д.

Исследование рисков. Как и в других странах в Кыргызской Республике достаточно много рисков информационной безопасности в сфере информационных услуг, особенно в телекоммуникациях. Основными рисками, влияющими на развитие телекоммуникационной сферы в Кыргызстане, является:

- медленное, по сравнению с другими странами, развитие технологий как в сфере ИБ, так и в телекоммуникационной в целом;
- дефицит квалифицированных специалистов в сфере телекоммуникации. Как известно на сегодняшний день в Кыргызской Республике оплата труда в сфере телекоммуникаций не столь велика по сравнению со сферой мобильной связи, в связи с чем, в ТКС дефицит квалифицированных кадров в области ИБ;
- «медленное реагирование государства на изменения и развития технологические процессы в сфере телекоммуникации».

Проведенный анализ консалтинговой компанией Ernst & Young внутренней среды телекоммуникаций в Кыргызской Республике показывает, что риски, определенные исследованием Ernst & Young практически в полном объеме присутствуют на рынке телекоммуникаций Кыргызской Республики. [9].

По результатам исследования в области информационной безопасности, был составлен список самых опасных угроз, который представлен на рисунке 1.

Как видно из выше приведённой диаграммы, кража информации (66%) является одной из самых опасных угроз, далее по списку идет халатность сотрудников (56%), которые по причине своей невнимательности совершают утечку информации, вредоносные программы (46%) закрывают тройку лидеров. Нельзя забывать и про аппаратные и программные сбои (44%), на которые приходится довольно большое количество угроз. Как ни странно, но на спам приходится всего 20%, хотя, его нельзя недооценивать, т.к. в сети Интернет его довольно много.

www.esa-conference.ru

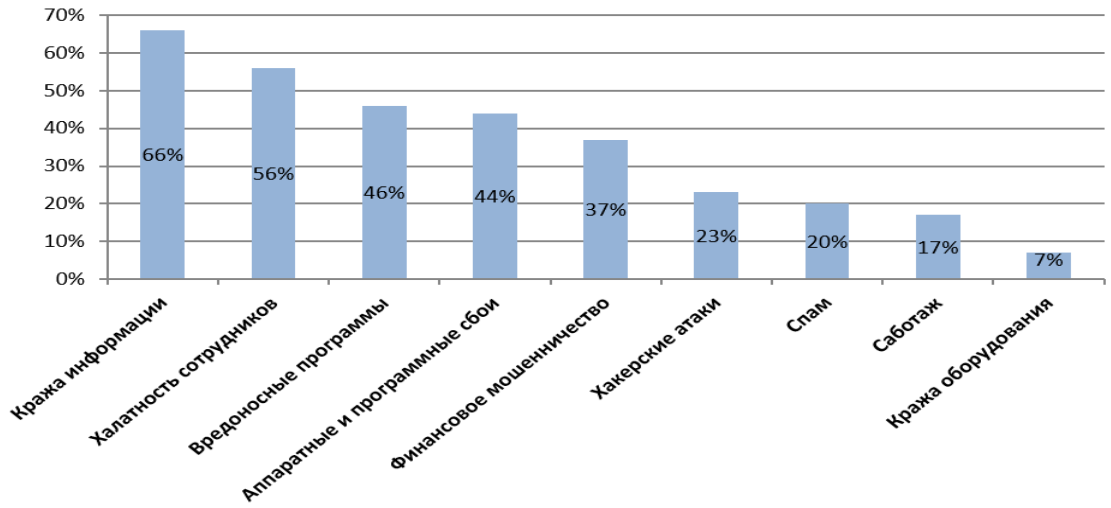

Рис.1. Самые опасные угрозы в процентах.

Проекты:

ППКР «Об уполномоченном государственном органе по персональным данным Кыргызской Республики» (Агентство по персональным данным);

ППКР «Об утверждении Требований к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных»;

ППКР «Об утверждении требований и защите информации, содержащейся в базах данных государственных информационных систем». В проекте постановления разработан перечень технологий, изложенных в международных стандартах, для государственных информационных систем, использующих системы шифрования и средства криптографической защиты информации (СКЗИ), а также разработаны технические требования к средствам криптографической защиты информации;

ППКР «О внесении изменений в постановление Правительства Кыргызской Республики» «Об утверждении Перечня главнейших сведений, составляющих государственную тайну и Положения о порядке установления степени секретности категорий сведений и определения степени секретности сведений, содержащихся в работах, документах и изделиях» от 7 июля 1995 года №267/9»;

В настоящее время в Кыргызской Республике для обеспечения и улучшения состояния кибербезопасности взаимодействуют и проводят исследования с различными международными организациями: [4]

Ключевой задачей в части наращивания человеческого потенциала является внедрение систематизированного преподавания дисциплин кибербезопасности, компьютерной гигиены и грамотности в систему школьного, среднего профессионального и высшего образования Кыргызской Республики. Для этой цели в горизонте 2020 г. Министерство образования Кыргызской Республики должно осуществить процесс пересмотра стандартов образовательной деятельности и образовательных регламентов, с целью включения:

- Дисциплины «Кибербезопасность» в список профильных дисциплин для технических специальностей в высших образовательных учреждениях Кыргызской Республики;
- Дисциплины «Компьютерная гигиена» и «Основы цифровой грамотности» в качестве обязательных предметов в учебных программах базового школьного образования Кыргызской Республики.

Для развития отрасли в первую очередь необходимо обеспечение качественного технического образования, подготовки высококвалифицированных технических специалистов. Только в условиях развитой научно-исследовательской и производственной платформы можно успешно реализовать стратегическую программу импорта - замещения в сфере информационной безопасности.

Литература:

1.Барсуков В.С., Обеспечение информационной безопасности Москва, Изд. ЭкоТренз, 1996-211с.

2.Зимин И.В., «Информационная безопасность», Учебное пособие, Бишкек Изд. КРСУ, 2018-132с.

3.Зимин И.В., Голомазов Е.Г., Проблемы и особенности информационной безопасности в Кыргызской Республике [Текст] И.В. Зимин, Е.Г. Голомазов // Научное издание Московского университета. — Гармиш-Партенкирхен, 2015. С.341-345.

4.Ибрагимова Г., Подходы государств Центральной Азии к вопросам управления интернетом и обеспечения информационной безопасности // Индекс безопасности. 2013. №1. (104). С. 103 — 128.

5.http://www.garant.ru

6.https://digital.report/bezopasnost/

7.https://www.itu.int/ru

8.https://iot.ru/wiki/kiberbezopasnost

9.Ясенев В.И. Информационная безопасность в экономических системах Учебное пособие — Н. Новгород: Изд-во ННГУ, 2006, 18 — 43 с.