ТЕРМИНОЛОГИЯ БЕЗОПАСНОСТИ: КИБЕРБЕЗОПАСНОСТЬ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ.

***Алпеев Анатолий Степанович**, кандидат технических наук, г. Москва*

В статье рассмотрены понятия «кибербезопасность» и «информационная безопасность», определения которых взяты из различных источников. Показана их родовая связь с понятием «безопасность» и предложены более корректные, с точки зрения автора, определения этих терминов. Показана не состоятельность на данное время термина «информационная безопасность» и предложено использование вместо него термина «информационная защищенность», что практически соответствует действительности.

***Ключевые слова**: кибербезопасность, кибератака, защищенность, понятие, термин, определение, свойство, информация, безопасность.*

TERMINOLOGY OF ISECURITY: CYBERSECURITY, INFORMATION SECURITY

***Anatoly Alpeev** Ph.D*

The article discusses the concept of «cyber safety» and «information safety», from various sources indicated. Shows their ancestral links with the concept of «Safety» and offered more correct from the point of view of the author, the definition of these terms. Shows no consistency at this time the term «information safety» and suggested instead use the term «information security», which is almost true.

***Keywords**: cyber safety, cyber attacks, security, concept, terms, definitions, property, information safety.*

Понятие «безопасность» в современном мире играет едва ли не самую главную роль во всех жизненных процессах: биологических, политических, экономических, социальных, технических, территориальных и др. Поэтому очень важно не только корректно определять это понятие и его производные, но и правильно применять их по назначению. К сожалению, к настоящему времени этот весьма желаемый результат не получен. Однако попытки его достижения продолжаются.

В этой статье рассматриваются сравнительно недавно появившиеся термины «Кибербезопасность» и «Информационная безопасность», определение которых, и их производных, на мой взгляд, выполнены не совсем корректно. Поскольку важность этих понятий в современном мире очень велика, то их анализ и предложения по корректировке заслуживают пристального внимания.

В качестве критикуемых определений термина «кибербезопасность» в этой статье взято определение этого термина из ISO/IEK 27032 2012 [1]:

«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».

И определение этого же термина в «Концепции стратегии кибербезопасности Российской Федерации» [2]:

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

При рассмотрении этих определений в первую очередь хочется отметить неправомерный выбор в них родового термина: «условия» из [1] и «совокупность условий» из [2] , поскольку сам термин указывает на необходимый родовой тер-

мин: «безопасность». Это говорит о том, что термин «кибербезопасность» является производным от родового термина «безопасность», таким образом, что «кибербезопасность» представляет собою часть понятия «безопасность», выделяемую некоторыми специфическими особенностями, которые должны составить вторую часть определения термина «кибербезопасность» следующую за родовым словом. Поскольку родовое слово в выбранных определениях термина «кибербезопасность» выбрано не правомерно, то обсуждать вторую часть этих определений не целесообразно. Дальнейшие соображения по поводу определения термина «кибербезопасность», связаны с выбором определения термина «безопасность», который бы позволил корректно сформировать вторую часть определения термина «кибербезопасность», следующую за родовым словом.

В этой статье для этой цели выбрано определение «безопасность» из [3] :

«Безопасность - наука, изучающая природные, техногенные, социальные, экономические и другие процессы образования, развития и взаимодействия субъектов, объектов, окружающей среды и их комбинаций с целью выявления источников опасностей, определения их характеристик и формирования законов и других нормативных актов, устанавливающих понятия, требования, рекомендации и методики, выполнение которых должно гарантировать защищенность интересов отдельной личности и общества в целом от всех выявленных и изученных источников опасности».

В [3] проведен анализ причин, по которым выбрано это определение и предложены методы формирования других понятий, связанных родовыми отношениями с термином «безопасность». Пользуясь этим методом формирования определений, предлагается следующая формулировка термина «кибербезопасность»:

Кибербезопасность – раздел безопасности, изучающий процессы формирования, функционирования и эволюции киберобъектов, с целью выявления источников киберопасности, которые могут нанести им ущерб, и формирования законов и других нормативных актов, регламентирующих термины, требования, правила, рекомендации и методики, выполнение которых должно гарантировать защищенность киберобъектов от всех известных и изученных источников киберопасности.

Под киберобъектом здесь понимается, любой объект, функционирование которого осуществляется с участием программируемых средств.

Заметим далее, что определение термина «кибербезопасность» из [1, 2] базируется на понятии «киберпространство»:

«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)» из [2].

В определении термина «киберпространство» также родовой термин «сфера» выбран не логично. Этот термин был бы уместен, если бы определялся термин «киберсфера». На мой взгляд, более корректно определить понятие «киберпространство» через понятие «киберобъект» следующим образом:

Киберпространство – пространство, в котором осуществляется функционирование и взаимодействие киберобъектов.

В соответствии с рекомендациями [3], далее следует определить термин «кибербезопасность объекта» как внутреннее свойство объекта не быть опасным для окружающей среды при его функционировании во всех режимах работы:

Кибербезопасность объекта – свойство объекта, характеризующее его внутренние возможности не быть причиной образования ущерба для внешней среды или ограничивать его величину допустимыми нормами.

При этом следует понимать, что ущерб киберобъекту наносится в результате специально организованных кибератак. Под кибератакой в этой статье понимается – предумышленно организованная совокупность действий с участием программно технических средств (ПТС), направленная на нанесение экономического, технического или информационного ущерба. Например, получение секретных сведений по различным аспектам.

По источнику организации кибератаки можно подразделять на две группы: внешние, по отношению к объекту кибератаки и внутренние. Так, например, в [4] описан случай организации внутренней кибератаки с корыстной целью заработать деньги.

«Первым хакером в истории СССР оказался простой программист Мурат Уртембаев, которому прочили блестящую карьеру математика в МГУ, но он отказался от научной стези, и по целевому распределению попал на АВТОВАЗ. Там его таланты никто не оценил, и он решил доказать, что

чего-то да стоит. Схема работы была следующей - программист, если считал нужным, вносил изменения в ПО, но не оставлял никаких данных или отметок о внесенных изменениях. Мурат смекнул, что можно без труда внести сбой в систему, и никто его не обнаружит. В результате конвейер ВАЗа остановился на три дня. В ходе проверки выяснилось, что первый хакер СССР был первым пойманным, но отнюдь не первым, кто обнаружил дыру в системе. В том же Управлении, в котором работал Уртембаев, «элита» регулярно создавала сбои на конвейере и оперативно их ликвидировала, выбивая у начальства за спасение конвейера в качестве награды дачи, квартиры, автомобили».

Таким образом, источником внутренней кибератаки может быть персонал объекта кибератаки или персонал имеющий доступ к его программному обеспечению, если за действиями этого персонала нет должного контроля.

Случаи внешних кибератак описываются довольно часто, особенно на сети банков и финансовых организаций с целью присвоения денег с чужих счетов и карт частных пользователей. Однако уже имеются случаи кибератак на АЭС, например, в [5] «глава Организации пассивной обороны Ирана Голям Реза Джалали заявил, что иранские специалисты завершили расследование обстоятельств кибератаки. Согласно его результатам, вирус Stuxnet, атаковавший Бушерскую АЭС, запустили из Израиля и американского штата Техас. Также Джалали высказал предположение, что инжиниринговая корпорация Siemens, которая поставила и установила на АЭС систему сбора и обработки данных SCADA, также причастна к атаке. Концерн, по мнению составителей доклада, должен объяснить, почему он предоставил «врагам» Ирана коды SCADA, в результате чего и стала возможной кибератака. В конце сентября иранским программистам удалось справиться с компьютерным вирусом, который, по утверждениям главы Организации по атомной энергии Ирана Али Акбара, находился в нескольких ПК, принадлежащих сотрудникам АЭС».

В [5] указывается также, что «Сейчас группа специалистов (или даже одиночка) способны с помощью технических и информационных средств нанести непоправимый вред военной, экономической, технологической, политической и информационной безопасности любого государства. Поэтому большинство действий, осуществляемых сторонами в кибервойне, влияет на межгосударственные отношения и может привести к политическому противостоянию».

В качестве критикуемых понятий «Информационная безопасность» в статье взяты следующие понятия:

«Информационная безопасность — защита конфиденциальности, целостности и доступности информации» из [6].

«Информационная безопасность – состояние защищенности личности, организации и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве» из [2].

Сложность этого понятия состоит в том, что сам предмет, безопасность которого определяется, не определен как по внутренней структуре, так и по внутренним свойствам, которые необходимы для формирования требований к его безопасности. Даже само определение информации, в настоящее время весьма не однозначно и противоречиво. Таким образом сформировать понятие безопасности такого предмета на основании его внутренней структуры и внутренних свойств не представляется возможным.

Тем более что к определению из [2] даны определения указанных в нем составляющих:

Конфиденциальность информации - такое состояние информации, при котором доступ к ней только у объектов с наличием прав на нее.

Целостность информации - блокировка несанкционированных изменений информации.

Доступность информации - избежание сокрытия информации от пользователей с правами доступа.

Обращает внимание то, что все составляющие представляют собой только внешние действия по отношению к информации: назначение прав доступа к информации; блокирование несанкционированных изменений информации; избежание сокрытия информации от пользователей с правами доступа.

К тому же, хочется отметить то, что оба взятых для критики понятия фактически устанавливают эквивалентность терминов «безопасность» и «защищенность», что соответствует [7]. Сравните сами: в [1] «безопасность – защита» и в [6] «безопасность – состояние защищенности». С моей точки зрения, это совсем не так. Такая ситуация в терминологии именуется порочным кругом: «безопасность это защищенность», а «защищенность это безопасность». Но, как правило, защищенность объекта это его защита от внешних источников опасности, в то время как безопасность объекта это внутреннее свойство объекта не быть источником опасности для окружающей среды. С этой точки зрения следует различать два терми-

на: «Кибербезопасность объекта» и «Киберзащищенность объекта», что соответствует в английской интерпретации «Cyber safety object» и «Cyber security object». Первый термин определен выше, второй термин, на мой взгляд, должен быть определен следующим образом:

Киберзащищенность объекта – свойство объекта, характеризующее его внешние возможности предотвращать образование ущерба от кибератак или ограничивать его величину допустимыми нормами.

Что касается термина «информационная безопасность», то имеет смысл пока рассуждать об информации как о черном ящике, т.е. только о защищенности информации. Поэтому термин «безопасность информации», на данный момент времени определяется только намерениями ее обладателя и ни чем другим.

Это дает основания утверждать, что термин «информационная безопасность» на данный момент времени (пока не определено корректно, что такое информация и какова ее внутренняя структура и свойства) не корректен по своей сути. Вместо него можно предложить термин «информационная защищенность» и использовать для него определение изложенное ранее т. е.:

«Информационная защищенность — защита конфиденциальности, целостности и доступности информации», что, на мой взгляд, соответствует реальному состоянию рассматриваемой проблемы.

В заключении автор выражает надежду на то, что приведенная в статье аргументация поможет некоторым образом продвинуть понимание терминологии безопасности на качественно новый уровень.

Литература:

1. ISO/IEK 27032 2012. «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности».
2. Концепция стратегии кибербезопасности Российской Федерации http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf
3. Ежемесячное приложение к журналу «Стандарты и качество». Экологические аспекты проблем надежности и безопасность технических систем. «Основные понятия безопасности». Алпеев А.С. М., 1994, вып. 7.
4. Первый хакер в СССР. Остановил конвейер ВАЗа и остался на свободе/ http://yandex.ru/yandsearch?lr=213&text=%D0%BF%D0%B5%D1%80%D0%B2%D1%8B%D0%B9+%D1%85%D0%B0%D0%BA%D0%B5%D1%80+%D1%81%D1%81%D1%81%D1%80&csg=5649%2C41594%2C12%2C25%2C3%2C0%2C0.
5. Армейский вестник от 04.09.2012г. «Мировые кибервойны». http://lastbabylon.com/node/387.
6. Википедия. https://ru.wikipedia.org/wiki Информационная безопасность

References:

1. ISO/IEK 27032 2012. «Informatcionny`e tekhnologii. Metody` obespecheniia bezopasnosti. Rukovodiashchie ukazaniia po obespecheniiu kiberbezopasnosti».
2. Kontceptciia strategii kiberbezopasnosti Rossii`skoi` Federatcii http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf
3. Ezhemesiachnoe prilozhenie k zhurnalu «Standarty` i kachestvo». E`kologicheskie aspekty` problem nadezhnosti i bezopasnost` tekhnicheskikh sistem. «Osnovny`e poniatiia bezopasnosti». Alpeev A.S. M., 1994, vy`p. 7.
4. Pervy`i` haker v SSSR. Ostanovil konvei`er VAZa i ostalsia na svobode / http://yandex.ru/yandsearch?lr=213&text=%D0%BF%D0%B5%D1%80%D0%B2%D1%8B%D0%B9+%D1%85%D0%B0%D0%BA%D0%B5%D1%80+%D1%81%D1%81%D1%81%D1%80&csg=5649%2C41594%2C12%2C25%2C3%2C0%2C0.
5. Armei`skii` vestneyk ot 04.09.2012g. «Mirovy`e kibervoi`ny`». http://lastbabylon.com/node/387.
6. Vikipediia. https://ru.wikipedia.org/wiki Informatcionnaia bezopasnost`