ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(СПбГУ)

Гроссман Екатерина Олеговна

**Проблема информационной безопасности и кибертерроризма в странах Азии**

Направление: 41.04.03 «Востоковедение и африканистика»

Магистерская диссертация

(Профиль: *Политика и международные отношения стран Азии и Африки*)

Научный руководитель: к.и.н. Османов Е.М.

Рецензент: к.т.н. Мельников А.В.

Санкт-Петербург

2016

# Оглавление

[Оглавление 2](#_Toc451803398)

[Введение 2](#_Toc451803399)

[Глава первая 5](#_Toc451803400)

[Основные вопросы международной информационной безопасности 5](#_Toc451803401)

[Глава вторая 22](#_Toc451803402)

[2.1.Проблема информационной безопасности в Индии 22](#_Toc451803403)

[2.2. Проблема информационной безопасности и кибертерроризма в Китае 35](#_Toc451803404)

[2.3. Проблема информационной безопасности и кибертерроризма в Южной Корее 46](#_Toc451803405)

[2.4. Проблема информационной безопасности и кибертерроризма в Японии 56](#_Toc451803406)

[Заключение 70](#_Toc451803407)

[Список использованной литературы и источников: 72](#_Toc451803408)

# Введение

Последняя четверть XX столетия ознаменовала собой вступление человечества в новую стадию развития – в эпоху информационного общества со всеми его достижениями и противоречиями. С момента изобретения компьютера и распространения сети Интернет, наш мир утратил статичность. Географические и временные границы были стерты, расстояние перестало оказывать какое-либо влияние на процесс обмена информацией. Подобный характер информационного процесса является опорой для формирования мирового демократического общества, стимулирует дальнейшее развитие экономики, науки.

Однако человечество, поставив глобальные информационные сети себе на службу, не предвидело, какие возможности для злоупотребления несет в себе столь бурное развитие информационной инфраструктуры и технологий. Поэтому, столкнувшись с качественно новой угрозой – на сей раз в глобальном информационном пространстве – мировое сообщество оказалось не готово ей противостоять. [[1]](#footnote-1)Сегодня жертвами преступников, орудующих в информационном пространстве, могут стать не только люди, но и целые государства. При этом безопасность тысяч людей может оказаться в зависимости от нескольких или даже одного преступников.

Поэтому сегодня как никогда актуальной является проблема обеспечения безопасности глобального информационного пространства. Необходимо отметить, что данная тема вызывает живейший интерес у исследователей по всему миру, но практически вся литература по проблеме освещает ситуацию на Западе – что вполне объяснимо, в конце концов, сеть Интернет впервые появилась именно там.

Однако на современном этапе развития мирового общества нельзя игнорировать ту роль, которую играют ведущие Азиатские страны в глобальных информационных процессах.

Целью данной научной работы является рассмотрение проблемы информационной безопасности и кибертерроризма в странах Азии, на примере четырех наиболее развитых в данном отношении государств Азиатско-Тихоокеанского региона. В соответствии с поставленной целью необходимо решить следующие исследовательские задачи:

- ознакомиться с доступной литературой по данному вопросу

- рассмотреть законодательную базу в сфере обеспечения информационной безопасности и борьбы с киберпреступностью каждого из исследуемых государств

- проанализировать особенности ситуации в сфере обеспечения информационной безопасности и борьбы с кибертерроризмом в каждом из исследуемых государств

- сделать выводы о текущей ситуации в сфере обеспечения информационной безопасности и борьбы с кибертерроризмом в каждом из исследуемых государств.

Следует отметить, что в отечественной литературе данная тема не освещается. Из русскоязычной литературы в исследовании были использованы труды В.А. Голубева, И.Ю. Алексеева, В.А. Васенина, В.Н. Галатенко, в которых поднимаются вопросы обеспечения информационной безопасности в мире и в России. Из работ сотрудников Университета ИТМО М.И. Шубинского, Н.А. Гатченко и др. можно почерпнуть общее представление о том, как понимается информационная система и информационная безопасность.

Работы зарубежных европейских ученых: М. Бреннера, Д. Льюиса и проч. посвященные киберпреступности, дают начальное представление об этом явлении, но, к сожалению, эти исследования не охватывают страны Азии их законодательство. Тем не менее они дают хорошие теоретические основы для изучения понятия «киберпреступность» в глобальном аспекте.

Наиболее ценными для исследования являются работы таких ученых стран Азии, как Цутия Мотохиро[[2]](#footnote-2), Хисамити Окамура[[3]](#footnote-3), Охара Бондзи[[4]](#footnote-4) и др. Интересным также представляется включить в исследование информацию, почерпнутую из работ таких журналистов, как, например Танигути Нагаё [[5]](#footnote-5) и др. Следует оговориться, что работы, принадлежащие перу зарубежных ученых, не переводились на русский язык, их перевод осуществлялся автором исследования.

Структура работы представлена введением, двумя главами, заключением и списком использованной литературы и источников. Первая глава является вводной, она посвящена общим вопросам обеспечения мировой информационной безопасности с акцентом на ситуации в странах Азии. Во второй главе подробно рассмотрены вопросы обеспечения информационной безопасности и борьбы с киберпреступностью в четырех наиболее развитых странах Азиатско-Тихоокеанского региона: Японии, Китае, Южной Корее и Индии.

# 

# Глава первая

## Основные вопросы международной информационной безопасности

Одна из специфических особенностей современного этапа развития мирового сообщества заключается в том, что деятельность любого характера так или иначе связана с информационной средой, и вне информационного потока человек уже не мыслит свою жизнь. Не случайно, одним из основополагающих прав человека сегодня стало право на «свободу самовыражения, свободу поиска, получения и распространения информации и идей, независимо от государственных границ, а также право на защиту от вмешательства в частную жизнь»[[6]](#footnote-6).

Важно отметить, что за прошедшее столетие возможность свободного обмена информацией, доступ к ней и способы ее передачи несказанно возросли. В истории развития информационной среды и информационных технологий выделяется несколько переломных моментов, называемых информационными революциями[[7]](#footnote-7), каждая из которых преобразовывала человеческое общество.

Первая информационная революция связана с изобретением письменности, возможности передачи знаний от поколения к поколению. Вторая информационная революция (XVI в) вызвана изобретением книгопечатания, благодаря которому радикально изменилось индустриальное общество, культура; ей человечество обязано появлением первых СМИ.

Третья информационная революция (конец XIX в) обусловлена изобретением электричества, а, следовательно, радио, телефона, телеграфа, телевидения. Возможность оперативно передавать большие объемы информации оказала существенное влияние на формирование картины мира, а также стала основным проводником идей глобализации. Четвертая информационная революция (70-е гг. XX в.) связана с появлением персональных компьютеров.

Сегодня человечество переживает пятую информационную революцию, главной особенностью которой является процесс формирования и развития трансграничных информационных сетей, охватывающих все страны и континенты, воздействующие на каждого человека в отдельности и на огромные массы людей. [[8]](#footnote-8)Пятой информационной революцией человечество обязано появлению сети Интернет. И сегодня под информационной сетью в большинстве случаев понимается компьютерная информационная сеть.

Совершенствование средств передачи информации, повсеместное распространение компьютерных сетей привели к тому, что на заре третьего тысячелетия сформировалось глобальное информационное пространство[[9]](#footnote-9); оформилось в качестве инфраструктуры современного постиндустриального общества. В политической сфере сегодня все большее влияние приобретают не силовые, а информационные факторы; в экономике – информационная продукция стала частью системы товарных отношений, появилось множество коммерческих структур – потребителей и производителей информации, средств ее защиты; уровень экономического потенциала теперь напрямую зависит от уровня развития информационной инфраструктуры. На международной арене – если в прошлом государства соперничали за господство на суше, море, в воздухе, в космосе – теперь же борьба переходит в глобальное информационное, другими словами, киберпространство. Информация становится важнейшим стратегическим ресурсом государств. Таким образом, формирование единого мирового киберпространства превращается в глобальный фактор развития, определяет основные направления общественного прогресса.[[10]](#footnote-10)

Однако, оборотной стороной нового витка развития общества является появление новых же угроз. И сегодня можно с уверенностью говорить о существовании угрозы нового вида – преступных действий, совершаемых в глобальном информационном пространстве, преступлений, главным объектом которых является информационная безопасность, а главным средством является компьютерная информационная сеть – киберпреступлений[[11]](#footnote-11).

Мир сегодня находится в прочной зависимости от бесперебойного функционирования информационной инфраструктуры. От ее степени зависит как моральное и материальное благосостояние людей, так и порой их жизнь. К сожалению, избежать этого риска невозможно, поэтому в современном мире все большую актуальность приобретают вопросы информационной безопасности и киберпреступности. [[12]](#footnote-12)

Следует отметить, что обеспечение информационной безопасности в мире – проблема сравнительно новая. Собственно, под информационной безопасностью понимается состояние защищенности информационной среды от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации[[13]](#footnote-13). А информационная среда, в свою очередь – это совокупность информационных ресурсов, система формирования, распространения, использования информационной инфраструктуры.

Выделяется три главных аспекта информационной безопасности: доступность (возможность за определенное время получить требуемую информационную услугу), целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения) и конфиденциальность (защита от несанкционированного прочтения). Нарушение вышеперечисленных аспектов информационной безопасности создает опасность функционированию и развитию информационной среды.[[14]](#footnote-14)

Современная информационная система являет собой сложный механизм, состоящий из многочисленных взаимосвязанных модулей, различной степени автономности, между которыми происходит обмен информацией. Каждый из модулей может подвергнуться опасному внешнему воздействию или выйти из строя. Выделяются следующие компоненты информационной системы: аппаратные средства (компьютеры и их периферийные устройства), программное обеспечение, информация (данные, хранимые временно и постоянно на разных носителях), персонал[[15]](#footnote-15).

Опасные воздействия на информационную систему можно разделить на случайные, которым система подвергается на протяжение всех этапов существования (к ним относят сбои в работе аппаратуры, человеческий фактор, аварийные ситуации из-за стихийных бедствий или отключения электропитания и проч.) и преднамеренные.

На второй категории следует остановиться подробнее, потому что именно преступные действия такого характера наносят максимальный ущерб информационной среде, владельцам и пользователям компьютерных информационных систем. К категории преднамеренного воздействия относятся все виды киберпреступлений[[16]](#footnote-16).

Несмотря на существование различных классификаций киберпреступлений, большинство исследователей в сфере обеспечения информационной безопасности подразделяют их на компьютерные преступления и преступления, совершаемые с помощью компьютеров и компьютерных информационных сетей, а также прочих устройств доступа к киберпространству. [[17]](#footnote-17)Такой классификации придерживается и Организация Объединенных Наций. К компьютерным преступлениям относят те действия, главным объектом посягательств которых является конфиденциальность, целостность, доступность информационных систем и данных. Остальные киберпреступления посягают на имущество и имущественные права (кражи, мошенничества в киберпространстве), авторские права (плагиат и пиратство), а также безопасность человека и общества – кибертерроризм.

Конвенция Совета Европы о киберпреступности выделяет четыре типа компьютерных преступлений, нарушающих конфиденциальность, целостность, доступность компьютерных информационных систем: незаконный доступ (противоправный умышленный доступ к компьютерной информационной системе), незаконный перехват, вмешательство в данные, вмешательство в систему (препятствование функционированию компьютерной информационной системы путем ввода, повреждения, удаления, изменения данных). [[18]](#footnote-18)

Остальные преступления относятся к совершаемым с помощью компьютера: преступления, связанные с нарушением авторских прав, преступления, где компьютер используется как орудие преступления, преступления, в которых компьютеры играют роль интеллектуальных средств (за разжигание вражды, размещение в сети детской порнографии и проч.) Последние два вида преступлений являются объектом дискуссий, так как их состав охватывается нормами национальных уголовных кодексов, и не являются новыми видами преступных действий. Соответственно наказание за действия такого рода тоже предусмотрены уголовным правом. И единственное чем они отличаются – современные средства их совершения.[[19]](#footnote-19)

Существует также классификация киберпреступлений, разработанная на Х Конгрессе ООН. Она подразумевает деление на насильственные (угрозы, киберпреследование, кибертерроризм) и ненасильственные (крыжи, финансовые махинации, реклама проституции в сети Интернет, отмывание денег с использованием электронного перемещения капитала и проч.) преступления.

Что же касается источников киберпреступлений, то лица и организации, совершающие атаки, условно подразделяются на несколько категорий, причем четкие границы между ними провести достаточно сложно. Во-первых, хакеры – лица, обладающие обширными знаниями в области информационной безопасности и компьютерных технологий. Хакеров разделяют на «белых» - которые занимаются поиском уязвимых точек в информационной системе для последующего их исправления, и «черных» - целью которых является нанесение ущерба данным, кража информации и прочее[[20]](#footnote-20).

Далее – хактивисты. Термин «хактивизм» возник от соединения слов «hack» и «activism»; он используется для обозначения актов социального протеста нового вида, соединяющих в себе социальный протест и использование Интернет-технологий с целью нанесения ущерба компьютерной информационной сети и ее пользователям. Так, например, после бомбежки силами НАТО китайского посольства в Белграде в 1999 группа хакеров из Китая развернула антиамериканскую кампанию, в рамках которой произошел взлом нескольких американских правительственных сайтов, в том числе сайта американского посольства в Пекине, на котором был помещен лозунг, называвший американцев варварами, а на сайте Департамента внутренних дел были размещены фотографии жертв бомбежки и изображение китайского флага.

В-третьих, киберпреступники – с тех пор, как корыстная преступность распространилась в Интернет, кибервымогательство стало популярным способом эксплуатации компьютерных сетей с целью незаконного извлечения прибыли.

Лица, занимающиеся промышленным шпионажем – как в пользу государства, так и в пользу индивидуального заказчика.

И, наконец, кибертеррористы. Несмотря на то, что единой крупномасштабной кибер атаки, организованной террористическими группами, пока не произошло, считается, что террористы достигли того уровня, при котором они могут использовать Интернет в качестве инструмента причинения вреда. Соединение физической атаки с успешной кибер атакой может привести к поистине ужасающим последствиям.

Все мировое сообщество признает опасность киберпреступности, ее трансграничный характер и невозможность решения этого вопроса, а также проблемы обеспечения информационной безопасности силами одного государства или международной организации.[[21]](#footnote-21) Решение этих проблем возможно только при активном сотрудничестве в принятии необходимых технических мер, выработке единого законодательства. ОЭСР, Совет Европы, Европейский Союз, ООН и Интерпол - эти европейские организации играют важную роль в координации международных усилий, построении международного сотрудничества в сфере борьбы с преступлениями в информационной среде. Так, например, первое всестороннее исследование вопроса киберпреступности и уголовно-правовых мер по борьбе с ней было предпринято Организацией экономического сотрудничества и развития в период с 1983 по 1985 гг. В 1995 году был опубликован «Справочник ООН по предотвращению и контролю преступности, связанной с компьютерами», который исследует явление компьютерной преступности, анализирует уголовное и процессуальное право в области обеспечения информационной безопасности, а также возможность международного сотрудничества в этой сфере.

Плодом многолетних усилий Совета Европы стала Конвенция Совета Европы по киберпреступности, принятая в Будапеште 23 ноября 2001 года. Это один из важнейших документов, регулирующих правоотношения в сфере глобальной информационной компьютерной сети и пока что единственный документ такого уровня. Кроме того, включение в процесс подготовки данного документа Канады, Японии, ряда стран Южной Америки и США означало, что Конвенция пересекла границы Европы. В 2004 г. количество стран, подписавших Конвенцию, увеличилось до 37. Конвенция обязывает государства расширять трансграничное сотрудничество в сфере обеспечения кибербезопасности. В настоящее время Конвенция стала мировым стандартом для международного сотрудничества в сфере обеспечения кибербезопасности.

Это лишь несколько примеров конструктивной деятельности европейских организаций в сфере обеспечения информационной безопасности и борьбы с киберпреступностью, которых можно привести великое множество. Однако, к сожалению, пока отсутствуют комплексные исследования о вкладе азиатских государств в борьбу с новой угрозой, равно как и нет фундаментальных исследований о вопросах информационной безопасности и киберпреступности в этих государствах.

Последние несколько лет для Азиатско-Тихоокеанского региона прошли под знаком значительного экономического роста, политических трансформаций и всевозможных социальных изменений. Неотъемлемой частью социально-экономического роста региона является динамичное развитие информационно-коммуникационных технологий и киберпространства. [[22]](#footnote-22)Как и во всем мире значимость киберпространства, как инструмента политического и социального выражения, в азиатских странах необычайно велика. Однако отличительной особенностью региона является существенное «цифровое»неравенство[[23]](#footnote-23) – различие в уровне информационно-технологического развития между его странами. Наиболее компьютеризированные страны региона – Японию (79.1%), Южную Корею (84.1%) и наименее компьютеризированные страны, такие как Мьянма (1.1%) и Камбоджа (4.9%) разделяет пропасть.

Еще одна особенность региона заключается в том, что в основном преобладают нелиберальные режимы. Правительства государств с авторитарным режимом имеют больше возможностей ограничить доступ граждан к сетевой информации. Поэтому в таких странах, как Вьетнам, Китай, Мьянма интернет-пользователям запрещено посещать сайты, которые содержат информацию, не прошедшую «модерацию» государством. В основном это касается материалов тех сайтов, которые противоречат реализуемому государством политическому курсу. Китай активно взаимодействует с транснациональными корпорациями (Yahoo и Google), по вопросам ограничения доступа китайских граждан к некоторым «неугодным» международным сайтам. Филиппины и Таиланд, однако, имеют относительно открытый доступ к сетевой информации. Стоить отметить, что уровень социально-экономического развития отдельных стран региона негативно влияет на их способность формировать эффективные системы «модерации» сетевой информации. Таким образом, транснациональные методы борьбы с угрозами, с одной стороны, ограничивают для граждан восточноазиатских стран доступ к информации, а с другой являются эффективным средством предотвращения киберугроз.

Культурно-цивилизационные и исторически сложившиеся традиции отдельных стран региона также оказывают значительное влияние на борьбу с киберугрозами.

В странах региона значительно различаются меры наказания за совершение киберпреступлений. Так, в Мьянме и Китае строгость наказания достигает крупных штрафов или даже длительных сроков лишения свободы. Во Вьетнаме за просмотр запрещенных сайтов как национальных, так и зарубежных, предполагается наказание виде тюремного заключения или штрафа. В других более либеральных странах в качестве наказания обычно назначается штраф или конфискация компьютерного оборудования; однако, в зависимости от тяжести совершенного преступления, также может быть назначен тюремный срок.

Со все большим развитием информационно-коммуникационных технологий растет и необходимость в проведении политики, регулирующей и ограничивающей деятельность в киберпространстве. Все больше правительств региона замечают недостатки внутренней политики и законодательства в этом вопросе, сдерживающим фактором для построения конструктивного сотрудничества в сфере киберпространства является тот факт, что регион представлен государствами, сильно отстающими или в формировании, или осуществлении политики, нацеленной на киберпространство.

За 2013-2015 годы деятельность правительственных и бизнес кругов в сфере борьбы с киберугрозой показала положительную динамику. Несмотря на разный уровень информационно-технического развития, каждая из стран региона тем не менее осознает, что киберпространство – это зона риска. В связи с этим Япония, Индия и Сингапур полностью обновили или запустили новую политику в отношении обеспечения кибербезопасности; Папуа Новая Гвинея и Камбоджа начали разработку нового законодательства, ограничивающего киберпреступность, Австралия заявила о создании Австралийского Центра Кибербезопасности (ACSC)[[24]](#footnote-24).

Как уже было сказано выше, для многих стран региона, например, Мьянмы, Папуа Новой Гвинеи, Камбоджи, главным препятствием на пути к достижению, так называемой «кибер зрелости» [[25]](#footnote-25)по-прежнему являются недостаточная развитость инфраструктуры, а также отсутствие поддержки государства. Разрыв в уровне компьютеризации между городом и деревней в этих странах продолжает быть серьезной помехой на пути к кибер зрелости. Нехватка ресурсов, а также слабая законодательная поддержка существенно ослабляют Филиппины, Малайзию, Индонезию и Таиланд в этой сфере.

Сравнительно сильные кибер игроки региона также сталкиваются с различными трудностями. В Китае, обладающем колоссальным техническим превосходством, практически полностью отсутствует политика по борьбе с киберпреступлениями. Для Сингапура серьезной проблемой является жесткий государственный надзор и цензура. Южная Корея, страна с одним из высочайших показателей уровня проникновения Интернета, сталкивается с серьезной угрозой внешних кибер атак, что вынуждает ее концентрировать все усилия на защите своего киберпространства. В Японии же обновленная политика обеспечения информационной безопасности государства не получает достойного воплощения в связи отсутствием согласованности в действиях правительства и префектуральных властей.

Большинство правительств Азиатско-Тихоокеанского региона ставят приоритетной задачей своей политической деятельности проблему информационной безопасности и кибер преступлений. За период 2013-2015 гг. во многих странах региона произошли коренные изменения в рамках политики по отношению к кибер пространству. На передовой этих изменений стояли Индия и Япония, каждая из стран представила впечатляющую подготовительную документационную базу, связывающую воедино деятельность всех организаций и отделов, отвечающих за обеспечение кибер безопасности. В арьергарде находятся Камбоджа, Мьянма, Филиппины, Таиланд, Новая Гвинея и Индонезия - в этих странах кибер политике пока не уделяется должного внимания.

Азиатско-Тихоокеанский регион активно участвует в диалоге по вопросам обеспечения безопасности киберпространства, а также его регулирования. На макрорегиональном уровне страны Азиатско-Тихоокеанского региона объединяют усилия в рамках таких организаций, как АСЕАН и АТЭС. В рамках АСЕАН выделяется два основных направления сотрудничества по вопросам обеспечения безопасности киберпространства: всеобщие усилия по усовершенствованию сетевых возможностей региона и выработка общих механизмов по защите регионального киберпространства от транснациональных и террористических угроз. Первым шагом к налаживанию ситуации в регионе можно считать состоявшийся в 1999 г. в Маниле саммит, целью которого было решение вопроса о комплексном развитии инфраструктуры, необходимой для интеграции АСЕАН в интернет-пространство, преодоления цифрового разрыва, создания единого киберпространства. Результатом стало подписание странами АСЕАН в 2000 году Рамочного соглашения по развитию интернет-технологий, которое стало своеобразным плацдармом для дальнейшего углубления сотрудничества в регионе.

Далее, в сентябре 2003 г. Министерством АСЕАН по телекоммуникациям и информационным технологиям (TELMIN) была принята Сингапурская декларация, которая способствовала подписанию некоторыми странами двусторонних и многосторонних соглашений по развитию единого интернет-пространства. В регионе была открыта сеть учебных центров по ИКТ для оказания помощи малым и средним предприятиям; был разработан ряд совместных проектов по развитию в регионе нормативно-правовой базы в соответствующей сфере. Стремление АСЕАН укрепить сетевые взаимодействия и развивать ИТ-возможности способствовало привлечение Китая в процесс формирования новых сетей ИКТ в рамках АСЕАН+1. Япония и Южная Корея также были вовлечены в этот процесс в рамках АСЕАН+3. Данные мероприятия выступили в качестве катализатора для более тесного сотрудничества стран внутри региона. В 2004 г. Форум АСЕАН вынес решение о создании регионального механизма по борьбе с кибертерроризмом. В октябре 2007 г. в Южной Корее прошел Саммит по кибертерроризму, с целью обмена информацией между членами АСЕАН. В 2007 г. в рамках АСЕАН была принята программа подготовки кадров интернет-полиции (англ. ASEANAPOL).

В обеспечении информационной безопасности региона важнейшую роль играет APCERT[[26]](#footnote-26) – специальная группа реагирования на чрезвычайные ситуации в информационном компьютерном пространстве в Азиатско-Тихоокеанском регионе. APCERT является частью глобальной системы CERT, ячейки которой расположены по всему миру. CERT - общее название для групп специалистов по информационной безопасности, занимающихся сбором информации о системах информационной безопасности, инцидентах ее нарушения, их классификацией и нейтрализацией. Организация также известна под названиями Центр экстренной компьютерной готовности или центр реагирования на инциденты нарушения компьютерной безопасности[[27]](#footnote-27).

История появления организации тесно связана с кибер угрозой информационной безопасности, первой из них стала проблема сетевых червей[[28]](#footnote-28). Первая такая программа попала в интернет в ноябре 1988 года, «червь Морриса» парализовал нормальное функционирование узлов сети. Для борьбы с программой и для устранения ущерба, нанесенного в сети, приказом правительства США в университете Карнеги-Меллон[[29]](#footnote-29) была сформирована первая команда CERT. В дальнейшем этой аббревиатурой стали пользоваться все подобные объединения. Команда CERT из университета Карнеги-Меллон выполняет роль координационного центра для все команд CERT на территории США.

На территории ЕС большинство групп CERT создавались силами университетов или крупных IT-компаний. Роль координационного центра CERT на территории Европейского Союза выполняет общеевропейская организация TF-CSIRT[[30]](#footnote-30). Эта организация запустила форум FIRST – форум центров (команд) реагирования на компьютерные инциденты Forum of incident response and security teams) для проведения совещаний по вопросам взаимодействия команд CERT по всему свету.

Что касается Азиатско-Тихоокеанского региона, то здесь представлены как центры CERT большинства стран по отдельности, так и APCERT – организация, объединяющая деятельность центров экстренного реагирования на компьютерные инциденты Азиатско-Тихоокеанского региона, а также форум. В марте 2002 года по инициативе и при поддержке правительства Японии прошла встреча, на которой было принято решение о формировании APCERT. И спустя год, в феврале 2003 года после подписания странами-учредителями соглашения организация APCERT официально начала свою деятельность.

Главной целью создания APCERT стала необходимость улучшения ситуации в регионе в сфере обеспечения информационной безопасности и отражения кибер угрозы. Так как страны региона находятся на разном уровне информационно-технического развития, и некоторые государства просто не в состоянии справиться с угрозой своими силами, достичь успеха можно только объединив усилия.

На настоящий момент в APCERT входит 28 команд (центров) из 21 страны – Австралия, Бангладеш, Бруней, Китай, Индия, Китайский Тайвань, Гонконг, Индонезия, Япония, Корея, Лаос, Мьянма, Монголия, Макао, Малайзия, Новая Зеландия, Сингапур, Шри-Ланка, Таиланд, Вьетнам. От Австралии – 2 команды – AusCert, CERT Australia. От Китайской Народной республики – 2 команды – CCERT, CNCERT/CC. От Гонконга – 2 команды – GovCERT.HK, HKCERT. От Индонезии – 2 команды – ID-CERT, IDSIRTII/CC. От Шри-Ланки, Китайского Тайваня, Монголии – также по 2 команды.

Вышеперечисленные государства являются действующими членами APCERT. Однако регламентом данной организации предусмотрена еще одна форма членства – через оказание поддержки организации. К ним относятся организации, которые могут оказать техническую поддержку APCERT и функционированию ячеек CSIRT/CERT. На настоящий момент три крупные корпорации поддерживают организацию - Корпорация Bkav – основанная в 1995 году одна из крупнейших фирм в сфере антивирусных программ, сетевой и мобильной безопасности, представлена в более чем 100 странах мира; компания Dell secure Works, Microsoft Corporation.

Председателем APCERT является CERT Австралии, заместителем председателя - Центр экстренного компьютерного реагирования Малайзии. Существует также Руководящий Комитет, который отвечает за общую рабочую стратегию, руководящие принципы деятельности и прочие соответствующие вопросы, затрагивающие функционирование APCERT как единой организации. В Руководящий Комитет входят группы CERT Австралии, Китая, Японии, Кореи, Макао, Малайзии и Китайского Тайваня. Секретариат APCERT обеспечивает общие точки соприкосновения в работе стран-участниц, также ответственен за проведение ежегодной конференции APCERT, осуществляет руководство членами организации и группами, желающими в нее вступить, а также несет ответственность за официальный сайт организации. Должность секретаря бессменно занимает CERT Японии.

В структуре APCERT на сегодняшний день действует 4 рабочие группы: Группа информационного обмена, основанная в 2011 году (осуществляет фильтрацию информации, которой обмениваются группы членов APCERT); Рабочая группа членства, основанная в 2011 году (рассматривает критерии/виды членства в организации, расширяет или исключает их по мере надобности); Рабочая группа политики, процедур и руководства, основанная в 2013 году (разрабатывает новые подходы и методы управления организацией); Рабочая группа Цубамэ, основанная в 2009 году силами JPCERT/CC – ячейки организации в Японии.

Своей главной целью APCERT называет поддерживание надежных контактов между группами экспертов по компьютерной безопасности в Азиатско-Тихоокеанском регионе для повышения осведомленности и компетентности в области в отношении инцидентов нарушения информационной безопасности.

Как можно увидеть, Азиатско-Тихоокеанский регион крайне неоднороден – богатство соседствует с нищетой, свобода слова – с жесткой правительственной цензурой, технический прогресс – с нехваткой инфраструктуры. Составить общее впечатление о ситуации в сфере информационной безопасности и борьбы с киберпреступностью в регионе невероятно сложно. И для того, чтобы это сделать, необходимо тщательно изучить положение дел в каждой из стран региона. В рамках следующей главы будет предпринята попытка рассмотреть ситуацию в четырех самых развитых странах региона – Индии, Китае, Южной Корее и Японии. Особое внимание будет уделено статистическим данным об уровне проникновения Интернета, основному законодательству в сфере обеспечения кибербезопасности, а также роли ячеек организации CERT в четырех странах.

# Глава вторая

## 2.1.Проблема информационной безопасности в Индии

## 

В современной научной литературе применительно к Индии экономисты, политологи, социологи все чаще употребляют слово «пробуждение». Использование подобного термина вполне обосновано – резкий скачок в экономическом развитии уже к 2010 году превратил страну в четвертую крупнейшую экономику мира после США, Китая и Японии. И сегодня после десятилетий «сна», Индия являет самые высокие показатели темпа роста в мире; индийский рынок, преимущественно еще закрытый, привлекает огромное количество иностранных инвесторов. Бурное развитие экономики дало необходимый толчок для трансформации информационной инфраструктуры, и сегодня специалисты IT сферы прогнозируют, что в ближайшем будущем Индия превратится в нового Интернет-гиганта[[31]](#footnote-31).

Подобно наиболее развитым странам региона, да и всего мира, Индия испытала на себе все положительные стороны информационно-технологического развития, но также, как и прочие государства, столкнулась с качественно новой угрозой преступлений против информационной безопасности, кибертерроризма.

Интернет проник в Индию в 1995 году, однако в течение первых десяти лет сеть не пользовалась большой популярностью. Начиная с 2005 года число пользователей сети Интернет начало неуклонно расти, а на 2014 г Индия стала третьей страной в мире по числу пользователей – более 198 млн человек. 38% пользователей – в возрасте от 25 до 34 лет. Согласно исследованию, проведенному силами группы CERT в Индии, в среднем пользователь сети в Индии проводит 5.1 часов в Интернете. Самым популярным сайтом является Facebook, на него приходится 53% от общей посещаемости сайтов в Интернете. Прочие популярные социальные сети – Google+, Twitter, LinkedIn. Социальные медиа и общение в социальных сетях необычайно популярно через мобильные устройства – на 2014 год число активных пользователей приложений типа WhatsApp достигло 70 миллионов человек – в два раза больше, чем в январе того же года. По данным на январь 2015 года, большинство пользователей мобильного интернета – городские жители. Еще одним видом популярной интернет активности в Индии является интернет-шоппинг – 24.4% жителей активно пользуются этой услугой. [[32]](#footnote-32)

Растущая популярность интернет-услуг вполне закономерно привела к резкому увеличению числа совершаемых киберпреступлений. По данным за 2014 год, было зафиксировано 9622 случаев киберпреступлений, попадающих под юрисдикцию акта об информационных технологиях Индии – что на 69% больше по сравнению с прошлым годом, и совершенно ясно, что пользователи интернета в Индии в опасности[[33]](#footnote-33).

Одной из специфических особенностей индийского киберпространства является гендерное неравенство среди его пользователей – 61% - мужчины, в то время, как на долю женщин приходится всего лишь 39%.[[34]](#footnote-34) С одной стороны, безусловно, социальные сети открывают поистине безграничные возможности для общения и социализации. В целом, Интернет сделал жизнь женщин Индии значительно проще – популярность сервисов по онлайн оплате счетов, налогов; онлайн шоппинга – тому доказательство. Киберпространство предоставляет женщинам Индии шанс отстаивать идеи равенства и эмансипации даже в условиях закрытого общества. Для многих женщин-пользователей киберпространства общение в социальных сетях с единомышленниками, возможность делиться своими переживаниями и опытом со всем миром – единственная отдушина в жизни, полной бесконечных ограничений.

Но с другой стороны, в киберпространстве женщины Индии подвергаются преследованию, нападкам, домогательствам, защититься от которых они не в состоянии.

Возникает вопрос, чем же женщины Индии так отличаются ото всех женщин-пользователей мирового киберпространства? Индия – преимущественно патриархальная и ортодоксальная страна, где, если женщина подверглась насилию, вина за это будет возложена на нее. Честь семьи, главным образом, связана с порядочностью женщин этой семьи, что ставит их в уязвимое положение. В Индии, по сравнению с мужчиной, женщина-жертва не имеет права голоса. И жертвы онлайн преступлений исключением не являются. Уже существуют прецеденты, когда брак был расторгнут по причине того, что женщина стала жертвой домогательств в сети. Семья мужа не смогла стерпеть тени, брошенной на ее имя.[[35]](#footnote-35) Также необходимо отметить, что женщины-пользователи сети в Индии, в отличие от жительниц европейских стран, никак не защищены государством.

Официальная позиция правительства Индии по вопросам информационной безопасности в киберпространстве и борьбы с киберпреступностью отражена в Национальной программе обеспечения кибербезопасности 2013 года.

Киберпространство рассматривается как сложная система, включающая в себя взаимодействия пользователей, программное обеспечение, услуги, которые поддерживаются информационными технологиями, устройствами и сетями по всему миру.[[36]](#footnote-36)

Информационные технологии (IT) – сфера деятельности, которая целиком и полностью расположена в киберпространстве. Для индийской экономики она стала главным катализатором роста. Помимо этого, сектор информационных технологий положительно влияет на жизнь населения Индии, внося существенный вклад в социальную, экономическую сферы, предоставляя рабочие места и т.п. Именно развитие этого сектора во многом сформировало современное представление об Индии, как о глобальном игроке, поставщике технологических решений в мире и в регионе, источнике IT бизнес услуг[[37]](#footnote-37). Главным инициатором внедрения информационных технологий в сферы здравоохранения (телемедицина, удаленные консультации и т.п.), образования (e-learning, виртуальные занятия и т.п.), финансов (мобильный банк, переводы) и т.п. является государство.

Киберпространство сегодня – среда, используемая различными группами пользователей: горожанами, бизнесменами, военными, правительственными структурами, СМИ. Кибератаки, целью которых является инфраструктура или экономическое благополучие населения, может нанести серьезный урон ресурсам государства и подорвать уверенность в государственных структурах у гражда.[[38]](#footnote-38) Крупные киберпреступления могут нарушить работу правительства, частного и государственного секторов. Под угрозой могут оказаться жизни граждан, экономическая и государственная безопасность. Примерами кибер угроз частным лицам могут быть кража личной информации, финансовое мошенничество, хакерство, атаки на мобильные устройства, фальсификация электронных сертификатов, отказ в доступе, утечка данных и проч. Обеспечение защиты информационной инфраструктуры и сохранение конфиденциальности, целостности и доступности информации в киберпространстве – первоочередные задачи правительства Индии.[[39]](#footnote-39)

Обеспечение кибербезопасности населеня – задача, усложняющаяся день ото дня. Круг пользователей и провайдеров,нуждающихся в поддержке необычайно широк – от рядовых пользователей, малых и средних предприятий, вплоть до государственных структур. Национальная программа обеспечения кибербезопасности 2013 года служит своего рода куполом, под которым объединена вся деятельность, имеющая отношение к киберпространству.[[40]](#footnote-40)

Главный замысел Программы заключается в создании надежного и безопасного киберпространства для горожан, бизнесменов и правительственных структур.

Для его осуществления необходимо прежде создать систему предотвращения и ответа на киберугрозы, уменьшить число уязвимых точек системы и свести к минимуму ущерб, наносимый киберпреступлениями, путем согласованной деятельности институтов, пользователей, процессов, технологий.

Министерство Коммуникаций и информационных технологий Индии выделило следующие первоочередные задачи[[41]](#footnote-41):

Создание системы проектирования политики безопасности и стимулирующих мер для соблюдения глобальных стандартов безопасности;

Укрепление нормативной базы по обеспечению безопасности киберпространства;

Создание механизма получения стратегической информации об угрозах информационно-технологической инфраструктуре национального и отраслевого уровня в режиме 24x7;

Подготовка 500,000 квалифицированных специалистов в сфере обеспечения кибербезопасности в ближайшие 5 лет; разработка эффективной программы повышения квалификации и профессиональной подготовки в данной сфере;

Обеспечение конфиденциальности данных граждан и уменьшение экономических потерь из-за кражи данных;

Обеспечение эффективного предупреждения, расследования и уголовного преследования актов киберпреступности и повышения потенциала правоохранительных органов посредством соответствующих законодательных мер. [[42]](#footnote-42)

Как можно заметить, Программа достаточно туманно обозначает основные направления государственной деятельности в сфере обеспечения национальной кибербезопасности. Главный акцент сделан на укрепление нормативно-правовой базы в данной области, однако, как на момент создания Программы 2013, так и на настоящий момент главным законом в сфере регулирования вопросов киберпреступности и кибертерроризма в Индии остается Акт об информационных технологиях от 2000 года[[43]](#footnote-43).

Закон применяется на всей территории Индии. Представители других национальностей также попадают под юрисдикцию этого закона, если в преступлении был использован компьютер или сеть, расположенные в Индии. Акт определяет содержание понятия «киберпреступления» и предписывает меру наказания за них. Также этим законом установлен апелляционный суд по кибер вопросам, для разрешения споров, с ним связанных.

Акт предусматривает наказание за следующие виды преступных деяний[[44]](#footnote-44):

За злонамеренное изменение программных средств и документов системы – предусмотрено наказание в виде лишения свободы сроком до 3 лет и/или же штраф в размере до 200 000 рупий – статья 65;

За взлом компьютерной системы – предусмотрено наказание в виде лишения свободы сроком до 3 лет и/или штраф в размере до 500 000 рупий – статья 66;

За укрывательство краденого компьютерного оборудования – предусмотрено наказание в виде лишения свободы сроком до 3 лет и/или штраф в размере до 100 000 рупий – статья 66В;

За использование паролей другого пользователя – предусмотрено наказание в виде лишения свободы сроком до 3 лет и/или штраф в размере до 100 000 рупий – статья 66 С;

За мошенничество с использованием компьютерных ресурсов – предусмотрено наказание в виде лишения свободы сроком до трех лет и/или штраф в размере до 200 000 рупий – статья 66D;

За опубликование частных фотографий других пользователей без их ведома – предусмотрено наказание в виде лишения свободы сроком до трех лет и/или штраф в размере до 200 000 рупий – статья 66Е;

За совершение акта кибертерроризма, под которым подразумевается получение незаконного доступа к защищенной системе или ввод в систему данных, нарушающих ее функционирование, с намерением подвергнуть угрозе единство, целостность, суверенитет или безопасность Индии – предусмотрено пожизненное лишение свободы – статья 66F;

За распространение порнографии – предусмотрено наказание в виде лишения свободы сроком до 7 лет и/или штраф в размере до 1 000 000 рупий – статья 67А;

За опубликование материалов, содержащих детскую порнографию или насилие над детьми – предусмотрено наказание в виде лишения свободы сроком до 5 лет и/или штраф в размере до 1 000 000рупий – статья 67В;

За отказ подчиняться приказам Инспектора Аттестационной организации, а также отказ в дешифровке информации по его приказу – предусмотрено наказание в виде лишения свободы сроком до 7 лет также возможен штраф – статьи 68,69;

За попытку получения доступа к «защищенной системе» - предусмотрено наказание в виде лишения свободы сроком до 10 лет и/или штраф – статья 70;

За предоставление заведомо ложных данных – лицо, предоставляющее неверные данные или скрывающие материалы от Инспектора или от Аттестационной Организации с целью получения лицензии или сертификата электронной цифровой подписи, подвергается наказанию в виде лишения свободы сроком до 3 лет и/или штрафа в размере до 100 000 рупий – статья 71.

Акт об Информационных Технологиях был пересмотрен несколько раз с 2000 года, серьезные поправки были внесены в 2008 году – была добавлена секция 66 А – предусматривающая наказание за рассылку «оскорбительных сообщений», также была добавлена секция 69, дающая властям право на «перехват, контроль и расшифровку любой информации с использованием любого ресурса». Также были внесены меры наказания за детскую порнографию, кибертерроризм.[[45]](#footnote-45)

Однако он по-прежнему подвергается критике за неспособность прекратить злонамеренную активность в сети. Согласно отчету Norton’s Cyber Crime за 2013 год, 66% взрослого населения, пользующегося интернетом стало жертвами киберпреступлений, однако заключенных под стражу преступников по-прежнему единицы[[46]](#footnote-46). Акт об Информационных Технологиях также дает индийскому правительству право цензурировать широкий круг тем и ресурсов, так, например, был заблокирован Twitter и другие сайты. То есть, по сути, правительство Индии использует законодательство в сфере обеспечения безопасности киберпространства не с целью ограничить киберпреступность в стране, а для того чтобы усилить государственный контроль в данной сфере жизни общества.

Ситуация в Индии усугубляется еще и тем, что отношение населения к лицам, совершающим преступления в киберпространстве, в целом, спокойное, даже положительное. На Facebook даже существуют группы, такие как «Hire Professional Hackers in India», которые открыто обещают предоставить услуги по взлому почты и слежки за коллегами и работодателями.[[47]](#footnote-47)

Хакеров Индии принято относить к «белым хакерам», даже несмотря на то, что группы хакеров, например, «Cyber Army», по политическим мотивам производили атаки на Пакистан и Бангладеш. Благодаря своей репутации специалистов в сфере информационных технологий и глубокому пониманию уязвимостей киберсистемы хакеры в Индии пользуются большим авторитетом. Публикуются списки так называемых этичных хакеров[[48]](#footnote-48), главные представители которых Анкит Фадиа и Рахул Тьяги - весьма влиятельные фигуры в индийском киберпространстве. Они выпускают книги с советами по обеспечению информационной безопасности, шоу, проводят обучающие семинары для желающих пройти сертификацию этичного хакера и готовят специалистов по информационной безопасности.

Однако далеко не всех хакеров Индии можно отнести к категории этичных. Специалисты по международной информационной безопасности считают индийских хакеров столь же опасными, как и китайских кибер бойцов, и сигнализируют об их вовлеченности в международный шпионаж и кражи интеллектуальной собственности[[49]](#footnote-49). Индийских хакеров впервые обвинили в международном кибершпионаже, после серии кибератак, получившей название «Operation hangover» была проведена по отношению как к гражданским корпорациям, так и к государственным – Холдинг Порше, Авиалинии Дельта, ряду американских компаний (The Chicago Mercantile Exchange и др.).

Позиция индийского населения по вопросам безопасности киберпространства видится несколько странной – при одобрительном, в общем-то, отношении к противозаконной хакерской деятельности, отношение к официальным организациям, усилия которых направлены на обеспечение информационной безопасности киберпространства, скорее, негативное.

Достаточно ярко это проявляется на примере ячейки организации CERT в Индии – ее деятельность, а точнее, спектр полномочий является предметом оживленных споров и протестов. CERT-In действует с января 2004 года. Полномочия центра распространяются на киберпространство Индии, все киберсообщество страны находится под его наблюдением. CERT-In предоставляет услуги организациям государственного, публичного и частного секторов, а также индивидуальным пользователям. Внутренняя функция подразумевает работу с антиправительственными сайтами, их блокировка и устранение – что как раз и вызывает массовое недовольство. CERT-In – открытая организация, поэтому не скрывает факт тесного сотрудничества с правительством Индии, а также Департаментом Электронных и Информационных Технологий, Министерством Информационно-Коммуникационных технологий. В лице CERT-In граждане Индии видят лишь еще один орган государственной цензуры, призванный ограничить свободу слова и самовыражения.

Однако в действительности, все обстоит совсем наоборот. Главная цель организации состоит в обеспечении безопасности киберпространства Индии. Основные направления деятельности CERT-In заключаются в предотвращении происшествий, реагировании и обеспечении высокого уровня защиты. Акт об Информационных технологиях от 2000 обязал CERT-In служить в качестве национального агентства, функции которого сводятся к следующему: сбор, анализ информации об инцидентах нарушения кибербезопасности; прогнозирование и предупреждение инцидентов нарушения кибербезопасности; экстренное реагирование на произошедший инцидент; координирование ответной деятельности; выпуск брошюр, предписаний, рекомендаций по обеспечению информационной безопасности и защиты от киберпреступлений, а также отчетов о деятельности центра.

За период с января по декабрь 2014 года CERT-In успешно разрешил более 130000 инцидентов нарушения кибербезопасности; основные типы угроз, с которыми центр столкнулся были: спам (85659 случаев), вредоносное программное обеспечение (7286 случаев), вирусы и черви (4307 случаев), повреждение сайта (25037 случаев) и проч. Согласно отчету за 2014 год, в незаконной кибер деятельности были выделены следующие тенденции: широкое распространение в сети получила вредоносная программа «D4reI Dev» иначе «DareDevil», атакующая системы общественного транспорта. Программа оказывает вредоносное воздействие главным образом на автоматы покупки билетов, банкоматы. Успешное проникновение в систему дает взломщику полный контроль над ней; распространилась вредоносная программа для кражи производственной информации «Havex». CERТ-In отслеживает нарушения в работе веб-сайтов и разрабатывает подходящие меры по укреплению их защиты. За 2014 год было отслежено и исправлено 25037 поврежденных сайтов.

Еще одно направление деятельности – отслеживание открытых промежуточных серверов (proxy server), которые являются популярным каналом для распространения спама и вредоносных программ. За 2014 год было найдено 2408 открытых промежуточных серверов. А также деятельность по отслеживанию и уничтожению ботов и ботнетов[[50]](#footnote-50) в индийском киберпространстве. Существенную помощь в обнаружении бот-сетей оказывают интернет провайдеры Индии, именно благодаря сотрудничеству с ними в 2014 году были отслежены такие бот-системы, как Baldabindi,Jenxus, Ganeover/ZeuS P2P.

CERT-In исполняет роль головного офиса организации на территории Индии, действуя согласованно с директорами по информационной безопасности секторальных ячеек CERT в сферах Защиты, Финансов, Энергетики, Транспорта, оказывая необходимую поддержку и консультирование их деятельности.

Силами CERT-In была организована система сканирования интернет трафика по всей стране, необходимая для отражения и прогнозирования кибер-атак. В настоящее время многие организации добровольно предоставляют центру информацию о своем интернет трафике, с целью построения эффективной системы защиты.

CERT-In организовывает обучающие семинары и программы для служащих финансовых и банковских секторов, системных администраторов для повышения уровня подготовленности к инцидентам нарушения кибербезопасности. В течение 2014 года было проведено 22 обучающих семинара, на которых подробно разбирались вопросы обеспечения безопасности различных компьютерных информационных систем, мобильного интернета.

CERT-In выпускает ежемесячный бюллетень о кибербезопасности, содержащий информацию об инцидентах нарушения кибербезопасности за прошедший месяц, Рекомендации по обеспечению безопасности для всех пользователей, включающие в себя описание наиболее эффективных способов защиты мобильных устройств, ПК, кредитных карт, персональной информации и проч.

В рамках международной деятельности CERT-In сотрудничает с ячейками CERT других стран региона с целью облегчения обмена данными и технологиями в сфере обеспечения информационной и кибербезопасности региона. CERT-In входит в FIRST – Forum of Incident Response and Security Teams, APCERT, Anti-Fishing Working Group (APWG). Также центр поддерживает отношения с US-CERT. Для дальнейшего укрепления сотрудничества в решионе был подписан Меморандум о взаимопонимании с Агентством Интернет Безопасности Кореи (KISA) в январе 2014 года.

Индия активно участвует в двусторонних и многосторонних дискуссиях по проблеме информационной и кибербезопасности с широким кругом организаций, включая ЕС, АСЕАН, APCERT. Индия оказывает поддержку менее развитым в кибер отношении странам региона. В январе 2015 года Индия принимала Конференцию по Кибербезопасности стран АСЕАН, на открытии которой Секретарь министерства иностранных дел выступил с заявлением, что Индия верит в то, что киберпространство должно регулироваться своими законами, которые, однако, не должны нарушать свободу деятельности и самовыражения пользователей.

Несмотря на положительную динамику в сфере кибербезопасности, которую можно наблюдать с 2014 года, вялость и бездействие властей привело к тому, что полноценной стратегии по обеспечению кибербезопасности в стране на данный момент нет. Законодательство, регулирующее данную область, устарело и не отвечает современным реалиям киберпространства.

Материальная база и устройства сферы обеспечения кибербезопасности используются как инструменты государственной цензуры, а уровень проникновения интернета в обществе продолжает оставаться очень низким.

Усилия индийского правительства по борьбе с киберугрозой на данный момент практически сошли на нет. Программа национальной кибер безопасности 2013 года достаточно туманно обрисовывает меры по борьбе с киберпреступностью, а данных о разработке новой программы пока нет.

За 2014-2015 годы в индийское законодательство в сфере урегулирования вопросов информационной и кибербезопасности не было внесено никаких изменений. Существенная работа должна быть проведена по обновлению и упрощению законодательства.

## 2.2. Проблема информационной безопасности и кибертерроризма в Китае

Если обратиться к истории формирования современной информационной инфраструктуры Китая, стоит отметить, что процессы компьютеризации Поднебесной и распространения Интернета протекали значительно позднее, нежели в странах Запада, в силу социально-экономической и политической ситуации в Китае в 80-е годы. [[51]](#footnote-51)Сеть Интернет впервые появилась в Китае в 1994 году, и в последующие годы число пользователей постоянно возрастало; в настоящее время Китай занимает лидирующие положение в мире в этой сфере.

По данным на декабрь 2015 года, на территории Китая зарегистрировано 688.26 млн пользователей сети Интернет, что равняется одной пятой от мирового числа пользователей киберпространства. Уровень проникновения Интернета в Китае достаточно высок – 42.1%. Число пользователей мобильного Интернета к 2012 году достигло отметки 356 миллионов человек.[[52]](#footnote-52)

Самым популярным видом онлайн деятельности является мгновенная переписка - с 415 млн пользователей. По данным опроса, проведенного силами CNCERT/CC в 2014 году, среднестатистический пользователь сети Интернет в Китае в течение недели посвящает 13 часов просмотру видео роликов, 4.5 часа – прослушиванию музыки, 4.5 часов – онлайн играм; что примечательно – определить хотя бы приблизительно, сколько времени пользователь отводит онлайн общению, не представляется возможным.[[53]](#footnote-53)

В условиях столь бурного развития Интернета, его проникновения во все сферы жизни общества, вполне ожидаемые изменения претерпевает и преступная деятельность в Китае. В частности, в сфере преступлений против информационной безопасности в последнее время наметились новые тенденции, главной из которых стала так называемая «интернетизация» преступлений. Суть этого феномена заключается в том, что растет количество преступлений, совершаемых в сети Интернет или с ее помощью. За период с января по декабрь 2014 года в CNCERT было направлено 56.2 тысячи жалоб на акты киберпреступности, что на 77.3% превышает показатель 2013 года. Большинство обратившихся стали жертвами фишинга[[54]](#footnote-54) 32.1%, вредоносной активности на веб-сайтах (16.3%). Наибольшее количество жалоб поступило в связи с уязвимостью систем защиты 36.4%.

На мировой арене в сфере обеспечения информационной безопасности и борьбы с киберпреступностью Китай не пользуется ни доверием, ни популярностью. Поднебесная прочно удерживает за собой положение мирового лидера в области киберпреступности. Согласно отчету APCERT за 2015 год, Китай, вместе с Индией и Южной Кореей вошел в тройку региональных лидеров по уровню совершаемых киберпреступлений. По результатам исследования 2014-2015гг, предоставленного корпорацией «Symantec», Китай занимает вторую строчку в списке стран с наиболее высоким уровнем хакерской и хактивистской активности. Специалисты Infosec Institute сочли Китай безоговорочным лидером в сфере киберпреступлений. В отчете об основных тенденциях в области кибер угроз, предоставленного компанией Sophos, Китай назван «главным агрессором международного киберпространства».

30% всех кибер атак 2013 года и 41% кибер атак 2014 года были осуществлены хакерами из Китая или же с использованием серверов, расположенных на территории Китая. Honker Union, Javaphile, Network Crack Program Hacker и другие названия групп-участников организованной сети хакеров Китая давно стали нарицательными в сфере обеспечения кибербезопасности и зашиты от кибер преступности. Южная Корея, Япония, Индия и США выдвигают все новые и новые обвинения в совершении актов киберпреступности и кибер шпионажа; необходимо отметить также, что не только в отношении отдельно взятых группировок хакеров, но и непосредственно в адрес правительства КНР.[[55]](#footnote-55)

Именно таков наиболее распространенный образ Китая в сфере обеспечения информационной безопасности и борьбы с киберпреступностью - государство, являющее собой кибер угрозу мирового масштаба, разрушительным атакам которого невероятно сложно противостоять. Государство, в котором практически вся незаконная хакерская деятельность поставлена на службу интересам военного сектора и правительства и им же финансируется. Такой образ необычайно популярен в японских, корейских и американских медиа.

Однако существует и другой образ Китая. В работах собственно китайских специалистов, а также в данных, предоставляемых независимыми организациями CNCERT и APCERT, Китай представлен в совершенно ином свете – как государство, в котором практически полностью отсутствует национальная стратегия по защите от киберпреступности, также, как и единая законодательная база, регулирующая область обеспечения кибербезопасности; государство, чья недостаточно гибкая внешняя политика препятствует выработке эффективного механизма решения транснациональных киберпреступлений; государства, чье киберпространство весьма уязвимо.

Какой же из существующих образов Китая более точно соответствует реальности – ответить на этот вопрос отнюдь не так просто, как может показаться на первый взгляд.

Дело в том, что ситуация в Китае достаточно интересная – в стране функционирует множество государственных органов, регулирующих вопросы информационной и кибербезопасности, таких как: Министерство промышленности и информатизации КНР[[56]](#footnote-56), Министерство общественной безопасности КНР[[57]](#footnote-57), Национальная администрация по охране государственных тайн [[58]](#footnote-58)и т.д. Однако складывается впечатление, что подобное многообразие не оказывает никакого положительного эффекта, скорее наоборот, указывает на отсутствие скоординированной деятельности по этим вопросам, а также на отсутствие всеобъемлющей, постижимой национальной киберполитики.

В сфере обеспечения безопасности киберпространства и борьбы с киберпреступлениями не существует единой законодательной базы – все вопросы регулируются рядом предписаний, главными из которых являются статьи 285-287 Уголовного Кодекса Китайской Народной Республики. Кроме того, существуют: Декрет об обеспечении безопасности компьютерных информационных систем от 1994 года, Положение об административном наказании в сфере обеспечения общественной безопасности, а также Решение о поддержании Интернет Безопасности и проч.[[59]](#footnote-59)

Китайское уголовное право содержит описание 5 видов киберпреступлений: незаконный доступ, незаконное получение данных, незаконное управление компьютерной информационной системой, предоставление компьютерной программы или иных средств для незаконного получения данных или управления информационной системой, а также нарушение функционирования компьютерной информационной системы.

Незаконный доступ определяется, как незаконное проникновение в компьютерную систему в сфере Государственных дел, структур государственной безопасности, а также научных и технологических разработок.[[60]](#footnote-60)

Незаконное получение данных определяется, как незаконное проникновение в компьютерную систему, которая не относится к вышеперечисленным, или использование других способов для получения данных из компьютерной системы.[[61]](#footnote-61)

Там же дается определение предоставление компьютерных программ или иных средств для незаконного проникновения в систему и хищения данных – предоставление специально разработанных программ или средств для взлома и хищения информации.[[62]](#footnote-62)

Статья 286 определяет преступное действие по нарушению деятельности системы, как нарушение функций системы или компьютерных данных в системе, что приводит к отказу системы[[63]](#footnote-63).

В целях борьбы со всеми видами киберпреступности, лица, уличенные в преступлениях, описанных в статьях 285, 286 уголовного права Китая, несут ответственность согласно статье 312 уголовного кодекса Китая. [[64]](#footnote-64)

За незаконный взлом компьютерной информационной системы, в сферах государственных дел, науки и технологии, предусматривается наказание в виде лишения свободы до 3 лет. В случаях, когда Интернет-провайдер или рекламная компания добровольно оказывает преступным элементам техническую или финансовую поддержку, то они будут наказаны как соучастники.

Если преступное действие или ряд действий были совершены на территории Китая, применяется уголовный кодекс Китая. Если китаец за пределами страны совершает киберпреступление, высшая мера наказания за которое не превышает 3 лет, нормы уголовного кодекса могут не применяться.

Следует отметить, что сам термин «хакер» был официально добавлен в уголовный кодекс КНР лишь в 2009. По нормам Китайского уголовного права, наивысшей мерой наказания за хакерскую деятельность является тюремное заключение сроком на 5 лет. Оно применяется в случае, если хакер вмешивается в деятельность компьютерной информационной системы, изменяет ее или своими действиями приводит к разрушению системы. В 2011 году Верховный народный суд КНР и Верховная Народная Прокуратура КНР выпустили предписание о кибер преступлениях, согласно которому хакер, взломавший 20-100 компьютеров, подлежит наказанию в виде лишения свободы на срок до 3 лет. Хакеры, совершившие более тяжкие преступления, приговариваются к сроку заключения до 7 лет. [[65]](#footnote-65)

В целом, при более близком изучении законодательства КНР в сфере борьбы с киберпреступлениями, оно отнюдь не производит впечатление зрелого и тщательно проработанного.

В эпоху интернета киберпреступность становится угрозой всему мировому сообществу, так как техническая база, на которую она опирается – компьютер и Интернет – одинаково доступна во всех государствах, поэтому в большинстве своем, характеристики и направления киберпреступности во всем мире примерно одинаковы.

Китай принимает активное и последовательное участие в двусторонних и многосторонних форумах по широкому спектру вопросов, касающихся информационной и кибербезопасности, активно продвигая идею о том, что суверенитет каждого государства должен распространяться и на его киберпространство. И в таком случае, иностранное вторжение в киберпространство другого государства, любая деятельность по контролю или наблюдению за ним будет считаться недопустимой, так как это будет нарушением права на суверенитет[[66]](#footnote-66). Также Китай ратует за предоставление государству права полностью контролировать свое киберпространство. В январе 2015 года, Китай представил свой пересмотренный вариант свода «Правил поведения в области обеспечения международной информационной безопасности» в ООН, с просьбой распространить его в 69-й сессии Генеральной Ассамблеи. Китай ведет последовательную работу для достижения своего видения государственного контроля киберпространства через ООН, Международный союз электросвязи (МСЭ), форумы АСЕАН, АТЭС, APCERT и проч.

Однако, что касается международного сотрудничества по обеспечению информационной безопасности и защиты от киберпреступности в законодательной сфере, этот вопрос для Китая на сегодняшний день остается нерешенным.

В 2001 году увидела свет Будапештская конвенция по борьбе с киберпреступностью, которая за последующие 13 лет подписана не только странами Европы, но и Японией, США, Канадой и Южной Африкой. На настоящий момент Конвенция является основным документом, регулирующим международную деятельность в сфере обеспечения информационной безопасности и защиты от киберпреступности в законодательной сфере. Главной целью создания Конвенции является создание универсальной законодательной базы, способной гарантировать безопасность общества от киберпреступности. [[67]](#footnote-67)

Китай отказался присоединиться к ряду стран, признавших Конвенцию по нескольким причинам. Главной из них стал пункт 32Б Конвенции, который предполагает доступ к персональным данным граждан государства без какого-либо уведомления об этом представителей власти этого государства[[68]](#footnote-68). Фактически этот пункт позволяет иностранным спецслужбам следить за гражданами государств, подписавших конвенцию. Пункт 32Б нарушает один из основополагающих принципов политики Китая – а именно, невмешательства во внутригосударственные дела. К тому же, как отмечает Лу Вэй, глава Администрации Киберпространства КНР, Будапештская Конвенция, сформированная в 2001 году, сегодня устарела, так как в ней не учитываются новейшие реалии киберприступности.

Китай стоит особняком от международного сотрудничества на законодательном уровне борьбы с кибер угрозой. Такое положение дел не только наносит вред безопасности китайского интернет сообщества, но также превращает страну в своеобразный плацдарм для атак на компьютерные системы других государств.

В Китае также отсутствует стратегическая образовательная программа по профилю подготовки кадров для работы в сфере кибер безопасности, но некоторую инициативу в последнее время на себя взяли CERT и Министерство производства и информационных технологий. О деятельности группы CERT в Китае следует сказать отдельно, ведь именно благодаря данным, предоставляемым этой организацией, мы имеем возможность взглянуть на ситуацию в КНР под новым углом.

CNCERT/СС – неправительственный, некоммерческий центр технической поддержки и реагирования на компьютерные инциденты является главным координирующим центром деятельности всех групп реагирования на территории Китая. Был основан в 2002 году, является членом-основателем APCERT. Головной офис CNCERT расположен в Пекине; на территории 31 провинции и автономных округов действуют местные ячейки CNCERT. Основной задачей своей деятельности организация ставит укрепление национальной системы обеспечения кибербезопасности, а также предотвращение, отражение и устранение последствий угроз национальной кибербезопасности.

За период с января по декабрь 2014 года центр CERT Китая успешно разрешил 56.1 тысячу инцидентов нарушения кибербезопасности. Случаев заражения серверов и отдельных устройств вредоносными программами достигло отметки 11.1 млн, что на 2.3% меньше, чем в 2013 году. Согласно данным CNCERT 70.1 млн устройств по всему свету были заражены червем Conficker за 2014 год. Из них 8.9 млн (12.7%) зараженных серверов находились на территории Китая; 7.9% находились на территории Индии. CNCERT также ведет деятельность по отслеживанию веб-сайтов, содержащих вредоносное программное обеспечение; за 2014 год было вычислено 10 тысяч доменов, порядка 5.1 тысяч IP адресов, 115.1 тысяч ссылок, содержащих вредоносное программное обеспечение. Из 5.1 тысячи вредоносных IP адресов 52.0% были зарегистрированы за рубежом.

В рамках своих полномочий раз в год CNCERT проводит конференцию, на которой оглашаются основные результаты, достигнутые организацией за прошедший год, а также приблизительный план действий на следующий.

Также раз в год проводится Конференция по Компьютерной и сетевой безопасности в городе Шаньтоу провинции Гуандун. В 2015 году конференция прошла 28 мая, самыми популярными темами для обсуждения стали вопросы обеспечения безопасности мобильного Интернета 4 G, защиты частной информации, а также обеспечение безопасного, бесперебойного функционирования ключевых отраслей инфраструктуры Китая.

В 2014 году прошла вторая ежегодная встреча Китай-Япония-Южная Корея по вопросам реагирования на компьютерные инциденты. Представители головных центров CERT Японии, Китая, Южной Кореи встретились в Сеуле 21 августа 2014 года. В рамках встречи техническими экспертами трех стран был произведен обмен новейшими данными и технологиями, необходимыми для построения крепкой системы кибербезопасности в регионе.

И, наконец, в мае 2014 года CNCERT организовал шестой семинар АСЕАН+Китай по вопросам обеспечения информационной безопасности. Представители CERT Камбоджи, Индонезии, Лаоса, Мьянмы, Филиппин, Таиланда и Вьетнама приняли участие в конференции. В рамках конференции были обсуждены вопросы дальнейшего сотрудничества по вопросам обеспечения информационной и кибербезопасности в регионе.

Как можно заметить, роль центра CERT в Китае не сводится только к разрешению инцидентов нарушения информационной безопасности и киберпреступлений. Организация также предоставляет КНР возможность открытого и конструктивного диалога со странами региона, что несомненно оказывает положительное влияние как на ситуацию в Китае, так и во всем регионе в целом.

При более пристальном изучении ситуации в Китае, становится ясно, что ни один из существующих образов Поднебесной не отражает действительность в полной мере. Китай сегодня – один из ведущих игроков регионального и мирового киберпространства. Но это отнюдь не страна-агрессор – применение жесткой силы противоречит политической доктрине страны.

В политике Китая в сфере обеспечения кибербезопасности и борьбы с кибертерроризмом много уязвимых точек, единого законодательства по-прежнему нет.

К положительным моментам можно отнести, пожалуй, только то, что Китай активно выстраивает партнерские отношения со странами региона в сфере обеспечения кибербезопасности. Ведь это указывает на то, что несмотря на все противоречия, Китай движется в том же направлении, что и его партнеры.

## 2.3. Проблема информационной безопасности и кибертерроризма в Южной Корее

Положение ведущей мировой державы в сфере информационных технологий Республики Корея подтверждается внушительным объемом производства и экспорта информационно-коммуникационных технологий, а также повсеместным распространением Интернета и устройств мобильной коммуникации на территории государства.

Если обратиться к данным статистики, можно увидеть, насколько впечатляющие изменения претерпела информационная инфраструктура государства в период с 2001 по 2015гг. По данным на 2001 год число пользователей сети Интернет составляло 7.81 млн человек. Сегодня же речь идет о 41 млн пользователей Интернета, а также уровне проникновения Интернета, равном 84 %. Республика Корея представлена наиболее высокой скоростью Интернет-соединения, а также наибольшим количеством точек доступного WiFi соединения. [[69]](#footnote-69)

В череде стран Азиатско-Тихоокеанского региона Южная Корея представлена наибольшим числом пользователей киберпространства всех возрастных категорий, включая группу пользователей пенсионного возраста. Наиболее популярные причины пользования Интернетом – поиск информации, досуг, онлайн общение. Корея является родиной лидера электронной индустрии и производства мобильных устройств – компании Samsung, поэтому неудивительно, что уровень проникновения мобильного Интернета составляет 84.8%. Мобильные социальные сети и приложения для онлайн общения необычайно популярны в стране – местное приложение Kakao Talk используется более чем 48 млн активных пользователей. Помимо мобильной переписки, популярными видами активности через мобильные устройства являются социальные медиа, онлайн-игры и просмотр видео. Наиболее популярные социальные сети – Facebook, Twitter, а также местные – M2Day, Nate Connect.

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[[70]](#footnote-70). Другие соотносят эти нежелательные явления с отсутствием социального и правового контроля онлайн-активности в Корее, а также парадоксальным невниманием властей.[[71]](#footnote-71)

Статистические данные о количестве совершаемых киберпреступлений в Корее впервые были выпущены в 1997 году Агентством Национальной Полиции Республики Корея. С тех пор подобные отчеты публикуются ежегодно, и на их основании можно увидеть, что вплоть до 2005 года продолжался беспрецедентно быстрый рост числа киберпреступлений.

Агентство Национальной Полиции разделило киберпреступления на две категории. К первой относятся акты так называемого «кибер-террора» - хакерство, распространение вредоносного программного обеспечения, а также DoS-атаки[[72]](#footnote-72). Ко второй категории «общих киберпреступлений» относят противозаконные деяния, в которых Интернет является главным средством, например, финансовое мошенничество, а также распространение детской порнографии в сети.

Два самых распространенных вида преступлений в корейском киберпространстве это взлом и финансовое Интернет-мошенничество. В обоих случаях более половины совершаемых преступлений связаны с индустрией онлайн-игр. [[73]](#footnote-73)

Киберпространство Республики Корея находится под постоянным наблюдением со стороны Национального разведывательного управления[[74]](#footnote-74) и Национального Агентства по информационной безопасности[[75]](#footnote-75). В рамках своей деятельности оба учреждения ежегодно публикуют отчет в форме Белой Книги[[76]](#footnote-76). Белая книга Национального разведывательного управления, а также аналогичный документ Национального агентства по Интернет-безопасности, помогают сформировать общее представление о тенденциях преступности в корейском киберпространстве, а также о методах борьбы с ней[[77]](#footnote-77).

Так, например, согласно Белой книге Национального Агентства по информационной безопасности за 2014 год, к хорошо известным типам киберпреступлений, таким как DoS-атаки, утечка персональной информации, спам, фишинг, добавился новый – он получил название «smishing» - от слов «SMS» и «Phishing» - своеобразная форма финансового мошенничества. [[78]](#footnote-78)Заключается она в следующем – преступные элементы рассылают сообщения о том, что член семьи получателя попал в аварию или был ранен, в связи с чем требуется немедленно выслать определенную сумму денег на номер счета, указанный в сообщении. При попытке получателя получить доступ к присланному счету снимается денежная сумма. Данный вид мошенничества поразил корейское киберпространство, подобно чуме. С 2013 года, когда впервые было объявлено о массовых случаях «smishing», по 2014 год количество инцидентов возросло в 8 раз и составило 18143 случая с общим ущербом на сумму 3.53 млрд вон.

Законодательная база 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. К ним относятся: Акт о поощрении использования сетевых информационных коммуникаций и информационной безопасности[[79]](#footnote-79), также Акт о защите информационно-коммуникационной инфраструктуры [[80]](#footnote-80)(которые, в свою очередь являются дополнительными пунктами Уголовного законодательства).

Помимо того, актуальными считаются следующие законы: в сфере электронной торговли - Рамочный закон об Электронной Коммерции, Акт о цифровой подписи; в сфере борьбы с домогательствами в сети – Закон о наказании за преступления, совершенные на сексуальной почве; Закон о защите несовершеннолетних – в сфере борьбы с распространением детской порнографии и проч.; Закон об авторском праве; Закон о содействии игровой индустрии, а также Закон о частных случаях регулирования и наказания за спекулятивные действия в сфере онлайн-игр.[[81]](#footnote-81)

Ряд вышеперечисленных законодательных актов предусматривает различные виды наказания за совершение следующих преступных деяний в киберпространстве:[[82]](#footnote-82)

За махинации с использованием общественных электромагнитных записей предусмотрено наказание в виде лишения свободы сроком до 10 лет); частных электромагнитных записей предусмотрено наказание в виде лишения свободы сроком до пяти лет; может быть заменено штрафом в размере до 10 млн. вон);

За акт компьютерного мошенничества (такой вид мошенничества, основным инструментом совершения которого является компьютер) предусмотрено наказание в виде лишения сроком до 10 лет; может быть заменено штрафом в размере до 20 млн вон;

За повреждение электромагнитных записей: в случае публичных отчетов, предусмотрено наказание в виде лишения свободы сроком до 7 лет или штраф в размере до 10 млн.вон); в случае любых других видов данных, предусмотрено наказание в виде лишения свободы сроком до 3 лет или штраф в размере до 7 млн. вон);

Акт об информационно-коммуникационной сети [[83]](#footnote-83)(пересмотрен в 2008 г.) предусматривает наказание за следующие виды киберпреступлений:

Незаконный доступ: Ст.63.1.1 и 48.2, предусматривает наказание в виде лишения свободы сроком до 3 лет или штрафа в размере до 30 млн. вон. Отмечается также, что попытка совершения подобного преступного деяния также уголовно наказуема.[[84]](#footnote-84)

Передача и распространение вредоносных программ: Ст.71.9 и 48.2 предусматривает наказание в виде лишения свободы сроком до 5 лет или штрафа в размере до 50 млн. вон. Отмечается, что написание вредоносной программы как таковой не является уголовно наказуемым деянием.[[85]](#footnote-85)

DoS-атака: Ст.71.10 и 48.3, предусматривает наказание в виде лишения свободы сроком до 5 лет или штрафа в размере до 50 млн. вон.[[86]](#footnote-86)

Кибер-порнография (распространение, рассылка, открытое размещение в информационно-коммуникационной сети материалов непристойного содержания): Ст.74.2 и 44.7.1.1, предусматривает наказание в виде лишения свободы сроком до 1 года или штрафа в размере до 10 млн. вон.[[87]](#footnote-87)

Кибер-преследование (многократное отправление через информационно-коммуникационную сеть текстов, звуков, изображений, видео, вызывающих у получателя чувство страха или беспокойства): Ст.74.3 и 44.7, предусматривает наказание в виде лишения свободы сроком до 1 года или штрафа в размере до 10 млн. вон.[[88]](#footnote-88)

К прочим видам киберпреступлений относятся: распространение, рассылка через информационно-коммуникационную сеть заведомо ложной информации (предусматривается наказание в виде лишения свободы сроком до 3 лет или штрафа в размере до 20 млн. вон, в зависимости от тяжести обстоятельств); передача или реклама информации, призывающей к совершению противозаконных деяний (предусматривается наказание в виде лишения свободы сроком до 1 года или штрафа в размере до 10 млн. вон); сбор адресов электронной почты без разрешения пользователей с помощью технических средств (предусматривается наказание в виде лишения свободы сроком до 1 года или штрафа в размере до 10 млн. вон). [[89]](#footnote-89)

Что касается преступлений против кибербезопаснoсти критических инфраструктур, в 2001 году был выпущен Акт о защите информационно-коммуникационной инфраструктуры, который объединил в себе меры по защите военной, информационно-коммуникационной, финансовой и т.п. инфраструктур. Наказание за преступления против безопасности критических инфраструктур значительно более суровые, чем в случае аналогичных атак на другие системы.[[90]](#footnote-90)

Действующая система обеспечения национальной кибербезопасности была сформирована с целью наращивания потенциала в сфере реагирования на инциденты нарушения кибербезопасности в общественном, частном и военном секторах. Деятельность системы сводится главным образом к объединению и претворению в жизнь различных протоколов кибербезопасности, сбору и анализу данных о кибер угрозах, реагированию и расследованию инцидентов нарушения кибербезопасности. В рамках данной системы действует несколько организаций, утвержденных директивой главы Республики Корея.[[91]](#footnote-91)

Центр обеспечения национальной кибербезопасности – его главной обязанностью является анализ кибер угроз и уязвимостей и распространение рекомендаций по борьбе с киберпреступлениями. Это также главный аналитический центр всей системы.

Центр по обеспечению безопасности военной инфраструктуры от актов киберпреступности;

Центр Информационной безопасности Кореи – один из филиалов Агентства по обеспечению информационной безопасности Кореи (KISA) – основные задачи центра – мониторинг сети, анализ произошедших инцидентов, техническая поддержка в устранении последствий кибер атаки, главным образом, организация работает в частном секторе.

К прочим организациям относятся Национальный институт исследований безопасности, научно-исследовательский институт электроники и телекоммуникаций, центр обеспечения финансовой безопасности.

Национальная полиция РК основала в 2000 году Центр реагирования на инциденты кибер террора – с целью оградить киберпространство Кореи от угрозы. Объектом расследований центра являются кибер атаки против РК и ее граждан. Ячейки этой организации есть в 16 управлениях провинциальной полиции. Состоит она из шести групп:

Группа управления и кооперации занимается разработкой мер по борьбе с киберпреступностью, обучением и координированием внутреннего и международного сотрудничества в этой сфере.

Три исследовательские группы производят сбор и анализ данных о кибер инцидентах на общегосударственном уровне.

Группа планирования расследований получает все отчеты о киберпреступности в стране, анализирует общие тенденции, планирует операции государственного масштаба по ликвидации кибер угроз.

Группа технической поддержки занимается разработкой технологий, необходимой в расследованиях, а также является отделом криминалистики всей организации.

Также важнейшую роль в системе обеспечения национальной кибербезопасности играет региональная ячейка организации CERT.

Группа CERT Южной Кореи – KrCERT/CC была основана в 1996 году. Следует отметить, что ячейка CERT Кореи поддерживает, пожалуй, самые тесные отношения с государственным аппаратом среди всех стран Азиатско-Тихоокеанского региона. Причина столь тесной связи правительства и независимой, неправительственной, некоммерческой организации кроется в раннем этапе деятельности Kr CERT/CC. [[92]](#footnote-92)

Активно функционировать группа начала в 1998 году, а уже в 2003 ей пришлось столкнуться с очень тяжелым испытанием – Интернет по всей стране был буквально парализован из-за активности червя Slammer. К угрозе такого масштаба еще молодая организация попросту не была готова – разрешить инцидент и ликвидировать его разрушительные последствия стало возможно только благодаря помощи Агентства по информационной безопасности Кореи. С того случая прошло уже много лет, центр успешно разрешил множество инцидентов нарушения кибербезопасности в стране самостоятельно, но тесные связи с государством поддерживаются по сей день.

KrCERT/CC служит центром координирования деятельности по борьбе с киберпреступностью по всей стране. Официально центр действует как филиал Агентства по информационной безопасности Кореи. За прошедшие годы центр CERT Кореи совместно с KISA разработали систему обнаружения скрытой вредоносной активности (MC-Finder), услугами которой пользуется более 2.5 млн доменов с 2014 года. Основная задача данной системы состоит в проверке домашней страницы на наличие любой скрытой вредоносной активности, ее блокировка и удаление. Среди сайтов, на которых была обнаружена скрытая вредоносная активность в 2014 году, домашние страницы малых и средних корпораций, благотворительных организаций, исследовательских институтов. Основные типы обнаруженной вредоносной активности – утечка финансовых данных, дистанционное управление сайтом, реклама фишинг-сайтов.

Как уже было упомянуто выше, одним из наиболее распространенных видов киберпреступлений в Корейском киберпространстве являются DDoS-атаки. В рамках своих полномочий, KrCERT/CC с 2009 года проводит политику предоставления «кибер-убежища от DDoS-атак» малым и средним предприятиям. В период с момента основания программы в 2009 году по 2015 год ей воспользовались более 2000 организаций.

Другой распространенный в корейском киберпространстве вид преступлений – атаки с использованием уязвимостей в популярном корейском программном обеспечении Hancom Office. В связи с этим KrCERT/CC подошел к решению вопроса нестандартно. Было объявлено о конкурсе, в рамках которого участникам было необходимо найти как можно больше уязвимостей в программном обеспечении. По результатам конкурса за 2014 год, было выявлено 9 уязвимостей. Hancom Office объявила о присуждении денежных призов участниками, обнаружившим три серьезнейшие уязвимости. После выпуска обновленной версии программного обеспечения конкурс объявляется снова. Конкурс даже получил официальное название – «Bug Bounty». [[93]](#footnote-93)

Как было упомянуто выше, Корея является одной из ведущих стран региона по уровню использования смартфонов и мобильного Интернета. Особенно увеличилось число пользователей мобильного Интернета и смартфонов после 2012 года, а соответственно резко подскочил уровень преступлений, связанных со столь популярным устройством. С конца 2013 года smishing-атаки на смартфоны платформы Android резко участились. Ячейка CERT Кореи прилагает все усилия с целью снижения числа подобных атак, но, к сожалению, добиться этого пока не удается. Активное сотрудничество ведется с центрами CERT Японии и Китая.

В рамках своих полномочий, KrCERT/CC разработал систему анализа информации о кибер угрозах и инцидентах нарушения кибербезопасности в 2013 году. Главной задачей данной системы является сбор информации о недавних кибер атаках и поиск корреляций между ними.

В июле 2014 года KrCERT/CC принимал Курсы по обучению специалистов в области обеспечения информационной безопасности стран Азиатско-Тихоокеанского региона. Это ежегодное мероприятие проводится с 2005 года и служит платформой для взаимодействия специалистов в сфере кибербезопасности, а также для свободного обмена данными и технологиями в сфере обеспечения информационной безопасности в киберпространстве.

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.

Постоянная угроза со стороны Пхеньяна оказывает существенное влияние на программу национальной кибербезопасности Южной Кореи, вынуждая Сеул концентрировать большую часть усилий на обороне домашнего киберпространства. Очевидное усиление Северной Кореи в киберпространстве в последние годы является причиной беспокойства мирового сообщества в целом. Что, в свою очередь, оказывает давление на Южную Корею, так как она должна отвечать на возникающие инциденты нарушения кибербезопасности, как только они появляются, не провоцируя конфликта с соседом. На Сеуле лежит ответственность по созданию совершенной системы киберзащиты, способной своевременно отвечать на внешние атаки, не допуская ситуаций, в которых провокация Пхеньяна может перерасти в полноценный военный конфликт.

## 2.4. Проблема информационной безопасности и кибертерроризма в Японии

Пожалуй, самое распространенное представление о Японии в современном мире – рай высоких технологий; государство, технически столь развитое во всех отношениях, что сравниться с ним не может никто. Реальность же до смешного не сходится с таким образом: в череде развитых стран мира Япония стоит особняком как раз из-за своей поразительной неспособности противостоять угрозам, которые несет в себе киберпространство.

Согласно данным о количестве пользователей киберпространства в Азиатско-Тихоокеанском регионе, Япония занимает третье место – в стране официально насчитывается более 101 млн пользователей сети. [[94]](#footnote-94)Демографические исследования показали, что наравне с подростками и молодежью, к числу активных пользователей Интернета в Японии принадлежат представители возрастной группы старше 55 лет. Также, в исследовании отмечается, что пользователей-мужчин значительно больше, чем женщин. Наиболее популярной деятельностью является поиск информации, а также просмотр видео.

Наиболее активными пользователями мобильного Интернета и приложений являются предстатели возрастной категории от 18 до 24 лет – в среднем, за такой активностью пользователь проводит 114 минут в день. Самым популярным приложением для мгновенной переписки является Line – с 21.2 млн пользователей, по данным на 2015 год.[[95]](#footnote-95)

Последние исследования показывают, что наиболее популярными социальными сетями в стране являются Twitter и Facebook, немного отстают местные социальные сети Mixi и LINE. На май 2015 года, число пользователей Twitter достигло отметки 21.75 млн человек.

Уровень проникновения Интернета в государстве высок – более 54% - по данным на 2014 год. Исследователи полагают, что к концу 2016 года будет достигнут уровень 60%.

Так в чем же причины того, что столь развитая в информационно-технологическом плане Япония настолько уязвима в киберпространстве?

Ключевых моментов выделяется несколько. Во, первых, нельзя отрицать что функционирование институтов, учреждений, организаций политической и финансовой сферы в Японии находится не просто в тесной связи с Интернетом – оно от него зависит. Согласно исследованию[[96]](#footnote-96), Япония, вместе с Южной Кореей, Сингапуром, Австралией и Новой Зеландией показывают наивысший уровень проникновения Интернета в экономику и бизнес сферы – в 9 раз выше, чем у остальных стран региона.

Во-вторых, несомненное влияние оказывает тот факт, что японское общество является стареющим. Как уже было сказано выше, к числу активных пользователей Интернета в Японии принадлежат представители возрастной группы старше 55 лет. Пожилые люди очень доверчивы, и большинство представителей старшего поколения не обладают даже базовыми знаниями о работе в сети Интернет и не имеют ни малейшего представления об угрозах киберпространства. В условиях, когда большая часть пользователей не осведомлена или безразлично относится к угрозам киберпространства, Интернет-мошенничество всех мастей просто обречено на процветание.

В-третьих, не стоит забывать о специфике японской ментальности. Как известно, в японской культуре жертва насилия, преступления не вызывает чувства жалости – она подвергается осуждению, осмеянию. Из этой давней традиции растут корни нежелания представителей власти, промышленности, бизнеса и рядовых жителей заявлять о том, что они подверглись кибер-атаке – ведь вина за это будет возложена на них самих.

И, наконец, в-четвертых, одной из главных проблем, с которыми сталкивается Япония в сфере обеспечения безопасности киберпространства – нехватка квалифицированных кадров. Уильям Хироюки Сайто[[97]](#footnote-97), специальный советник премьер-министра по кибер-вопросам, отмечает, что в Японии не хватает, по самым скромным подсчетам, 80 000 квалифицированных специалистов в сфере кибербезопасности. [[98]](#footnote-98)А одним из главных препятствий для их подготовки является особенность системы образования – в Японии учащиеся не допускаются к компьютерному программированию вплоть до поступления в ВУЗ.

В мировом киберпространстве Япония сегодня представляет собой цель высоко уровня важности – в военном, экономическом и технологическом плане. [[99]](#footnote-99)В августе 2011 года была произведена массированная атака на базы данных компании Мицубиси[[100]](#footnote-100); в том же году в результате взлома, в сети появилась рабочая и личная информация 480 членов правительства. В 2012 году атаке подверглось Министерство Сельского хозяйства и Рыболовства; в 2013 году Министерство иностранных дел заявило к краже как минимум 20 документов государственной важности из базы данных министерства.

2015 год принес множество серьезных инцидентов нарушения кибербезопасности Японии. Выделяется четыре ключевых проблемных момента, разрешение которых стало приоритетной задачей правительства Японии на 2016 и последующие годы: Взлом базы данных Государственной Пенсионной системы Японии; атаки на базу данных новой страховой и налоговой системы «My Number»; серьезная нехватка квалифицированных кадров в сфере обеспечения кибербезопасности; разработка новой национальной стратегии по обеспечению кибербезопасности.

Так как именно произошедшие в 2015 году события, послужили катализатором для активизации деятельности Японии в сфере обеспечения информационной безопасности в киберпространстве, представляется интересным рассмотреть каждое из них более подробно.

1. Взлом базы данных Государственной Пенсионной Системы Японии.

В июне 2015 года на первых полосах газет страны появились заголовки о взломе базы данных Государственной Пенсионной Системы Японии[[101]](#footnote-101), в результате которого персональные данные более 1.25 млн граждан были выложены в открытый доступ в сеть. Это далеко не первый и не самый крупный случай взлома – в 2014 году атаке подверглась корпорация Benesse (утечка персональных данных 22.6 млн), а ранее в 2011 году была взломана система Sony’s Playstation (утечка информации 77 млн).

Однако атака на базы данных пенсионной системы отличается по мере психологического воздействия. Инцидент в полной мере показал населению, насколько рядовые граждане уязвимы перед киберпреступностью. В ходе расследования, которым занимался как сам Пенсионный фонд, так и Национальный центр по информационной безопасности, было выявлено, что причиной утечки стала устаревшая система защиты данных, а также нескоординированная деятельность по реагированию на инцидент. Атака, как таковая, производилась в форме рассылки сообщений по электронной почте, по самым скромным подсчетам было отправлено около 124 сообщений, три из который, замаскированные под деловую переписку, были открыты. Они, в свою очередь, привели к полному обрушению системы безопасности, несмотря на то, что своевременные действия грамотных специалистов в сфере кибербезопасности, могла бы легко предотвратить подобный ущерб. Сотрудники пенсионного фонда не соблюдали базовые правила кибербезопасности – данные, которые должны быть под защитой системы паролей, находились в открытом доступе; устройства, которые в нерабочее время должны быть отсоединены от сети, находились в подключенном состоянии. Все эти нарушения, будь они вовремя замечены и исправлены компетентными специалистами, могли бы существенно уменьшить разрушительные последствия взлома.

Как уже было сказано выше, взлом базы данных государственного пенсионного фонда Японии вывел киберпреступность на всеобщее обозрение. Однако, этот инцидент также породил и волну паники и сомнения в компетентности правительства в вопросах обеспечения информационной безопасности своих граждан.

1. Атаки на базы данных новой страховой и налоговой системы «My Number»

До 2015 года налоговые, финансовые и страховые данные каждого гражданина Японии хранились отдельно друг от друга, и занимались ими разные специалисты. Государственная система «My number» [[102]](#footnote-102)имеет своей целью их объединение путем присвоения каждому человеку 12-тизначного регистрационного номера, привязанного к налоговой, страховой, финансовой информации каждого их них. В период с октября по ноябрь 2015 года каждый житель Японии должен был получить уведомление о присвоении им персонального номера, который будет введен в эксплуатацию к январю 2016 года. Первоначальный план предполагал использование номера только для оплаты налогов, а также для социальной защиты, но в планах правительства глобальное расширение системы, включение в нее управление банковским счетом, а также медицинское страхование.

Появившаяся столь скоро после взлома пенсионного фонда система, вызвала у граждан лишь недоверие. Каналов утечки информации из этой системы множество. Уже к концу ноября 2015 года – за месяц до фактического введения системы в эксплуатацию, полиция уже получила 168 отчетов об инцидентах нарушения ее безопасности. Сегодня система «My number» успешно функционирует, но по-прежнему продолжает оставаться целью киберпреступников.

1. Нехватка квалифицированных специалистов в сфере обеспечения кибербезопасности.

Согласно публичному отчету Агентства продвижения информационных технологий,[[103]](#footnote-103) в Японии насчитывается 265 069 специалистов в сфере обеспечения кибербезопасности, что на 81 590 меньше, чем необходимо. К тому же отмечается, что из 265 069 специалистов, больше половины из них некомпетентны и нуждаются в дальнейшем обучении. Правительство Японии называет нехватку кадров в этой сфере одной из главных проблем современности. Различные организации частного и государственного секторов взялись за решение этой проблемы. Летом 2016 года Министр Внутренних коммуникаций выделил бюджетные средства на срочную программу подготовки 50 000 специалистов сферы кибербезопасности сроком до открытия Олимпиады 2020 в Токио. Телекоммуникационный гигант NTT заявил о намерении в четверо увеличить число сотрудников, доведя его до 10 000 в 2020 году. Также NTT совместно с университетом Васэда разработал курс по обеспечению компьютерной безопасности, который официально вошел в учебную программу заведения с апреля 2015 года.

1. Разработка новой стратегии по обеспечению кибербезопасности Японии.

Важным шагом на пути к гармонизации киберпространства стало принятие в сентябре 2015 года второй Стратегии по обеспечению кибербезопасности Японии, которая определяет подход государства к вопросам кибербезопасности на ближайшие три года. В отличие от предыдущей Стратегии от 2013 года, проект 2015 года был полностью одобрен правительством Японии,[[104]](#footnote-104) на основании чего можно сделать вывод о том, что правительственные круги Японии, наконец, осознали всю глубину проблемы обеспечения кибербезопасности в стране.

В стратегии от 2015 года можно выделить четыре основных особенности.

Во-первых, в тексте документа подчеркиваются как положительные, так и отрицательные аспекты киберпространства – являющегося одновременно источником инноваций и угроз. В отличие от стратегии 2013 года, в которой говорилось исключительно о рисках и угрозах, которые несет в себе киберпространство. Стратегия 2015 года подчеркивает инновационную функцию киберпространства, а также признает, что в одиночку Японское правительство не может ответить на все вызовы информационной безопасности в киберпространстве. Стратегия призывает всех – пользователей, гражданское общество, предприятия критических инфраструктур, бизнес-сектор – внести посильный вклад в обеспечение безопасности киберпространства Японии.[[105]](#footnote-105)

Во-вторых, говорится о дальнейшем преобразовании государственных учреждений, действующих в сфере обеспечения информационной безопасности. Годом ранее парламент Японии принял закон о формализации роли Национального центра информационной безопасности (NISC). Центр, в действительности, был основан решением премьер-министра 10 лет назад, однако в силу отсутствия правовых полномочий, влияние Центра на прочие министерства и организации было невелико. Благодаря Акту об основах кибербезопасности от 2014 года, Центр теперь отвечает за разработку национальной стратегии и политики по обеспечению кибербезопасности министерств и агентств.[[106]](#footnote-106)Стратегия 2015 года признает существующую иерархию организаций сферы обеспечения кибербезопасности Японии, согласно которой Национальный центр Информационной Центр отвечает за разработку национальной стратегии и политики по обеспечению кибербезопасности министерств и агентств. В числе прочих организаций, действующих в данной сфере, называются Национальное Управление Полиции[[107]](#footnote-107), Министерство Внутренних Дел и Коммуникаций[[108]](#footnote-108), Министерство безопасности[[109]](#footnote-109).

В-третьих, стратегия 2015 года напоминает о таком серьезном происшествии, как взлом базы данных Японского Пенсионного Фонда в мае 2015 года. А также выражается обеспокоенность правительства Японии обеспечением безопасности новой системы «My Number».

И в-четвертых, стратегия 2015 года освещает международную деятельность Японии в сфере обеспечения кибербезопасности, отмечая отдельно успехи в диалоге с АСЕАН, отношениях с США и Африкой, а также с Евросоюзом. Из текста Стратегии становится ясно, что Япония со своей стороны намерена углублять сотрудничество в рамках существующих партнерских отношений. [[110]](#footnote-110)

В целом, можно отметить положительную динамику по сравнению с аналогичным документом 2013 года. Стратегия подчеркивает роль государства в обеспечении национальной кибербезопасности, при этом не ограничивается рост рынка технологий, главного источника инноваций.

Само собой, это не единственные трудности в сфере обеспечения информационной безопасности в киберпространстве, с которыми Япония столкнулась за период 2014-2015 гг., и с которыми страна борется в году нынешнем. Атаки хактивистской группировки Anonymous (10.12.2015 нападению подверглась домашняя страница премьер-министра Абэ), постоянное давление со стороны Северной Кореи и Китая – эти проблемы ни в коей мере не отходят на второй план.

Однако при всех негативных инцидентах, с которыми Японии пришлось столкнуться в прошедшие два года, у такой ситуации есть и положительная сторона – в японском обществе, наконец, появилось четкое представление о реальной опасности киберугрозы. Что, в свою очередь подтолкнуло правительство Японии к активной деятельность в сфере преобразования законодательной базы, результатом которой стало создание Акта об основах кибербезопасности от 2014 года[[111]](#footnote-111), появление Штаб-Квартиры Стратегической Кибербезопасности[[112]](#footnote-112), а также формирование новой Стратегии по обеспечению кибербезопасности[[113]](#footnote-113).

До недавнего времени, наказание за противозаконную деятельность в киберпространстве предусматривалось лишь следующими законами:

Акт о несанкционированном компьютерном доступе[[114]](#footnote-114) от 1999 года. В данном законе прописывается определение несанкционированного компьютерного доступа, а также наказание за совершение подобного деяния – лишение свободы сроком более одного года или штраф в размере от 500,000 йен. Отмечается, что посредничество в проведении актов несанкционированного компьютерного доступа также является преступным деянием и подлежит наказанию в виде штрафа в размере от 300,000 йен.[[115]](#footnote-115)

Статьи 258 и 259 уголовного кодекса Японии также можно отнести к законодательству в сфере обеспечения информационной безопасности. Статья 258 предусматривает наказание за повреждение официальных документов, а также электромагнитных записей, находящихся в общественном пользовании – лишение свободы сроком до семи лет.[[116]](#footnote-116)

Статья 259 регулирует преступную деятельность по повреждению документов и электромагнитных записей, находящихся в частном пользовании – лишение свободы сроком до 5 лет.[[117]](#footnote-117)

Весьма распространенным видом преступлений в киберпространстве Японии является распространение порнографии, в том числе и детской. Наказание за подобную деятельность предусмотрено в уголовном кодексе Японии (статья 175); в Законе о наказании за деятельность, имеющую отношение к детской проституции и детской порнографии № 52 от 1999 года.

Что касается статьи 175 уголовного кодекса Японии, она предусматривает наказание за распространение в сети материалов непристойного содержания – в виде лишения свободы сроком от двух лет или штрафа в размере до 2,5 млн йен. [[118]](#footnote-118)Однако, следует отметить, что в законе четко не прописано, какие именно материалы относятся к «непристойным», отсюда непрекращающиеся споры об интерпретации данной статьи. Большинство исследователей указывают на то, что данная статья не включает в себя распространение порнографии в сети, так как статья вступила в силу в 1907 году, а в то время, подобной проблемы еще не было.

Далее, касаемо закона №52 от 1999 года, согласно статям 7 и 10 лицо, занимающееся распространением детской порнографии, подлежит наказанию в виде лишения свободы сроком до 3 лет или штрафа в размере до 3 млн йен. Аналогичному наказанию подлежат лица, перевозящие в или из Японии материалы, содержащие детскую порнографию.[[119]](#footnote-119)

Большим шагом вперед в обеспечении безопасности киберпространства Японии стало принятие Акта об основах кибербезопасности 6 ноября 2014 года. [[120]](#footnote-120)Этот документ на настоящее время является основным законом в государстве в сфере обеспечения кибербезопасности.

Статьи 6 и 7 нового закона обязывают бизнес сферы информационной инфраструктуры, киберпространства принимать меры по обеспечению кибербезопасности своих предприятий, а также сотрудничать с государственным сектором, предоставлять всю необходимую информацию по этому вопросу. [[121]](#footnote-121)

В законе также прописаны и обязательства государственного сектора по оказанию поддержки инфраструктурному бизнесу в обеспечении кибербезопасности (Ст.14).[[122]](#footnote-122)

Статья 13 нового Акта обязывает правительство установить единые стандарты кибербезопасности для правительственных учреждений; вести наблюдение за правительственной сетевой информационной системой, фиксировать и анализировать все инциденты по нарушению ее безопасности.[[123]](#footnote-123)

Также закон обязывает правительство развернуть деятельность по укреплению сотрудничества между организациями, действующими в сфере обеспечения кибербезопасности, а также внести ясность в полномочия каждой организации, с целью противодействия кибер атакам, которые могут нанести ущерб государству (Ст.18). [[124]](#footnote-124)

Согласно 21 статье Акта, государство должно приложить усилия в решении вопроса о нехватке и низкой квалификации специалистов соответствующей отрасли.

Статьей 29 Акта об основах кибербезопасности также предписано преобразование Совета по информационной безопасности в Штаб-квартиру по стратегии обеспечения кибербезопасности. Штаб-квартира, возглавит которую Генеральный секретарь кабинета министров, должна будет разработать стратегию противодействия кибер-атакам, а также по предотвращению распространения ущерба от этих атак. Члены Штаб-квартиры, включая министра иностранных дел, министра обороны, министра торговли и экономики, министра внутренних дел, а также председателя комиссии по национальной безопасности и др. назначаются премьер-министром. [[125]](#footnote-125)

Согласно дополнительным положения Акта, Национальный центр информационной безопасности[[126]](#footnote-126), который занимается отражением кибер-атак на правительственные учреждения, должен быть наделен дополнительными полномочиями. Центр Национальной Информационной безопасности будет выступать в роли секретариата при штаб-квартире. Все правительственные учреждения и агентства обязаны докладывать о кибер-атаках в штаб-квартиру. В случае отказа в сотрудничестве со специалистами штаб-квартиры, премьер-министр будет обладать полномочиями по их роспуску.

Принятие данного закона несомненно является признаком положительных изменений ситуации в Японии.

Еще одна организация, ведущая активную деятельность в сфере обеспечения кибербезопасности Японии – ячейка организации CERT в Японии. Причем, следует отметить, что она осуществляет свою деятельность в русле новой стратегии по кибербезопасности Японии.

Ячейка CERT в Японии – JPCERT/CC – независимая, некоммерческая организация, исполняющая помимо прочего функцию посредника в общении центров CERT других стран региона и мира. Проект по ее созданию появился в 1992 году, а официально объявлено о создании данной организации было в 1996 году. С тех пор JPCERT/CC взял на себя деятельность по исправлению нарушений информационной компьютерной безопасности, исправление уязвимостей, выпуск материалов, помогающих защититься от кибер-атак, а также осуществляет взаимодействие со всеми центрами CERT.

В рамках своих полномочий JPCERT/CC основал информационный веб-портал JVN (Japan Vulnerability Notes), на котором размещается информация об инцидентах нарушения кибербезопасности, а также руководства по противодействию подобным происшествиям[[127]](#footnote-127). Контроль за активностью веб-портала осуществляет JPCERT/CC совместно с Агентством по продвижению информационных технологий (IPA), которое, со своей стороны предоставляет описание каждого конкретного случая нарушения кибербезопасности, методы его разрешения.

Пожалуй, наиболее важным аспектом деятельности ячейки СERT в Японии является проект группы Цубамэ. Группа Цубамэ осуществляет сбор, анализ данных об Интернет-траффике стран Азиатско-Тихоокеанского региона, с целью выявления основных угроз его странам.

Также JPCERT/CC активно занимается подготовкой и повышением квалификации специалистов сферы обеспечения информационной безопасности в киберпространстве – несколько раз в год проводятся обучающие семинары, курсы повышения квалификации.

Для Японии, период 2014-2015 гг. во многом стал поворотным. В силу вышеописанных происшествий ни рядовые граждане, ни правительство страны больше не могут игнорировать серьезность угрозы, которую несет в себе киберпространство. И хотя шаги, предпринятые правительством Японии по решению насущных вопросов обеспечения кибербезопасности, еще достаточно несмелые и пока не принесли ощутимых результатов, можно с уверенностью утверждать, что в сфере обеспечения информационной безопасности Японии в киберпространстве наступил качественно новый период.

# Заключение

В заключение, хотелось бы отметить, что ни одно из вышеописанных государств, пусть и признанных лидеров региона, а в некоторых аспектах, и всего мира, не может похвастаться тщательно проработанной, эффективной системой обеспечения информационной безопасности в киберпространстве. А ведь речь идет о таких гигантах, как Китай, Япония, Индия и Южная Корея. В одном случае, отсутствует законодательная база, в другом – бездействие правительства приводит к катастрофическим последствиям. Причины могут различаться, зато един результат – ведущие страны Азиатско-Тихоокеанского региона в условиях киберпространства необычайно уязвимы.

Однако, при всей серьезности, ситуация вовсе не является безнадежной – ведь и Китай, и Япония, И Индия, и Южная Корея при всех различиях и противоречиях разделяют точку зрения о том, что ключ к формированию безопасного киберпространства лежит в сотрудничестве.

В рамках данного исследования совершенно не был затронут военный аспект проблемы. Однако при современном темпе развития общества, это лишь вопрос времени, когда киберпространство станет полноценным театром военных действий.

Хотелось бы провести одну любопытную историческую параллель. В 1903 году состоялся первый полет на самолете модели братьев Райт. Событие по значению своему революционное – человек покорил воздушное пространство! Однако уже через восемь лет такое чудесное изобретение было использовано как оружие в разгоревшейся Итало-Турецкой войне 1911 года. Небо превратилось в третий фронт. От первого полета до первой бомбежки – чуть больше 10 лет. Но ничего не поделаешь, такова уж человеческая природа – любое изобретение, сколь угодно благое, рано или поздно будет поставлено на службу войне.

Похожую ситуацию сегодня можно наблюдать в отношении киберпространства. По своей новизне и революционности, компьютер и сеть Интернет, вполне сравнимы с первыми самолетами. А по силе влияния, оказываемого на политическую, экономическую и другие сферы жизни общества, информационные технологии продвинулись намного дальше первых летательных аппаратов.

Информационные технологии уже давно играют важную роль в военных операциях на суше, море, в воздухе и в космосе. Сегодня можно все чаще слышать выражения «информационная война», «кибертерроризм», в работах нескольких японских авторов можно прочесть, что киберпространство превращается в «пятый фронт», наряду с наземным, водным, воздушным и космическим.

Характер противостояния государств в киберпространстве будет иметь ряд отличительных особенностей. [[128]](#footnote-128)Если речь идет о наземном, наводном или воздушном конфликте – определить территорию, участок пространства, принадлежащий одной из сторон достаточно легко. А в случае с космическим пространством и киберпространством – это сделать пока просто невозможно – ни космос, ни киберпространство на данном этапе не признают границ. Еще одной особенностью киберпространства является то, что подкованный специалист с легкостью сможет замести следы или вовсе возложить свою вину на другого человека. Отсюда возникает вопрос, какие меры наказания и к кому именно следует применять в сфере преступлений против кибербезопасности?

Данная тема актуальна и сегодня, и тем более будет актуальна в будущем. Поэтому представляется интересным заняться ее исследованием в рамках следующей научной работы.

# Список использованной литературы и источников:

Законы и нормативные акты

1. Акт об основах кибербезопасности. サイバーセキュリティ基本法案. [Электронный ресурс]. Доступно из URL: <http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/houan/g18601035.htm> (дата обращения 19.12.2015)
2. Закон о наказании за деятельность, связанную с детской проституцией и детской порнографией, 1999г. [Электронный ресурс]. Доступно из URL: <http://taroyamada.jp/wp-content/uploads/2014/05/f7f0f191e6ccf9c3b31f1399957cac8d.pdf> (дата обращения 26.11.2015)
3. Окинавская Хартия глобального информационного сообщества. [Электронный ресурс]. Доступно из URL: <http://www.mofa.go.jp/policy/economy/summit/2000/documents/charter.html> (Дата обращения: 29.03.2015 )
4. Act on the Protection of Personal Information (Act No. 119 of 2003. Effective April 1, 2005). [Электронный ресурс]. Доступно из URL: <http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf> (дата обращения 17.12.2015)
5. China Penal code. [Электронный ресурс]. Доступно из URL: <https://www.oecd.org/site/adboecdanti-corruptioninitiative/46814270.pdf> (Дата обращения 28.03.2016)

Convention on cybercrime., Budapest, 23 November 2001. [Электронный ресурс]. Доступно из URL : <http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf> (дата обращения 12.01.2016)

1. India Informarion Tecnology Act. [Электронный ресурс]. Доступно из URL: <http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan010239.pdf> (Дата обращения: 15.05.2016)
2. India National security policy 2013. [Электронный ресурс]. Доступно из URL: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NationalCyberSecurityPolicyINDIA.pdf> (Дата обращения 15.05.2016)
3. The Act on Promotion of Information and Communications network
4. utilization and data protection, etc. [Электронный ресурс]. Доступно из URL: <http://www.koreanlii.or.kr/w/images/d/df/DPAct2014_ext.pdf> (Дата обращения 15.02.2016)
5. The Act on Promotion of Information and Communications network utilization and Information Protection. [Электронный ресурс]. Доступно из URL: <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN025694.pdf> (Дата обращения 18.12.2015)
6. The Act on the protection of Information and communications infrastructure. [Электронный ресурс]. Доступно из URL: [http://www.law.go.kr/LSW/LsInfoP.do?lsiSeq=136754#](http://www.law.go.kr/LSW/LsInfoP.do?lsiSeq=136754) (Дата обращения 21.12.2015)

United Nations Manual on the Prevention and Control of Computer-Related Crime. [Электронный ресурс]. Доступно из URL: <http://www.uncjin.org/8th.pdf> (Дата обращения: 11.01.2016)

1. 不正アクセス行為の禁止等に関する法律. [Электронный ресурс]. Доступно из URL: <http://www.npa.go.jp/cyber/legislation/pdf/2_houritsujoubun.pdf> (Дата обращения: 08.10.2015)
2. 不正アクセス行為の禁止等に関する法律の解説.[Электронный ресурс]. Доступно из URL: <http://www.npa.go.jp/cyber/legislation/pdf/1_kaisetsu.pdf> (Дата обращения 08.10.2015)

Литература на русском языке:

1. Алексеев И.Ю. Информационные вызовы национальной международной безопасности. — М.: «Международные отношения», 2001.
2. Батурин Ю.М., Жодзишский A.M. Компьютерная преступность и компьютерная безопасность. М.: 1991.
3. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: Учебник. СПб., 2005. – 439с.
4. Васенин В.А. Информационная безопасность и компьютерный терроризм. // Научные и методологические проблемы информационной безопасности / Под ред. Шерстюк В.П. М., 2004.
5. Галатенко В.Н. Информационная безопасность: практический подход. М., 1998.
6. Галатенко В.А. Основы информационной безопасности. - М.: Интернет-университет информационных технологий - ИНТУИТ.ру.,2008. - 208 с.
7. Гатченко Н.А., Исаев А.С., Яковлев А.Д. Криптографическая защита информации – СПб: НИУ ИТМО, 2012. – 142с.
8. Голубев В.А. Кибертерроризм – угроза национальной безопасности [Электронный реcурс]. – Доступно из URL: [www.crive-research.ru](http://www.crive-research.ru) (дата обращения 13.12.2014)
9. Голубев В. А. Электронный терроризм — проблемы противодействия. [Электронный ресурс]. Доступно из URL: http:// [www.crime-research.ru/articles/Golubev/](http://www.crime-research.ru/articles/Golubev/) (дата обращения 25.03.2016)
10. Безопасность: теория, парадигма, концепция, культура. Словарь-справочник / Автор-сост. профессор В. Ф. Пилипенко. 2-е изд., доп. и перераб. — М.: ПЕР СЭ-Пресс, 2005. – 992с.
11. Закупень Т. Понятие и сущность информационной безопасности, и ее

место в системе обеспечения национальной безопасности РФ //Информационные Ресурсы России. 2009. №4.

1. Мазуров, В.А. Компьютерные преступления: классификация и способы противодействия/ В.А. Мазуров. М.: «Палеотип», «Логос», 2002. – 187с.
2. Пюкке С. Информация без опасности // Компьютерра. 2002. № 19.

Ричардсон, Р. Хакеры: дьяволы или святые? / Р. Ричардсон // Журнал сетевых решений. 1998. - Т.4. – 316с.

1. Шубинский М.И. Информационная безопасность для работников бюджетной сферы: Учебное пособие. – СПб.: НИУ ИТМО, 2012. – 102с.

Литература на иностранном языке:

APCERT Annual Report, 2014. [Электронный ресурс]. Доступно из URL: <http://www.apcert.org/documents/pdf/APCERT_Annual_Report_2014.pdf> (дата обращения 05.04.2016)

1. Aldrich, Richard W. Cyberterrorism and Computer Crimes: Issues Surrounding the Establishment of an International Legal Regime / Richard W. Aldrich. Colorado: USAF Institute for National Security Studies, 2000.

Cho Kyon Seok. The Current Situation of Measures for Crime Victims in the Korean Criminal Justice System. [Электронный ресурс]. Доступно из URL: <http://www.unafei.or.jp/english/pdf/RS_No81/No81_10VE_Seok.pdf> (дата обращения 27.03.2016 )

Creating regional cyber maturity metric: Cyber Maturity in Asia-Pacific Region 2015 – Sidney, 2015., Australian Strategic Policy Institute. [Электронный ресурс]. Доступно из URL: <https://www.aspi.org.au/publications/cyber-maturity-in-the-asia-pacific-region-2015/Cyber-Maturity-2015.pdf> (дата обращения 12.05.2016)

Cybercrime survey report, 2014, KPMG in India”. 2014, KPMG international cooperative (“KPMG International”), 2014.

Deloiette’s Asia-Pacific Defence Outlook 2016. [Электронный ресурс]. Доступно из URL: <http://www2.deloitte.com/sg/en/pages/public-sector/articles/deloitte-2016-asia-pacific-defense-outlook.html> (дата обращения 13.01.2016)

Halder, D.,& Jaishankar, K. (2011b). Cybercrime and victimization of Women: Laws, Rights, and Regulations. Hershey, USA: IGI Global. 263р.

Halder, D.,& Jaishankar, K. (2011a). Cyber Gender Harassment and secondary Victimization: A Comparative Analysis of US, UK and India. Victims and Offenders, 6(4), 567р.

Junsik Jang. Best Practices in Cybercrime Investigation in the Republic of Korea. [Электронный ресурс]. Доступно из URL: <http://www.unafei.or.jp/english/pdf/RS_No79/No79_09VE_Jang2.pdf> (дата обращения 20.03.2016)

Korean Internet White Paper 2014. [Электронный ресурс]. Доступно из URL: <http://isis.kisa.or.kr/eng/ebook/EngWhitePaper2014.pdf> (дата обращения 13.04.2015)

1. Lewis, James A. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats / James A. Lewis. Washington D. C., 2002. – 462р.

National Cyber Security Policy – 2013(NCSP-2013)., 02.06.2013, Ministry of Information and Communication Technology, Department of Electronics and Information Technology.

“Norton Cyber Crime Report: The Human Impact”.2013, Norton. From Symantec, USA, 2013.

Pi Yong. New China Criminal Legislations in the Progress of Harmonization of Criminal Legislation against Cybercrime. 2001.

Saito, William. ザ・チーム 日本の一番大きな問題を解く.日経BP社, 2012. – 381р.

Saito, William. その考え方は、「世界標準」ですか?. 日経BP社, 2012. – 539р.

Окамура Хисамити岡村久道. Кодзиндзёхохого 個人情報保護法 (Законодательство в сфере обеспечения безопасности персональных данных). Токио 東京, Сёдзихомукабусикигайся商事法務株式会社,2011, - 204с.

Окамура Хисамити岡村久道. Дзёхосэкюрити-но хорицу情報セキュリティの法律 (Законодательство в сфере информационной безопасности). – Токио 東京, Сёдзихомукабусикигайся商事法務株式会社, 2011, - 402с.

Окамура Хисамити 岡村久道. Кодзиндзёхохогохо-тисики個人情報保護法の知識 (Осмысление законов в сфере обеспечения безопасности персональной информации). – Токио 東京, Сёдзихомукабусикигайся商事法務株式会社,2011, - 218с.

1. 岡村久道　Окамура Хисамити. Тонанадзиасёкоку дзёхосэкюрити-но хорицу 東南アジア諸国情報セキュリティーの法律 (Законодательство в сфере информационной безопасности стран Юго-Восточной Азии). – Токио .東京: Сёдзихомукабусикигайся商事法務株式会社、2010. 403с
2. Охара Бондзи小原凡司. Тюгоку-но гундзи сэнряку 中国の軍事戦略(Военная стратегия Китая). – Токио 東京, Тоёкэйдзай синхося東洋経済新報社, 2014. – 198с.
3. Сонода Хисаси園田寿. Интанэтто то кэйхо インターネットと刑法 (Интернет и Уголовное право). – Токио 東京, Нихонкэйхогаккай日本刑法学会、2001. – 548с.

Сонода Хисаси園田寿. Кэйхо ка кикоэру миэру 刑法が「聞こえる」「見える」(Уголовное право – слышится и видится). – Токио 東京, Нихонсирицудайгакурэммэй日本私立大学連盟, 2000. – 315с.

1. Сонода Хисаси園田寿. Нэттоваку сэкюрити-но кэйдзихотэкихогоネットワークセキュリティの刑事法的保護 (Правовое обеспечение сетевой безопасности). – Токио 東京, Нихонхёронся日本評論社, 2003. – 269с.
2. Танигути Нагаё谷口長世. Сайба дзидай-носэнсоサイバー時代の戦争 (Война в кибер-эпоху). – Токио 東京, NTT сюппан NTT出版, 2010, - 175с.
3. Цутия Мотохиро 土屋大洋. Сайба тэро нитибэй vs. тюгоку サイバーテロ日米vs.中国 (Кибер террор США-Япония против Китая). – Токио東京, Бунгэй сюндзю文藝春秋, 2012 – 258с.
4. Цутия Мотохиро土屋大洋. Нэттоваку пава – дзёходзидай-но кокусай сэйдзиネットワーク・パワー――情報時代の国際政治 (Сила Сети – международная политика в информационную эпоху). – Токио 東京, NTTкабусики гайся NTT出版株式会社, 2007 – 318с.
5. Цутия Мотохиро土屋大洋. Дзёхо ниёру андзэнхосё 情報による安全保障――ネットワーク時代 (Информационная безопасность – Сетевая эпоха). – Токио 東京, Кэйогидзюцудайгакусюппанкай慶應義塾大学出版会, 2007 – 184с.
6. Цутия Мотохиро 土屋大洋. Нэттоваку хэгэмони тэйкоку-носэкайсэнрякуネットワーク・ヘゲモニー「帝国」の世界戦略 (Сетевая гегемония – мировая стратегия «империи»). – Токио 東京, NTT сюппан, 2001 – 243с.
7. Цутия Мотохиро 土屋大洋. Сайба сэкюрити то кокусайсэйдзиサイバーセキュリティと国際政治 (Кибербезопасность и международная политика). – Токио 東京, Тикурасёбо千倉書房, 2015 – 306с.
8. Цутия Мотохиро 土屋大洋, Кимура Тадамаса木村 忠正. Нэттовакудзидай-но гоикэйсэй ネットワーク時代の合意形成 (Формирование взаимопонимания в информационную эпоху). – Токио, 東京, NTT сюппан NTT出版, 1998 – 289с.
9. 日本の刑事施設. 法務省橋正局. [Электронный ресурс]. Доступно из URL: <http://www.moj.go.jp/content/000079580.pdf> (дата обращения 17.10.2015)

1. Saito William. その考え方は、「世界標準」ですか?. 日経BP社, 2012. – P. 312. [↑](#footnote-ref-1)
2. 土屋大洋 Цутия Мотохтро – родился в 1970 году в Токио, окончил юридическое отделение университета Кэйо, которое впоследствии возглавил. Основные работы – 「サイバーテロ日米vs.中国」, 「サイバーテロ・反対対策」. [↑](#footnote-ref-2)
3. 岡村久道　Окамура Хисамити – в прошлом выпускник, а затем и декан юридического факультета государственного университета Киото. Основные работы –　「情報セキュリティーの法律」,　「アジア諸国情報セキュリティーの法律」и проч. [↑](#footnote-ref-3)
4. 小原凡司 Охара Бондзи – выпускник отделения международных отношений Токийского университета, специалист по Японо-Китайским отношениям. Основные работы посвящены военному противостоянию Японии и Китая. Например, 「中国の軍事戦略」 и проч. [↑](#footnote-ref-4)
5. 谷口長世 Танигути Нагаё – глава отделения газеты 毎日新聞 в Брюсселе, родился в городе Нагоя префектуры Айти, выпускник Токийского университета иностранных языков, кафедры французского языка. Основные работы - 「サイバー時代の戦争」,　「NATO – 変象する地域安全保障」. [↑](#footnote-ref-5)
6. Convention on cybercrime., Budapest, 23 November 2001. URL : <http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf> (дата обращения 12.01.2016) [↑](#footnote-ref-6)
7. Lewis, James A. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats / James A. Lewis. Washington D. C., 2002. – Р.12. [↑](#footnote-ref-7)
8. Lewis, James A. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats / James A. Lewis. Washington D. C., 2002. – Р.39. [↑](#footnote-ref-8)
9. Термин «глобальное информационное пространство» получил широкое распространение в социальных науках на рубеже XX – XXI вв. В зарубежных исследованиях и многих международных документах по этой актуальной проблеме названное понятие используется в более узком значении и фигурирует чаще всего как «глобальное киберпространство» (global cyberspace). Большинство исследователей роли информационно - коммуникационных технологий в жизни мирового сообщества рассматривают глобальное информационное пространство как совокупность информационных ресурсов и инфраструктур, которые составляют государственные и межгосударственные компьютерные сети , телекоммуникационные системы и сети общего пользования , иные трансграничные каналы передачи информации . – см. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: Учебник. СПб., 2005. – С. 116. [↑](#footnote-ref-9)
10. Пюкке С. Использование информационной сферы в социальных конфликтах // Компьютера. 2001. - № 40. - С. 48. [↑](#footnote-ref-10)
11. От англ. «cyber crime». См. Aldrich, Richard W. Cyberterrorism and Computer Crimes: Issues Surrounding the Establishment of an International Legal Regime / Richard W. Aldrich. Colorado: USAF Institute for National Security Studies, 2000. – Р.9. [↑](#footnote-ref-11)
12. Сонода Хисаси園田寿. Интанэтто то кэйхо インターネットと刑法 (Интернет и Уголовное право). – Токио 東京, Нихонкэйхогаккай日本刑法学会、2001. – C.47. [↑](#footnote-ref-12)
13. Безопасность: теория, парадигма, концепция, культура. Словарь-справочник / Автор-сост. профессор В. Ф. Пилипенко. 2-е изд., доп. и перераб. — М.: ПЕР СЭ-Пресс, 2005. – С.89. [↑](#footnote-ref-13)
14. Ibid С. 16. [↑](#footnote-ref-14)
15. Шубинский М.И. «Информационная безопасность для работников бюджетной сферы: Учебное пособие». – СПб.:НИУ ИТМО, - 2012. – С. 23. [↑](#footnote-ref-15)
16. Мазуров, В.А. Компьютерные преступления: классификация и способы противодействия/ В.А. Мазуров. М.: «Палеотип», «Логос», 2002. – С. 67. [↑](#footnote-ref-16)
17. Lewis, James A. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats / James A. Lewis. Washington D. C., 2002. – P. 56 . [↑](#footnote-ref-17)
18. Convention on cybercrime., Budapest, 23 November 2001. URL : <http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf> (дата обращения 12.01.2016) [↑](#footnote-ref-18)
19. Сонода Хисаси園田寿. Нэттоваку сэкюрити-но кэйдзихотэкихогоネットワークセキュリティの刑事法的保護 (Правовое обеспечение сетевой безопасности). – Токио 東京, Нихонхёронся日本評論社, 2003. – C.87. [↑](#footnote-ref-19)
20. Ричардсон, Р. Хакеры: дьяволы или святые? / Р. Ричардсон // Журнал сетевых решений. 1998. - Т.4. - С. 108. [↑](#footnote-ref-20)
21. United Nations Manual on the Prevention and Control of Computer-Related Crime Electronic resource. Доступно из URL: http://www.uncjin.org/8th.pdf [Дата обращения: 11.01.2016 г.] [↑](#footnote-ref-21)
22. 岡村久道　Окамура Хисамити. Тонанадзиасёкоку дзёхосэкюрити-но хорицу 東南アジア諸国情報セキュリティーの法律 (Законодательство в сфере информационной безопасности стран Юго-Восточной Азии). – Токио .東京: Сёдзихомукабусикигайся商事法務株式会社、2010. C.196. [↑](#footnote-ref-22)
23. Creating regional cyber maturity metric: Cyber Maturity in Asia-Pacific Region 2015 – Sidney, 2015., Australian Strategic Policy Institute, Р. 5. [↑](#footnote-ref-23)
24. Creating regional cyber maturity metric: Cyber Maturity in Asia-Pacific Region 2014 – Sidney, 2014., Australian Strategic Policy Institute, Р. 21. [↑](#footnote-ref-24)
25. От англ. Cyber maturity – термин, используемый для обозначения уровня развития государства в сфере обеспечения информационной безопасности и борьбы с киберпреступностью. [↑](#footnote-ref-25)
26. От англ. Asia-Pacific Computer Emergency Response Team, APCERT. [↑](#footnote-ref-26)
27. Computer Emergency Readiness Team и Computer Security Incident Response Team (CSIRT). [↑](#footnote-ref-27)
28. Разновидность вредоносной программы, самостоятельно распространяющейся через локальные и глобальные компьютерные сети. [↑](#footnote-ref-28)
29. Университет Карнеги — Меллон (англ. Carnegie Mellon University, CMU) — частный университет и исследовательский центр, расположенный в Питтсбурге, США. [↑](#footnote-ref-29)
30. Task Force - collaboration security incident response teams. [↑](#footnote-ref-30)
31. Creating regional cyber maturity metric: Cyber Maturity in Asia-Pacific Region 2015 – Sidney, 2015., Australian Strategic Policy Institute, P.18. [↑](#footnote-ref-31)
32. Statistics and facts about Internet usage in India. URL: <http://www.statista.com/topics/2157/internet-usage-in-india/> (дата обращения 25.02.2016) [↑](#footnote-ref-32)
33. APCERT Annual Report, 2014, <http://www.apcert.org/documents/pdf/APCERT_Annual_Report_2014.pdf> [↑](#footnote-ref-33)
34. Halder, D.,& Jaishankar, K. (2011b). Cyber crime and victimization of Women: Laws, Rights, and Regulations. Hershey, USA: IGI Global. P.5. [↑](#footnote-ref-34)
35. Halder, D.,& Jaishankar, K. (2011a). Cyber Gender Harassment and secondary Victimization: A Comparative Analysis of US, UK and India. Victims and Offenders, 6(4), P.387. [↑](#footnote-ref-35)
36. National Cyber Security Policy – 2013(NCSP-2013)., 02.06.2013, Ministry of Information and Communication Technology, Department of Electronics and Information Technology/ Preamble. P.1 [↑](#footnote-ref-36)
37. Ibid.P.3. [↑](#footnote-ref-37)
38. Ibid. P.8. [↑](#footnote-ref-38)
39. Ibid.P.8. [↑](#footnote-ref-39)
40. Ibid. P.9. [↑](#footnote-ref-40)
41. Ibid. P.10. [↑](#footnote-ref-41)
42. Ibid.P.10-14. [↑](#footnote-ref-42)
43. The Information Technology Act. Акт парламента Индии №21 принятый 17 октября 2000 года. За основу был Типовой закон об электронной коммерции 1996 рекомендованный Генеральной Ассамблеей ООН в 1997 году. Первоначальная версия содержала 94 секции, разделенные на 19 глав и 4 раздела. [↑](#footnote-ref-43)
44. The Information Technology Act, 2000 (№21 of 2000)., Ministry of Law, Justice and Company Affairs (Legislative Department). New Dehli, 09.06.2000. – P.6-20. [↑](#footnote-ref-44)
45. 岡村久道　Окамура Хисамити. Тонанадзиасёкоку дзёхосэкюрити-но хорицу 東南アジア諸国情報セキュリティーの法律 (Законодательство в сфере информационной безопасности стран Юго-Восточной Азии). – Токио .東京: Сёдзихомукабусикигайся商事法務株式会社、2010. С.247. [↑](#footnote-ref-45)
46. “Norton Cyber Crime Report: The Human Impact”.2013, Norton., from Symantec, USA, 2013. P. 24. [↑](#footnote-ref-46)
47. “Cybercrime survey report, 2014, KPMG in India”. 2014, KPMG international cooperative (“KPMG International”), 2014. P.31. [↑](#footnote-ref-47)
48. От англ. **Certified Ethical Hacker –** специалист, чей уровень знаний в сфере безопасности сетей соответствует официальной международной сертификации. Сертифицированный этичный хакер является квалифицированным специалистом, который понимает и знает, как искать слабые места и уязвимости в целевых системах и использует те же знания и инструменты, что и хакер. [↑](#footnote-ref-48)
49. “Norton Cyber Crime Report”.2012, Norton., from Symantec, USA,2012.P.26. [↑](#footnote-ref-49)
50. От англ. botnet – сеть компьютеров, которая состоит из некоторого количества хостов, с запущенными ботами – программами, которые устанавливаются на компьютер жертвы без ее ведома и дают злоумышленнику возможность выполнять некие действия с использованием ресурсов зараженного компьютера. Ботнет используется для рассылки спама, хищения личных данных пользователей или осуществления атак на отказ в обслуживании. См. Cybercrime survey report, 2014, KPMG in India”. 2014, KPMG international cooperative (“KPMG International”), 2014. [↑](#footnote-ref-50)
51. После смерти Мао Цзэдуна в 1976 г в стране были проведены кардинальные эконмические реформы, осуждению и критике подверглась политика «большого скачка» и «культурной революции»; обострились социальные противоречия, популярность набирало, так называемое, «Движение за демократию» и проч. [↑](#footnote-ref-51)
52. Creating regional cyber maturity metric: Cyber Maturity in Asia-Pacific Region 2015 – Sidney, 2015., Australian Strategic Policy Institute, Р. 43. [↑](#footnote-ref-52)
53. Statistics and facts about Internet usage in China. URL: <http://www.statista.com/topics/1179/internet-usage-in-china/> (Дата обращения: 28.03.2016г.) [↑](#footnote-ref-53)
54. Вид финансового интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. После того, как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам. [↑](#footnote-ref-54)
55. Цутия мотохиро 土屋大洋. Сайба тэро нитибэй vs. тюгоку サイバーテロ日米vs.中国(Кибер террор США-Япония против Китая). – Токио東京, Бунгэй сюндзю文藝春秋, 2012 – С.51. [↑](#footnote-ref-55)
56. 工業和信息化部 - созданное в 2008 году ведомство КНР, ответственное за регулирование и развитие в стране почтовой связи, Интернета, беспроводной связи, теле- и радиовещания, производства электронных и информационных товаров, индустрии программного обеспечения и развитие информационного общества. [↑](#footnote-ref-56)
57. 公安部 - орган исполнительной власти КНР, в чьи обязанности входит выполнение полицейских функций, охрана общественного порядка, защита политического и государственного строя, высшего руководства государства и важных государственных объектов, антитеррористическая борьба против экстремизма и сепаратизма на территории Китая. Имеет те же функции, что и Министерство внутренних дел в других странах. [↑](#footnote-ref-57)
58. 国家保密局 - орган Государственного совета КНР, который отвечает за защиту государственной тайны. Наряду с государственным органом по защите государственных тайн, в КНР также существует аналогичный партийный орган — «Центральный комитет по защите государственной тайны», подчинённый Центральному комитету Коммунистической партии Китая. [↑](#footnote-ref-58)
59. Pi Yong. New China Criminal Legislations in the Progress of Harmonization of Criminal Legislation against Cybercrime ., 2001. - P.8. [↑](#footnote-ref-59)
60. Ibid. P. 16. [↑](#footnote-ref-60)
61. Ibid. P. 19. [↑](#footnote-ref-61)
62. Ibid.P.28. [↑](#footnote-ref-62)
63. Criminal Law of the People’s Republic of China. Article 286. URL: <https://www.oecd.org/site/adboecdanti-corruptioninitiative/46814270.pdf> (Дата обращения: 28.03.2016г.) [↑](#footnote-ref-63)
64. Статья 312 гласит, что лицо, занимающееся торговлей нелегально приобретенными товарами, подлежит наказанию в виде лишения свободы сроком до 3 лет или штрафа. См. Criminal Law of the Peoples’s Republic of China. Article 312. URL: <https://www.oecd.org/site/adboecdanti-corruptioninitiative/46814270.pdf> (Дата обращения: 28.03.2016г.) [↑](#footnote-ref-64)
65. Охара Бондзи小原凡司. Тюгоку-но гундзи сэнряку 中国の軍事戦略(Военная стратегия Китая). – Токио 東京, Тоёкэйдзай синхося東洋経済新報社, 2014. – С.47.　 [↑](#footnote-ref-65)
66. Ibid. С.82.　 [↑](#footnote-ref-66)
67. Convention on cybercrime., Budapest, 23 November 2001. – P.2. [↑](#footnote-ref-67)
68. Ibid.P. 13. [↑](#footnote-ref-68)
69. Statistics and facts about Internet usage in South Korea. URL: <http://www.statista.com/topics/2230/internet-usage-in-south-korea/> (Дата обращения: 06.11.2015г.) [↑](#footnote-ref-69)
70. Cho Kyon Seok. The Current Situation of Measures for Crime Victims in the Korean Criminal Justice System. URL: <http://www.unafei.or.jp/english/pdf/RS_No81/No81_10VE_Seok.pdf> (дата обращения 16.03.2016) [↑](#footnote-ref-70)
71. Junsik Jang. Best Practices in Cybercrime Investigation in the Republic of Korea, <http://www.unafei.or.jp/english/pdf/RS_No79/No79_09VE_Jang2.pdf> (дата обращения 16.03.2016) [↑](#footnote-ref-71)
72. Dos – Denial of Service – тип хакерской атаки на вычислительную систему с целью доведения ее до отказа, т.е. создание таких условий, при котором легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам, либо этот доступ затруднен. [↑](#footnote-ref-72)
73. Окамура Хисамити岡村久道 . Кодзиндзёхохого 個人情報保護法(Законодательство в сфере обеспечения безопасности персональных данных). Токио .東京: Сёдзихомукабусикигайся商事法務株式会社、2011.С.78. [↑](#footnote-ref-73)
74. Korean Central Intelligence Agency (KCIA) (중앙정보부). [↑](#footnote-ref-74)
75. The Korea Internet & Security Agency (한국인터넷진흥원, KISA). [↑](#footnote-ref-75)
76. От англ. «White paper» - официальное сообщение в письменном виде. Это может быть государственное сообщение, поясняющее политику; справочный документ для корпоративных клиентов; официальная документация, содержащая описание решения. [↑](#footnote-ref-76)
77. Creating regional cyber maturity metric: Cyber Maturity in Asia-Pacific Region 2015 – Sidney, 2015., Australian Strategic Policy Institute. P.54. [↑](#footnote-ref-77)
78. Junsik Jang. Best Practices in Cybercrime Investigation in the Republic of Korea, <http://www.unafei.or.jp/english/pdf/RS_No79/No79_09VE_Jang2.pdf> [↑](#footnote-ref-78)
79. The Act on Promotion of Information and Communications network utilization and data protection, etc. URL: <http://www.koreanlii.or.kr/w/images/d/df/DPAct2014_ext.pdf> (Дата обращения: 16.12.2015г.) [↑](#footnote-ref-79)
80. Act on the protection of Information and communications infrastructure. URL: [http://www.law.go.kr/LSW/LsInfoP.do?lsiSeq=136754#](http://www.law.go.kr/LSW/LsInfoP.do?lsiSeq=136754) (Дата обращения 21.12.2015г.) [↑](#footnote-ref-80)
81. Окамура Хисамити岡村久道 . Кодзиндзёхохого 個人情報保護法(Законодательство в сфере обеспечения безопасности персональных данных). Токио .東京: Сёдзихомукабусикигайся商事法務株式会社、2011. С .64. [↑](#footnote-ref-81)
82. 岡村久道　Окамура Хисамити. тонанадзиасёкоку дзёхосэкюрити-но хорицу 東南アジア諸国情報セキュリティーの法律 (Законодательство в сфере информационной безопасности стран Юго-Восточной Азии). Токио .東京: Сёдзихомукабусикигайся商事法務株式会社、2010. С .41. [↑](#footnote-ref-82)
83. Act on Promotion of Information and Communications network utilization and Information Protection. URL: <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN025694.pdf> (Дата обращения 18.12.2015г.) [↑](#footnote-ref-83)
84. Act on Promotion of Information and Communications network utilization and Information Protection. URL: <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN025694.pdf> P. 6. (Дата обращения 18.12.2015г.) [↑](#footnote-ref-84)
85. Ibid. P.7. [↑](#footnote-ref-85)
86. Ibid. P. 9. [↑](#footnote-ref-86)
87. Ibid. P. 12. [↑](#footnote-ref-87)
88. Ibid. P. 15. [↑](#footnote-ref-88)
89. Ibid. P.24. [↑](#footnote-ref-89)
90. Junsik Jang. Best Practices in Cybercrime Investigation in the Republic of Korea. URL: <http://www.unafei.or.jp/english/pdf/RS_No79/No79_09VE_Jang2.pdf> (дата обращения 16.02.2016) [↑](#footnote-ref-90)
91. Ibid. P. 44. [↑](#footnote-ref-91)
92. APCERT Annual Report, 2014, <http://www.apcert.org/documents/pdf/APCERT_Annual_Report_2014.pdf>. P.64. [↑](#footnote-ref-92)
93. APCERT Annual Report, 2014, <http://www.apcert.org/documents/pdf/APCERT_Annual_Report_2014.pdf>.P.66. [↑](#footnote-ref-93)
94. Statistics and facts about Internet usage in Japan. URL: <http://www.statista.com/topics/2361/internet-usage-in-japan/> (дата обращения 08.11.2015г.) [↑](#footnote-ref-94)
95. Ibid. [↑](#footnote-ref-95)
96. Deloiette’s Asia-Pacific Defence Outlook 2016. URL: <http://www2.deloitte.com/sg/en/pages/public-sector/articles/deloitte-2016-asia-pacific-defense-outlook.html> (дата обращения 13.01.2016) [↑](#footnote-ref-96)
97. Уильям Хироюки Сайто (ウィリアム 浩幸 齋藤) – переводчик, общественный деятель, специальный советник премьер-министра Японии по киберполитике. [↑](#footnote-ref-97)
98. William Saito. "ザ・チーム 日本の一番大きな問題を解く".日経BP社, 2012. – P. 74. [↑](#footnote-ref-98)
99. Танигути Нагаё谷口長世. Сайба дзидай-носэнсоサイバー時代の戦争 (Война в кибер-эпоху). – Токио 東京, NTT сюппан NTT出版, 2010, - C.86. [↑](#footnote-ref-99)
100. Охара Бондзи小原凡司. Тюгоку-но гундзи сэнряку 中国の軍事戦略(Военная стратегия Китая). – Токио 東京, Тоёкэйдзай синхося東洋経済新報社, 2014. – С.38.　 [↑](#footnote-ref-100)
101. Хисанага Рюити久永隆一. Фуёна тэйсэй мотомэру бунсё, 1.9 ман нин ни аяама софунэнкин кико不要な訂正求める文書、１．９万人に誤送付　年金機構 // Асахи Симбун 朝日新聞. Токио 東京, 28.04.2016. URL: <http://www.asahi.com/articles/ASJ4X5H8NJ4XUTFL00Y.html> [↑](#footnote-ref-101)
102. マイナンバーと言う制動がはじまるとどうなるの?// Режим доступа: <http://www.gov-online.go.jp/tokusyu/mynumber/point/#sec1> (Дата обращения 25.10.2015г.) [↑](#footnote-ref-102)
103. 独立行政法人情報処理推進機構（じょうほうしょりすいしんきこう）、Information-technology Promotion Agency. [↑](#footnote-ref-103)
104. Правительство Японии отказывалось принять Стратегию от 2013 года в силу того, что она нарушала статью 21, раздел 2 Конституции Японии о тайне любых средств общения. [↑](#footnote-ref-104)
105. Ibid С.4. [↑](#footnote-ref-105)
106. NISC, “Waga kuni no saiba sekyuriti suishin taisei no kino kyoka ni kansuru torikumi hoshin [Policy to Enhance Japan’s Cyber Security],” November 25, 2014,   
     [http://www.nisc.go.jp/conference/seisaku/dai41/pdf/houshin20141125.pdf, 6.](http://www.nisc.go.jp/conference/seisaku/dai41/pdf/houshin20141125.pdf)  [↑](#footnote-ref-106)
107. 警察庁,National Police Agency. [↑](#footnote-ref-107)
108. 総務省,Тhe Ministry of Internal Affairs and Communications. [↑](#footnote-ref-108)
109. 防衛省,The Ministry of Defense. [↑](#footnote-ref-109)
110. NISC, “Waga kuni no saiba sekyuriti suishin taisei no kino kyoka ni kansuru torikumi hoshin [Policy to Enhance Japan’s Cyber Security],” November 25, 2014,   
     [http://www.nisc.go.jp/conference/seisaku/dai41/pdf/houshin20141125.pdf, 12.](http://www.nisc.go.jp/conference/seisaku/dai41/pdf/houshin20141125.pdf,%2012.%20)  [↑](#footnote-ref-110)
111. NISC, “Shiryo 1-1 ‘Waga kuni no saiba sekyuriti suishin taisei no kino kyoka ni kansuru torikumi hoshin (an)’ gaiyo [Outline of Policy to Enhance Japan’s Cyber Security (draft),” November 25, 2014,   
     <http://www.nisc.go.jp/conference/seisaku/dai41/pdf/41shiryou0101.pdf> [↑](#footnote-ref-111)
112. Ibid [↑](#footnote-ref-112)
113. Nihon Keizai Shimbun, “Saiba kogeki taisaku de Senryaku Honbu Seihu, 15 nen 1 gatsu nimo secchi [Japanese government will launch the Cyber Security Strategy Headquarters to deal with cyber-attacks in January 2015],” November 25, 2014,   
     <http://www.nikkei.com/article/DGXLASFS25H3G_V21C14A1PP8000/> [↑](#footnote-ref-113)
114. “Fusei akusesu gyoui no kinshitou ni kansuru no houritsu no kaitetsu[Explanation of Laws concerning acts of unauthorized access ”<https://www.npa.go.jp/cyber/legislation/pdf/1_kaisetsu.pdf> [↑](#footnote-ref-114)
115. 不正アクセス行為の禁止等に関する法律. URL: <http://www.npa.go.jp/cyber/legislation/pdf/2_houritsujoubun.pdf> (Дата обращения: 08.10.2015г.) [↑](#footnote-ref-115)
116. Уголовный кодекс Японии. Ст.258. URL: <http://law.e-gov.go.jp/htmldata/M40/M40HO045.html> (дата обращения 16.02.2016г.) [↑](#footnote-ref-116)
117. Уголовный кодекс Японии. Ст.259. URL: <http://law.e-gov.go.jp/htmldata/M40/M40HO045.html> (дата обращения 16.02.2016г.) [↑](#footnote-ref-117)
118. Уголовный кодекс Японии. Ст.175. URL: <http://law.e-gov.go.jp/htmldata/M40/M40HO045.html> (дата обращения 16.02.2016г.) [↑](#footnote-ref-118)
119. Закон о наказании за деятельность, связанную с детской проституцией и детской порнографией, 1999г. URL: <http://taroyamada.jp/wp-content/uploads/2014/05/f7f0f191e6ccf9c3b31f1399957cac8d.pdf> (дата обращения 26.11.2015г.) [↑](#footnote-ref-119)
120. サイバーセキュリティ基本法案, The Basic Act on Cybersecurity. [↑](#footnote-ref-120)
121. Акт об основах кибербезопасности. サイバーセキュリティ基本法案. URL: <http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/houan/g18601035.htm> (дата обращения 19.12.2015г.) [↑](#footnote-ref-121)
122. Ibid. [↑](#footnote-ref-122)
123. Ibid. [↑](#footnote-ref-123)
124. Ibid. [↑](#footnote-ref-124)
125. Ibid. [↑](#footnote-ref-125)
126. 内閣サイバーセキュリティーセンター, National Center of Incident readiness and Strategy for Cybersecurity (NISC). [↑](#footnote-ref-126)
127. Japan Vulnerability notes. URL: <https://jvn.jp/nav/jvn.html> (дата обращения 23.03.2016) [↑](#footnote-ref-127)
128. Танигути Нагаё谷口長世. Сайба дзидай-носэнсоサイバー時代の戦争 (Война в кибер-эпоху). – Токио 東京, NTT сюппан NTT出版, 2010, - C.16. [↑](#footnote-ref-128)