Региональная конференция по модели ООН
KhaMUN2017
"Вызовы 21 века: сотрудничество в целях устойчивого развития"

Генеральная Ассамблея

Руководство по теме:

«Кибербезопасность как основа стабильного развития информационного общества»

Содержание

Основные термины

Наиболее распространенное определение кибербезопасности даётся в руководящих указаниях по кибербезопасности (ISO/IEK 27032 2012 года):

Кибербезопасность – условия защищенности от физических, духовных, финансовых, политических, эмоциональных, профессиональных, психологических, образовательных или других типов воздействий, или последствий аварии, повреждения, ошибки, несчастного случая, вреда или любого другого события в киберпространстве, которые могли бы считаться не желательными.

Так же существуют термины, не закреплённые в мировом праве, но, как правило, их трактовка сводится к следующему:

Кибервойна – противостояние в сети Интернет, направленное, в первую очередь, на выведение из строя компьютерных систем госорганов страны-противника, а также систем ее критических отраслей инфраструктуры.

Кибератака – несанкционированное воздействие на вычислительную систему специальными программными средствами с целью нарушения её работ, получения засекреченной информации и т.п.

Эксперты выделяют несколько видов атак в глобальной сети Интернет: вандализм, пропаганда, сбор информации, отказ сервиса, вмешательство в работу оборудования, а также атаки на узлы инфраструктуры.

Вандализм – использование интернета для порчи web-страниц, замены контента оскорбительными или пропагандистскими картинками.

Пропаганда – рассылка сообщений пропагандистского характера.

Сбор информации – взлом частных страниц или серверов для сбора секретной информации или ее замены на фальшивую, полезную другому государству.

Отказ сервиса – атаки на компьютерные системы, направленные на дестабилизацию работы атакованного сайта или компьютера.

Вмешательства в работу оборудования – атаки на компьютеры, контролирующие работу гражданского или военного оборудования, что приводит к его отключению или поломке.

Атаки на узлы инфраструктуры – атаки на компьютеры, обеспечивающие жизнедеятельность городов, их инфраструктуры, таких как телефонные системы, системы водоснабжения, электроэнергетика, пожарная охрана или транспорт.

Краткое содержание проблемы

История появления и эволюции компьютерных вирусов, сетевых червей, троянских программ представляет собой достаточно интересный для изучения предмет. Зародившись как явление весьма необычное, как компьютерный феномен, в 1980-х годах, примитивные вирусы постепенно превращались в сложные технологические разработки, осваивали новые ниши, проникали в компьютерные сети. Идея вируса, заражающего другие программы и компьютеры, за двадцать лет трансформировалась в криминальный бизнес.

В 1980-х компьютеры становятся всё более и более популярными. Появляется всё больше и больше программ, авторами которых являются не фирмы-производители программного обеспечения, а частные лица. Развитие телекоммуникационных технологий даёт возможность относительно быстро и удобно распространять эти программы через серверы общего доступа — BBS (Bulletin Board System). Позднее, полулюбительские, университетские BBS перерастают в глобальные банки данных, охватывающие практически все развитые страны. Они обеспечивают быстрый обмен информацией между самыми удаленными точками планеты. «Глобальная сеть» серверов BBS становится популярной и в результате привлекает внимание программистов-хулиганов. Появляется большое количество разнообразных «троянских коней» — программ, не имеющих способности к размножению, но при запуске наносящих системе какой-либо вред в виде безвозвратного удаления всех файлов в папке, переименование всех файлов, удаление всех иконок с рабочего стола и даже изменение текущей учетной записи.

Будучи изначально творчеством вирусописателей-исследователей, компьютерные вирусы сначала стали чем-то вроде развлечения в руках одарённых юных программистов, создававшие первые вредоносные ПО с целью розыгрыша, а позднее оружием в руках интернет-преступников, требовавших

выкуп за разблокировку зашифрованных данных или просто уничтожавших важную правительственную информацию.

Самыми яркими представителями вирусных программ прошлой эпохи были: червь I love you, выпущенный на Филиппинах в мае 2000 года, который нанес владельцам компьютеров ущерб на сумму, по некоторым оценкам превышающую $10 млрд. Следующий червь, вошедший в историю как Code Red, за 14 часов сумел заразить более 300 тыс. компьютеров, подключенных к Интернету, даже защита белого дома США на тот момент не смогла отбить кибератаки. После них были и другие, часто — первые в определенной категории. Например, Nimda (слово admin, прочитанное наоборот), многовекторный червь, распространялся сразу несколькими способами, включая «черные ходы», оставленные другими червями. MyDoom был признан самым быстрым червем, распространяю щимся по электронной почте.

Однако технологии не стоят на месте, также, как и киберпреступления последних 20-ти лет, которые останавливали деятельность некоторых компаний на неопределенный срок или же ограничивали доступ к сети Интернет для целой страны. Самыми именитыми из них являются:

1) Неоднократный взлом американского космического агентства NASA

2) Взлом системы безопасности Пентагона (2000 год), в ходе которого были украдены коды программы наведения ракет и стратегических спутников.

3) Взлом системы безопасности банка RBS WorldPay, в результате которого были одновременно сняты 9 миллионов долларов по всему миру (2008 год)

4) В Иране были выведены из строя аппараты по переработке и обогащению урана, что могло привести к критическим последствиям. Наиболее часто в этой кибератаке винят США. (2010)

5) Китайские хакеры использовали методы фишинга, чтобы заразить вредоносным ПО компьютеры европейских участников G20, заседающих на

встрече в Санкт-Петербурге. В итоге хакеры получили доступ к подробностям предлагаемого военного вмешательства США в Сирии (2013 год).

Сегодня общие годовые потери всех коммерческих организаций от действий вирусов могут сравниться с бюджетом небольшой страны и эта сумма каждый год удваивается. Прогнозируют, что к 2021 году потери возрастут до 9 триллионов долларов. Заявления некоторых специалистов по безопасности свидетельствуют о серьезности проблемы. По сведениям экспертов, в 1999 году фиксировалось в среднем по одному новому вирусу в час, в 2000 году эта цифра составляла уже по одной программе каждые три минуты, а в 2004 году это время сократилось до нескольких секунд. По данным Санкт- Петербургской антивирусной лаборатории И. Данилова (ООО «СалД»), только за март 2007 года в антивирусную базу добавлено более 7 тыс. записей.

На сегодняшний день обстановка в мире крайне напряженная, причин этому несколько:

1) Хакерские группировки, действующие вне своих государств, подрывают до стран друг к другу;

2) Подозрения некоторых государств в промышленном и интернациональном шпионаже.

Согласно данным исследования крупной компании, занимающей разработкой антивирусного ПО, самыми развитыми кибервойсками в мире в настоящее время обладают США. По мнению аналитиков, государственное финансирование этого направления в Штатах может составлять около $7 млрд в год, а численность хакеров, сотрудничающих с государством, — 9 тыс. человек.

На втором месте находится Китай, где финансирование данного направления может составлять $1,5 млрд в год, а киберармия оценивается как самая многочисленная, до 20 тыс. человек.

Тройку стран, где наиболее развиты спецподразделения по кибербезопасности, замыкает Великобритания, выделяющая кибервойскам,

состоящим из 2 тыс. человек, $450 млн в год. На четвертом месте Южная Корея с бюджетом $400 млн в год и составом в 700 хакеров. На пятом месте Россия, чьи расходы на кибервойска составляют около $300 млн в год, а численность российских спецподразделений составляет примерно 1 тыс. человек.

На 2015 год около 60 стран занимаются разработкой средств компьютерного шпионажа, хакерских атак и наблюдения. В общей сложности 29 стран, включая Китай, Данию и Францию, имеют специализированные военные киберподразделения, занимающиеся противодействием угрозам информационной безопасности. В то же время 49 стран, включая Россию, Австралию, Бразилию и Египет, закупают специализированное хакерское программное обеспечение, а 63 страны, включая Чехию, Италию и Мексику, используют инструменты сплошного наблюдения как внутри страны, так и глобально, говорилось в исследовании WSJ. Создание и использование кибервооружений не требует колоссальных вложений в обогатительные заводы, разработку средств доставки и строительство пусковых установок.

Достаточно не обладать большими финансовыми ресурсами и высокопроизводительными компьютерными системами, достаточно доступа к глобальным сетям. Кибератаки сложно остановить и зачастую невозможно отследить.

Благодаря этому инструменты хакерских атак стали доступны не только правительствам, но и агрессивным политическим группировкам и террористическим организациям, таким как ХАМАС, который пытается заполучить засекреченную информацию путём внедрения троянских программ в мобильные телефоны солдат ЦАХАЛа. Так же не стоит забывать об запрещенной организации напрямую связанную с ИГИЛом - Киберхалифат, которые в 2015 году взломали более 54 000 аккаунтов в социальной сети "Twitter». В ответ на агрессию со стороны США, Россия была вынуждена пересматривать свою военную доктрину в сфере кибербезопасности.

Последними шагами к стабилизации положения в мировом информационном сообществе является создание Проекта глобального пакта об электронном ненападении, датированного 2015 годом.

В соответствии с достигнутыми договоренностями государства обязуются использовать кибертехнологии «исключительно в мирных целях». Среди прочего предполагается, что они не будут атаковать объекты критически важной инфраструктуры друг друга (АЭС, банки, системы управления транспортом и т. п.), перестанут вставлять вредоносные «закладки» (вредоносный софт) в производимую ими ИТ-продукцию, воздержатся от огульного обвинения друг друга в кибератаках и начнут прилагать усилия по борьбе с хакерами, осуществляющими компьютерные диверсии с их территории или через нее[1].

Работа над текстом документа велась несколько лет. Теперь, как ожидается, он должен поступить на обсуждение в Генеральную ассамблею ООН.

В конечный текст документа не вошло предложение США о том, чтобы распространить международные правовые нормы на киберпространство. Против него выступили Россия, Белоруссия, Китай и другие страны, решившие, что такая мера может закрепить гегемонию США в киберпространстве. Также в текст не попало предложение США о возможности использования силовых методов для ответа на кибератаки — представители Китая выступили против, потому что это бы привело к милитаризации киберпространства, хотя не раз представительство Китая высказывалось о том, что готов предпринять все необходимые меры для защиты своей кибербезопасности, не исключая возможности применения военной силы.

Однако из-за специфики кибертехнологий пока совершенно непонятно, как контролировать его выполнение. Исполнение также не обязательно, ведь все пункты настоящего договора носят сугубо рекомендательный характер. Обстановка осложняется тем, что на протяжении нескольких лет, пока создавался данный договор, доверие стран друг к другу было подорвано несколько раз, как

реальными кибератаками, так и подозрениями в их свершении.

Такая ситуация опасна еще и потому, что ведущие кибердержавы — включая Россию и США — официально приравняли кибератаки к традиционным военным действиям, заявив о своем праве реагировать на них как на акт агрессии. А поскольку отследить источник атаки в киберпространстве очень сложно, то возможна провокация стран третьей стороной.

Обстановка ещё более накаляется тем, что такие термины как «кибератаки», «кибероперации» или «компьютерные сетевые атаки» не имеют согласованного на международном уровне правового определения и используются в разных контекстах и с разным значением. То есть страны, имея свободную трактовку таких важных терминов способны применять военный действия к любым источникам потенциально угрозы.

Значительная часть кибероперацій сегодня, определяемых как «кибератаки», являются нелегальным сбором информации или преступлениями в области компьютерных технологий и не регулируются нормами международного гуманитарного права. Эксперты напоминают, что не стоит пренебрегать разрушительным потенциалом, которым обладает на сегодняшний день кибероружие.

Для недопущения прямовыраженной агрессии в 2013 году была запущена горячая линия между Россией и США для обмена информацией для предотвращения перерастания киберинцидентов в полномасштабный кризис. Аналог данной системы был запущен только в период "Холодной войны".

При сохранении существующих тенденций, которые заключаются только в наращивание военной мощи и бюджета кибероборонь различных стран, увеличения недоверия и закрытости информационных сообществ, любые конфронтации интересов кибергосударств могут вылиться в кровопролитные войны - в худшем случае, а в лучшем - к затяжным экономическим санкциям,

способным погрузить несколько десяток мировых экономик в стадию стагнации или деградации.

Таким образом, государствам необходимо активно налаживать контакты друг с другом по всем основным вопросам киберугроз. На данный момент, вероятно, мы не можем с полной уверенностью говорить о глобальном соглашении по сотрудничеству в сфере информационной безопасности; однако, широкие двусторонние контакты будут способствовать формированию устойчивого и безопасного информационного пространства.

Список рекомендуемых источников

1. http://www.itu.int/ru - Международный Союз электросвязи
2. http://www.securitylab.ru/ - Информационный портал по безопасности
3. http://www.un.org/ru/ecosoc/itu/ - Международный союз электросвязи
4. http://www.cybersecurity.ru/ - Мировые новости высоких технологий
5. http://www.kaspersky.ru/ - Лаборатория Касперского
6. http://www.icrc.org - Международный комитет красного креста
7. https://www.microsoft.com/ru-ru/devcenter/Research.aspx - Центр исследований Майрософт
8. https://fas.org/irp/doddir/army/pam525-7-8.pdf - Концепция возможности киберпространства
9. https://www.un.org/disarmament/ru - Управление ООН по вопросам разоружения
10. http://www.journal.ib-bank.ru/ - Журнал информационной безопасности банков
11. http://www.cyberrus.com - Журнал Кибербезопасности
12. http://www.cisco.com/ - Сайт сетевой ТНК
13. http://cyberseclab.ru/ - Лаборатория кибербезопасноти
14. http://icenter.ru/fullsubject/vkb - Вестник безопасности
15. http://www.ipg-journal.io/ - Журнал международной политики