КИБЕРБЕЗОПАСНОСТЬ – ПОДХОДЫ К ОПРЕДЕЛЕНИЮ ПОНЯТИЯ

***Безкоровайный Михаил Михайлович**, кандидат технических наук, доцент*
***Татузов Александр Леонидович**, доктор технических наук, доцент*

Существенный рост инцидентов, возникающих в информационной сфере, привел к необходимости системного анализа источников возникновения угроз. Для этого необходимы согласованные среди специалистов понятия, ключевым из которых является кибербезопасность. Оно трактуется неоднозначно многими экспертами. В статье предлагается подход к рассмотрению понятия киберпространства и кибербезопасности.

***Ключевые слова**: информационная безопасность, кибербезопасность, киберпространство, киберпреступления.*

CYBERSECURITY - APPROACHES TO THE DEFINITION

***Mikhail Bezkorovainy**, Ph.D. , Associate Professor*
***Alexander Tatuzov**, Doctor of Technical Sciences , Associate Professor*

Many experts treat this concept in different ways. The paper proposes an approach to the consideration of cyberspace and cybersequrity.

***Keywords**: information security, cybersecurity , cyberspace , cybercrime .*

В настоящее время наблюдается резкий рост инцидентов в области информационной безопасности, которые имеют широкое распространение и приобретают угрожающий характер. Многие из подобных атак затрагивают широкий круг частных, корпоративных, а также государственных интересов.

Главными тенденциями развития угроз являются следующие:

- рост числа атак, многие из которых ведут к большим потерям;
- возрастание сложности атак, которые могут включать несколько этапов и применять специальные методы защиты от возможных методов противодействия;
- воздействие практически на все электронные (цифровые) устройства, в числе которых в последнее время все большую значимость приобретают мобильные устройства, а они в наибольшей степени подвержены рискам в области информационной безопасности;
- все более частые случаи нападения на информационную инфраструктуру крупных корпораций, важнейших промышленных объектов и даже государственных структур;
- применение наиболее развитыми в области компьютерных технологий странами средств и методов кибернападения на другие государства.

Это подтверждается практически ежедневными сводками новостей, в которых сообщается о новых атаках преступников в информационной сфере.

Число вредоносных объектов, которые обнаруживаются в сети ежегодно, исчисляется миллиардами, их распространение ведется более чем 100 миллионов интернет адресов [1] [2]. Каждый год это число увеличивается на 40% [3]. Атаки в информационном пространстве наносят ущерб, который оценивается в 100 миллиардов долларов [4]. По заявлению начальника Бюро специальных технических мероприятий МВД России Алексея Мошкова каждую секунду 12 человек на Земле становятся жертвами киберпреступников. Только в России удалось предотвратить хищение около 1 миллиарда рублей с банковских счетов граждан [5].

Особую опасность составляют угрозы мобильным устройствам, которые ранее редко подвергались атакам. За один год практически в 30 раз увеличилось количество Android-троянцев [3].

Появились крайне сложные элементы нападения, направленные на ухудшение работы промышленных объектов. Это обнаруженный в 2009 г.,

и наделавший много шума червь Stuxnet, разработки этого года Duqu и Flame, последний из которых имеет очень сложную архитектуру. Стало известно о причастности специалистов американских спецслужб к созданию этих комплексных вредоносных программ. Государственными структурами ведется финансирование нападений в области киберпространства [6].

Зафиксированы многочисленные атаки на крупнейшие банки США. Эти атаки смогли взломать передовые системы защиты и создать угрозы национальной инфраструктуре. Предположительно, нападения чаще всего организуются из Китая [7]. В начале года была проведена серия атак на крупнейшие американские СМИ [8], что заставило правительство США еще раз серьезно задуматься об усилении кибербезопасности в стране [9].

В 2013 г. Лабораторией Касперского была опубликована информация о совершенно новом явлении в области компьютерных атак. Была раскрыта шпионская сеть «Красный Октябрь (Red October)», на протяжении пяти лет занимающаяся хищением государственных секретов. Это сложнейший комплекс вредоносных программ, около 1000 вредоносных файлов, относящихся к 30 различным группам модулей [10]. Аналогичные методы уже активно применяются и для мобильных устройств на платформе Android [11].

В конце 2012 г. американские и китайские государственные структуры публично высказали свои подозрения в создании оборудования с недокументированными возможностями, посредством которых из одного государства были атакованы сети другой страны. Под подозрением оказалась продукция фирм Huawei и ZTE с китайской стороны и Cisco с американской стороны [12].

Заявления Эдварда Сноудена подтверждают активное участие государственных структур развитых стран в сборе информации о гражданах, чиновниках, корпорациях и других, казалось бы, общедоступных сведений, которые можно агрегировать для достижения кумулятивного эффекта и получения закрытой информации. С целью манипулирования общественным мнением масс людей активно применяются специальные методы социальной инженерии, во многом опирающиеся на средства коммуникаций с помощью Интернета.

Таким образом, имеется ряд проблем в сфере информационной безопасности, которые не могут быть полноценно решены традиционными средствами и на которые следует обратить внимание обществу и государственным органам. Масштабные нарушения, затрагивающие все стороны жизни общества, в основе которых лежат новейшие методы осуществления атак на компьютерные сети, а также управление общественным сознанием требуют системного подхода к созданию комплексной системы безопасности, способной противостоять этим угрозам.

Общий анализ проблематики защиты от подобных, вновь возникающих и продолжающих развиваться угроз, можно обозначить понятием кибербезопасность. Вопросы обеспечения кибербезопасности были проанализированы в работе [13] и была показана необходимость принятия масштабных мер со стороны государства по обеспечению безопасности в области информационных и телекоммуникационных технологий (далее – ИКТ). Речь идет о координации усилий в этом направлении государственных органов, бизнеса и общества в целом.

Столь сложная задача должна решаться на основе ясно выработанной позиции, однозначном понимании того, что имеется в виду под кибербезопасностью. В работе [14] рассмотрены подходы к выработке терминологии в этой области.

Очевидно, что кибербезопасность должна быть нацелена на обеспечение защиты в киберпространстве. Поэтому основным для анализа проблем кибербезопасности является понятие киберпространство.

Для понимания его содержания целесообразно основываться на термине кибернетика. Кибернетика (от греч. «искусство управления») – наука об управлении, связи и переработке информации.

Абстрактная кибернетическая система представляет собой множество взаимосвязанных объектов, называемых элементами системы, способных воспринимать, хранить и перерабатывать информацию, а также обмениваться информацией. То есть, к предметной области кибернетики относятся все современные информационные и телекоммуникационные технологии. Важно, что в рамках кибернетического подхода элементы системы рассматриваются как непрерывно взаимодействующие между собой и в качестве важных составляющих элементов в киберпространство включены люди – активные участники информационного обмена и использования информационных ресурсов.

В начале 2014 г. Советом Федерации для публичного обсуждения был предложен проект Концепции Стратегии кибербезопасности Российской Федерации (далее – Концепция). Он призван определить направления усилий государства в отношении новых угроз, возникающих в современном информационном мире [15].

Понятие кибербезопасности очень многогранно и поэтому непросто и трудно формализуемо.

Здесь существует очень много различных представлений и взглядов.

Специалисты по информационной безопасности и просто заинтересованные пользователи, в частности, те, которые оставили комментарии к Концепции, высказывают очень противоречивые взгляды на эту проблематику. Анализ комментариев показывает, что одной из основных проблем разработки подобных документов заключается в трудности понимания термина киберпространство и соотнесенным с ним понятием кибербезопасность.

Киберпространство в проекте Концепции определяется следующим образом:

«Киберпространство – сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)».

В принципе, такое определение в какой-то степени трактует отдельные аспекты этого важного понятия, но отсутствие дальнейших подробных разъяснений приводит к неточному его пониманию. Абсолютное большинство экспертов, которые оставили свои комментарии к проекту Концепции, считают, что в определении речь идет исключительно о технологической составляющей информационного поля, то есть о компьютерной и телекоммуникационной инфраструктуре. Совсем упущен из рассмотрения вопрос о деятельности на основе этой инфраструктуры и любых видах человеческой активности, которая осуществляется посредством технологий. А об этом прямо сказано в определении. Для документа, имеющего столь важное значение это неприемлемо и указывает на необходимость дальнейшей методологической работы по определению кибербезопасности как характеристики киберпространства.

Приведенное в концепции определение во многом перекликается с позицией международного стандарта ИСО/МЭК 27032:2012 Руководящие указания по кибербезопасности (ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity).

Киберпространство – это сложная среда, не существующая ни в какой физической форме, возникающая в результате взаимодействия людей, ПО, интернет сервисов посредством технологических устройств и сетевых связей.

В программной статье по кибербезопасности специалистами Великобритании определяется это понятие как *всякая деятельность в сетевой, цифровой форме*, добавляя после этого, что *сюда же относятся информационное содержание и действия осуществляемые посредством цифровых сетей*. (Klimburg A. et al. National cyber security framework manual //NATO CCD COE Publications (December 2012). – 2012. http://belfercenter.hks.harvard.edu/files/hathaway-klimburg-nato-manual-ch-1.pdf).

При всем многообразии этих определений можно отметить, что при четком указании на связанность киберпространства с ИКТ инфраструктурой, основное внимание обращено не на технологии, а на деятельность людей, которые используют эти технологии.

Важно, что основное содержание киберпространства заключается в деятельности пользователей цифровыми информационными ресурсами и ИКТ инфраструктурой. Киберпространство можно рассматривать как триаду, которая включает в себя три основные составляющие.

Информация в ее цифровом представлении: статическом (файлы, записанные на носители данных) и динамическом (пакеты, потоки, команды, запросы, и т.д. передаваемые по различным сетям, обрабатываемые в автоматизированных системах и представляемые на средствах отображения в графическом или текстовом виде).

Техническая инфраструктура, ИКТ, программное обеспечение, с помощью которых осуществляется реализация основных действий с информацией: сбор, обработка, хранение и передача. К таким средствам относятся инфраструктура Интернет и сетевых взаимосвязей, компьютеры, всевозможные гаджеты и т.п.

Информационное взаимодействие субъектов с использованием информации получаемой (передаваемой) и обрабатываемой посредством технической инфраструктуры. Здесь имеются в виду все виды деятельности пользователей или участников киберпространства, которые они осуществляют с использованием информационных ресурсов, потоки и хранилища которых располагаются на технической инфраструктуре.

Все эти составляющие в совокупности и образуют сущность, которую можно именовать киберпространством. Можно выделить следующие его основные свойства.

Первое. Киберпространство определено на множестве цифровых устройств и систем на их основе, которые оперируют с информацией или во многом с ее помощью. Важно, что имеются в виду не отдельные системы, а их совокупность, когда подобных устройств (систем) достаточно много. То есть, в общем виде существенное уменьшение

числа функционирующих устройств (систем) в киберпространстве или нарушение их нормальной работы является угрозой киберпространству. Но речь идет не просто об отдельных устройствах (системах), а о большом числе таких объектов и способности оперировать ими информацией (обеспечивать сервисы) с заданным качеством, то есть осуществлять действия, которые обычно связываются с информационными технологиями. Отсюда вытекает второе свойство.

Активное оперирование информацией и сохранение этой информацией главных ее свойств: целостности, доступности, конфиденциальности и других, определяемых в современных стандартах. В отличие от информационной безопасности речь идет не об информации вообще, а о той информации, которая циркулирует в киберпространстве и составляет важную часть ее содержания. Таким образом, нарушение работы отдельного компьютера подключенного к киберпространству или утеря информации, которая в нем содержится, или нарушение ее свойств, безусловно важных для пользователя данного компьютера, вряд ли может рассматриваться как угроза кибербезопасности.

Третье. Наличие «добропорядочных» связей, связей, которые составляют основу киберпространства, и без которых рассматривать поле цифровых устройств (систем) в качестве некоторой новой сущности вряд ли имело бы смысл. Здесь имеется в виду способность киберпространства передавать, получать и обрабатывать информацию с сохранением ее существенных для целей применения свойств.

Четвертое. Собственно понятие кибер-. Оно относится к управлению. Управление в данном случае подразумевает не наличие прямолинейных команд, которые непосредственно исполняются всеми агентами (участниками) киберпространства, а формирование и передача таких сигналов, которые способны придать рассматриваемой области киберпространства некий «разумный» характер поведения и устойчивость к возникающим угрозам.

Способы управления оказывают непосредственное воздействие на структуру киберпространства. Здесь важно учитывать управление технической основой киберпространства и чисто физическими связями между отдельными узлами или даже областями киберпространства. Но определяющую роль играет управление участниками киберпространства: пользователями и их группами. Под управлением понимается комплекс усилий, направленный на повышение квалификации участников, стимулирование благоприятных для развития киберпространства действий и подавление или прямое запрещение злонамеренных действий. Управление субъектами киберпространства играет определяющую роль в возникновении, существовании и поддержке основных свойств этого образования.

Указанные свойства, а именно многочисленность элементов, составляющих киберпространство, обилие взаимосвязей между ними, возможность применения специальных техник управления действиями этих элементов, и определяют развитие тех угроз, о которых говорилось выше. Необыкновенно высокая и все нарастающая интенсивность атак происходит от громадных масштабов киберпространства, всевозможных и разнохарактерных связей между ними. Сложные атаки, имеющие комплексную структуру, опираются на возможность различных направлений распространения информации и сигналов. Использование методов социальной инженерии позволяет изыскивать наиболее продуктивные методы организации атак. В киберпространстве могут развиваться все более опасные и сложные угрозы. Они используют особенности его построения для достижения максимального эффекта.

Но те же самые особенности, проистекающие из многочисленных взаимосвязей между участниками киберпространства, могут стать важным фактором в повышении эффективности систем, которые обеспечивают защиту от подобных угроз [16]. Для этого необходимо координировать усилия всех заинтересованных участников, создавать механизмы, способствующие наилучшему распределению их усилий. Нужно правильно определять возникающие и прогнозируемые опасности и обоснованно выбирать рациональные меры защиты.

Кибербезопасность имеет целью решение этих вопросов и обеспечение нормального функционирования киберпространства, защищая его от возникающих угроз эффективным образом.

Важно правильно сформулировать понятие кибербезопасности, чтобы главные цели работы служб и средств защиты киберпространства от возникающих угроз были точно определены. Однако в концепции приведена формулировка, которая не может удовлетворить этим требованиям.

В проекте Концепции говорится следующее:

«кибербезопасность – совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями».

Кибербезопасность не может быть направлена на защиту от максимального числа угроз. Нужно

обеспечить максимально благоприятную среду для работы пользователей и всех систем в киберпространстве.

Указанная в Концепции постановка неявно призывает разрабатывать и выявлять все новые и новые угрозы, создавая новые средства и способы защиты от них.

Доля ресурсов, необходимых для обеспечения защиты, при таком подходе будет неуклонно расти, а устойчивая работа киберпространства может даже ухудшаться.

Поэтому в определении кибербезопасности основной упор и целевая установка должны быть сделаны на сохранение благоприятного состояния киберпространства, а не на число угроз. Если мы смогли защититься от невообразимо большого числа угроз, но работоспособность киберпространства нарушена, то это хуже, чем защититься от двух десятков угроз и при этом сохранить приемлемый уровень работоспособности.

Кибербезопасность так же, как и киберпространство может описываться триадой составляющих ее сущностей определенных на составных частях киберпространства: информационных ресурсах, компьютерной и сетевой архитектурах (инфраструктуре) и способах взаимодействия пользователей.

Кибербезопасность охватывает уже не только информацию как объект защиты, не исключительно технические средства, которые определяют возможности функционирования информации, а защиту способов функционирования новой сущности – киберпространства. Защищается деятельность людей, которая осуществляется с помощью информации, распространяемой посредством технической инфраструктуры ИКТ.

При обеспечении кибербезопасности важно учитывать указанные особенности киберпространства и ее наиболее важный аспект – наличие взаимосвязей между участниками (пользователями), что приводит к возможности возникновения синергетического эффекта.

В проекте Концепции указывается на необходимость проведения научных исследований в области кибербезопасности, в частности, на реализацию научно-технических программ и исследований в соответствии с «Приоритетными направлениями научных исследований в области обеспечения информационной безопасности Российской Федерации», утвержденными Советом Безопасности Российской Федерации. Но это лишь общая постановка, отсылающая к списку из более 100 направлений, среди которых необходимо выделить наиболее значимые с точки зрения кибербезопасности. На этих направлениях стоит сосредоточить основные усилия. Предложения по таким работам приведены в статье [17]. Кроме того, следует дополнить тематику перспективных исследований направлениями, которые вытекают из основных свойств киберпространства.

Необходимо подробно и тщательно исследовать основные свойства киберпространства, динамику его развития в различных масштабах времени от мгновенных до многолетних, методы управления этой динамикой. Важно обосновать подходы к определению показателей кибербезопасности, разработать модели для их оценки, выработать способы обоснования критериев.

Без проведения системного анализа и получения оценок применения тех или иных мер невозможно построить эффективную систему кибербезопасности.

Представляется целесообразным в комплекс исследований в области кибербезопасности включить следующие направления:

1. Выработка единой терминологии киберпространства и кибербезопасности, гармонизированной с существующей терминологией в области информационной безопасности.

2. Разработка комплексной системы показателей, охватывающих все стороны функционирования киберпространства и обеспечения его защиты от возможных угроз.

3. Разработка моделей самого киберпространства и основных факторов, оказывающих влияние на его функционирование. Безусловно, необходима тщательно продуманная модель угроз. Одним из важнейших направлений является создание математических моделей, позволяющих получать численные характеристики информационной безопасности (степени угроз информационной безопасности, анализа информационных рисков, оценки эффективности мер защиты).

4. Создание специальных методов обеспечения устойчивости киберпространства или его областей при воздействии угроз. Здесь несколько возможным тем:

- анализ топологической структуры и выработка рекомендаций по ее изменению, способов и конкретных алгоритмов их реализации;

- новые методы криптографической защиты, основанные не только на чисто вычислительных механизмах реализации стойкости, но и на использовании преимуществ многосвязной архитектуры связей и большого числа добропорядочных пользователей;

- методы информационной безопасности на основе социальных сервисов для противодействия кибер-атакам с применением специальных процедур анализа группового поведения.

5. Интеллектуальные методы обеспечения кибербезопасности:

- методы интеллектуальной идентификации пользователей;

- интеллектуальные методы предотвращения вирусных и других атак;

- интеллектуальные методы выявления атак и проникновений;

- методы ситуационного анализа состояния информационной безопасности;

- новые методы криптографической защиты, основанные на нейросетевых технологиях.

Литература

1. http://www.securelist.com/ru/analysis/208050763/Razvitie_informatsionnykh_ugroz_vo_vtorom_kvartale_2012_goda.
2. Trustwave 2013-Global-Security-Report
3. http://www.symantec.com/security_response/publications/threatreport.jsp
4. 2012 Norton Cybercrime Report (http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf)
5. http://mvd.ru/news/item/1033853
6. http://www.sophos.com/en-us/security-news-trends/reports/security-threat-report/cyber-attacks.aspx
7. http://www.cybersecurity.ru/crypto/171331.html
8. http://www.politico.com/story/2013/02/washington-cybersecurity-china-attacks-87087.html
9. http://www.nytimes.com/2013/01/28/us/pentagon-to-beef-up-cybersecurity-force-to-counter-attacks.html
10. http://habrahabr.ru/company/kaspersky/blog/169839/
11. http://www.itsec.ru/newstext.php?news_id=91005
12. http://www.cybersecurity.ru/telecommunication/165487.html
13. Старовойтов А. В. Кибербезопасность как актуальная проблема современности // Информатизация и связь. – 2011. – №. 6. – С. 4-7.
14. Безкоровайный М. М., Лосев С. А., Татузов А. Л. Кибербезопасность в современном мире: термины и содержание // Информатизация и связь. – 2011. – №. 6. – С. 27-32.
15. http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf
16. Безкоровайный М. М., Татузов А. Л. Подходы к математическому моделированию в области кибербезопасности // Информатизация и связь. – 2012. – №. 8. – С. 21-27.
17. Безкоровайный М. М., Татузов А. Л. Информационная безопасность в сфере образования и науки // Информатизация и связь. – 2011. – №. 6. – С. 34-39.

References

1. http://www.securelist.com/ru/analysis/208050763/Razvitie_informatsionnykh_ugroz_vo_vtorom_kvartale_2012_goda.
2. Trustwave 2013-Global-Security-Report
3. http://www.symantec.com/security_response/publications/threatreport.jsp
4. 2012 Norton Cybercrime Report (http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf)
5. http://mvd.ru/news/item/1033853
6. http://www.sophos.com/en-us/security-news-trends/reports/security-threat-report/cyber-attacks.aspx
7. http://www.cybersecurity.ru/crypto/171331.html
8. http://www.politico.com/story/2013/02/washington-cybersecurity-china-attacks-87087.html
9. http://www.nytimes.com/2013/01/28/us/pentagon-to-beef-up-cybersecurity-force-to-counter-attacks.html
10. http://habrahabr.ru/company/kaspersky/blog/169839/
11. http://www.itsec.ru/newstext.php?news_id=91005
12. http://www.cybersecurity.ru/telecommunication/165487.html
13. Starovojtov A. V. Kiberbezopasnost' kak aktual'naja problema sovremennosti (Cybersecurity as an actual modern problem) // Informatizacija i svjaz' (Informatization and communication). – 2011. – №. 6. – P. 4-7.
14. Bezkorovajnyj M. M., Losev S.A., TatuzovA.L. Kiberbezopasnost' v sovremennom mire: terminy i soderzhanie (Cybersecurity in the modern world : terms and content) // Informatizacija i svjaz' (Informatization and communication) – 2011. – №. 6. – P. 27-32.
15. http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf
16. Bezkorovajnyj M. M., TatuzovA.L. Podhody k matematicheskomu modelirovaniju v oblasti kiberbezopasnosti (Approaches to mathematical modelling in sphere of cybersecurity) // Informatizacija i svjaz' (Informatization and communication). – 2011. – №. 6. – P. 21-27.
17. Bezkorovajnyj M. M., TatuzovA.L. Informacionnaja bezopasnost' v sfere obrazovanija i nauki (Information security in the sphere of education and science) // Informatizacija i svjaz' (Informatization and communication). – 2011. – №. 6. – P. 34-39.