УДК 004.056.5

УПОРЯДОЧЕНИЕ ТЕРМИНОЛОГИИ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ СИСТЕМЫ УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИЯМИ

МИХОВА А.И.

Одесская национальная академия связи им. А.С. Попова

REGULARIZATION OF TERMINOLOGY IN THE FIELD OF CYBERSECURITY TELECOMMUNICATIONS MANAGEMENT SYSTEM

MIKHOVA A.I.

Odessa national academy of telecommunications n.a. O.S. Popov

Аннотация. *Прослежено развитие терминологии. Рассмотрена взаимосвязь параметров международных и отечественных стандартов. Определено соотношение понятий связанных с кибербезопасностью системы управления телекоммуникациями.*

Abstract. *The development of terminology is studied. The interrelation of the parameters of international and native standards. The correlation of the concepts associated with cybersecurity management system telecommunications is defined.*

Данная работа касается сферы информационной безопасности, где, как и в других областях науки, существует проблема определения терминов и понятий.

В сфере информационной безопасности (ИБ) терминология устанавливается стандартами [1], нормативными документами [2], справочниками [3], научными справочниками [4], а также международными рекомендациями, например X.800 [5] и другие. Сложившийся подход к ИБ различает службы, услуги, механизмы.

Основой классической парадигмы защиты информации (ЗИ) является контроль доступа, конфиденциальность, целостность и доступность, а так же наблюдаемость информации [2, с. 4,5].

В отечественной нормативной базе [1…4] в сфере ТЗИ по защите от несанкционированного доступа в компьютерных системах предприятий и организаций, местных и центральных органах власти, и субъектов предпринимательской деятельности проведена гармонизация нормативно-правовых документов.

Однако в имеющихся научных и технических материалах наблюдается разнобой в определениях, даже в основополагающих терминах, таких как: “услуги безопасности” и “механизмы”. В ходе исследований литературы [6…7] появилась необходимость упорядочить терминологию как в новых, так и в первичных документах. Для исследователей и разработчиков актуально иметь чёткое представление о существе и точном определении всех понятий.

Одними из средств обеспечения комплексной технической ЗИ (ТЗИ) является информационное и правовое обеспечение, которые предотвращают реализацию угроз и атак.

Целью данной работы является упорядочение терминологии относительно кибербезопасности системы управления телекоммуникациями.

При сравнении международных и отечественных нормативных документов обнаруживается, что они не раскрывают всю полноту понятий и не определяются с достаточной четкостью. В стандартах Международного союза электросвязи более ранние издания имеют менее содержательные определения, а более поздние вкладывают больший смысл, соответственно появляется необходимость соотнести и упорядочить определения.

Анализируя международные и отечественные стандарты, находим, что украинский нормативный документ [2] является примерным аналогом рекомендации [6]. В украинской нормативной базе относительно ЗИ нет точного аналога в рекомендациях [5…7], а некоторые понятия вовсе не определены.

В рекомендации [6] русскоязычной версии дано такое определение: «Измерения защиты (security dimension) – это комплекс мер защиты, предназначенных для реализации конкретного аспекта

сетевой защиты; кроме того, применяются к поставщикам услуг и к организациям, предлагающим услуги по обеспечению безопасности своим клиентам [6]. Из-за не точного перевода понятие, связанное с услугами защиты, перевели общим словом «dimension».

В отечественном документе [2] так же присутствует понятие “услуга безопасности”: “4.3.8 Услуга безопасности (security service) – это совокупность функций, обеспечивающие защиту от определенной угрозы или от множества угроз” (табл. 2). По сути, как слово dimensions, так и services имеют те же смысловые наполнения, они являются синонимами. Однако, понятие “dimension” довольно многозначное и среди различных переводов имеется значение его как “член ряда” [3] (Табл. 1).

Таблица 1 – Соотношение значения “dimension” различных источников

Словарь [3]	Рек. X.805 [6]	Рек. X 1205 [7]	Рек. X.1031 [10]
Член ряда	Аспект архитектуры; измерения защиты	Фактор безопасности; совокупность мер безопасности	Набор мер безопасности, предназначенных для решения конкретного аспекта безопасности сети

По сути, изначально сложились меры безопасности (dimensions), которые в ходе развития перешли в услуги (services). В нормативном документе [2] раскрывается понятие “механизмов защиты”: “4.3.9 Механизмы защиты (security mechanism) – конкретные процедуры и алгоритмы, которые используются для реализации определённых функций и услуг безопасности”. Так же в [5] определено, что механизмы могут использоваться для реализации комбинации услуг базовой безопасности, в соответствии с определенным уровнем модели “взаимодействия открытых систем”.

Исходя из этого, можно сделать вывод, что услуги (services) базируются на механизмах (mechanisms), а это как программные, так и аппаратные модули, предназначенные для реализации услуг. В ходе анализа [2], [5], [6] следует, что более ранние и отечественные издания менее содержательны (табл. 2).

Таблица 2 – Соотношение определений согласно рекомендациям

Определения, представленные в [2]	Определения, представленные в [5]	Определения, представленные в [6]
1	2	3
Контроль доступа (access control)		
Совокупность мер по определению полномочий и прав доступа, контроля о следовании правилам разграничения доступа	Предотвращение несанкционированного использования ресурсов, включая предотвращение использования ресурса несанкционированным образом	Защищает от несанкционированного использования сетевых ресурсов. Контроль доступа гарантирует, что только авторизованному персоналу или устройствам разрешен доступ к элементам сети, хранимой информации, информационным потокам, службам (услугам – services) и приложениям
Аутентификация (authentication)		
Процедура проверки соответствия предъявленного идентификатора или компьютерной системы (КС) на предмет принадлежности его этому объекту; установление или подтверждение аутентичности	Видеть проверку подлинности источника данных и равноправного органа проверки подлинности	Предназначено для удостоверения личностей поддерживающих связь объектов. Аутентификация гарантирует подлинность заявляемой личности объектов, участвующих в связи (например, человека, устройства, услуги или приложения), и обеспечивает уверенность в том, что объект не пытается осуществлять подмену или неправомочно использовать предыдущий сеанс связи

Продолжение таблицы 2

1	2	3
Целостность данных (data integrity)		
Свойство данных (информации), которое заключается в том, что данные не могут быть модифицированы неавторизированным пользователем и/или процессом	Это свойство, при котором данные не были изменены или уничтожены несанкционированным образом	Гарантирует правильность и точность данных; данные защищены от несанкционированного изменения, удаления, создания и дублирования, а также обеспечивается обнаружение такой несанкционированной деятельности
Безотказность (non-repudiation)		
–	Эта служба может занять одну или обе из двух форм	Обеспечивает средства для предотвращения отказа выполнения определенного действия, связанные с данными, обеспечивая наличие доказательств совершения различных действий, связанных с сетью или организацией (такие, как подтверждение обязательства, намерения или готовности; использование доказательства происхождения данных, доказательство права собственности, доказательство использования ресурсов). Гарантируется наличие данных, которые могут быть представлены третьим лицам и использованы как доказательства, что некоторое событие или действие имело место
Конфиденциальность (data confidentiality)		
Свойство данных (информации), которое заключается в том, что данные не могут быть получены неавторизированным пользователем и/или процессом	Предусмотрена для защиты данных от несанкционированного разглашения (раскрытия)	Защищает данные от несанкционированного раскрытия. Конфиденциальность данных гарантирует, что содержание данных не может быть понято неуполномоченными лицами. Шифрование, списки контроля доступа и разрешение доступа к файлам являются методами, часто используемые для обеспечения конфиденциальности данных
Приватность (privacy)		
–	Право контроля или влияния отдельных лиц, какая информация, связанная с ними, может быть собрана и хранится, и кем и кому эта информация может быть раскрыта	Предусмотрена для ЗИ, которая могла бы быть получена от наблюдения сетевой деятельности. Примеры такой информации – Web-сайты, которые пользователь посетил, географическое расположение пользователя, IP-адреса и DNS-имена в сети поставщика услуг
Доступность (availability)		
Свойство ресурса системы (компьютерной системы (КС), услуги, объекта КС, информации), которое заключается в том, что пользователь и/или процесс, который владеет соответствующими полномочиями, может использовать ресурс в соответствии с правилами, установленными политикой безопасности, не ожидая больше заданного (малого) промежутка времени, т.е., когда он находится в виде, необходимому пользователю, в месте, необходимому пользователю, и в то время, когда он ему необходим	Свойство данных быть доступными и полезными по требованию уполномоченного лица	Гарантирует отсутствие какого-либо ограничения на санкционированный доступ к элементам сети, хранимой информации, потокам данных, к услугам и приложениям из-за событий, влияющих на сеть; в эту категорию включены варианты аварийного восстановления

Окончание таблицы 2

1	2	3
Авторизация (authorization)		
Предоставление полномочий; установление соответствия между сообщением (пассивным объектом) и его источником (созданным его пользователем или процессом)	Предоставление прав, которые включает в себя предоставление доступа на основе прав доступа	–
Идентификация (identification)		
Процедура присвоения идентификатора объекту КС или установление соответствия между объектом и его идентификатором; опознавание	–	–

Исходя из вышеизложенного предлагается в дальнейшем термин “dimensions” заменить как “services” понимая под ним “услуги”. Табл. 3 показывает разницу между механизмами защиты системы ЗИ в ТКС и в TMN.

Таблица 3 – Сравнение терминологии механизмов в стандартах

Терминология	Стандарты	
	X. 800 ЗИ ТКС	M.3016.3 04/2005 ЗИ TMN
	Specific security mechanisms	Security mechanisms
Контроль доступа	Access control	Access control
Аутентификация	Authentication exchange mechanism (проверка подлинности обмена)	User authentication, (аутентификация пользователя) Peer entity and data origin authentication (аутентификация равноправного объекта и источника данных)
Целостность данных	Data integrity	data integrity
Конфиденциальность	–	Data confidentiality
Аварийная сигнализация	–	Alarm reporting
Проверка(фильтрация) пакетов	–	Packet filtering
Контрольный журнал	–	Audit trail
Обмен ключами	–	Key exchange
Механизмы цифровой подписи	Digital signature mechanisms: signing a data unit, verifying a signed data unit	–
Шифрование	Encipherment	–
Заполнение трафика	Traffic padding	–
Механизм маршрутизации управления	Routing control mechanism	–
Механизм нотариального засвидетельствования	Notarization mechanism	–
Повсеместная безопасность	Pervasive security mechanisms	–

Некоторая разнесённость в понятиях двух стандартов объясняется тем, что X.800 относится к системе защиты телекоммуникаций, а M.3016.3 – к системе защите TMN. И механизмы, в отличие от услуг, иногда несут иное наполнение в тех же понятиях. Так как первые, входят в состав вторых.

Учитывая, что развитие нормативно-правовой базы проходит поэтапно и с каждым новым этапом происходит наращивание понятий как в содержательной форме, прослеживается тенденция укрупнения предмета исследования. На каждом этапе производится ввод в эксплуатацию новых средств защиты и их усовершенствование за счет расширение функций.

Вначале мы имели четкую иерархию: служба защиты, услуги защиты, механизмы защиты, приложения защиты. В ходе эволюции наблюдаются укрупнения базовых элементов защиты. При этом часть терминов переносится на новый базис, и термин наполняется новым содержанием. Например, “контроль доступа” был механизмом, а затем стал услугой, а в последних рекомендациях он трактуется как технология кибербезопасности. Также иерархия служба-услуги-механизмы-приложения переходит в служба-методы-категории-технологии.

Другая часть терминов вводится как новые. Например, аудит и мониторинг [7]; определение идентичности [11], [12] (табл. 4). Табл. 4 заимствована из рекомендации МСЭ-Т X.1205 [7].

Таблица 4 – Технологии кибербезопасности

Методы	Категории	Технологии	Цель
1	2	3	4
Криптография	Сертификат и архитектура открытого ключа	Цифровые подписи	Используется для того, чтобы разблокировать выпуск и сохранение сертификатов, которые будут использоваться в цифровом виде
		Шифрование	Используется для шифрования данных во время передачи и хранения данных
		Обмен ключами	Устанавливает или сеансовый ключ, или ключ управления информационным обменом, чтобы им пользоваться для безопасной связи
	Гарантия	Шифрование	Страхует аутентичность данных
Контроль доступа	Защита периметра	Брандмауэр	Контроль доступа в сеть и из сети
		Управление содержанием	Ведет текущее наблюдение за потоком несовместимой информации
	Аутентификация	Однофакторная	Система, использующая комбинации идентификатора/пароля пользователя для проверки идентификатора
		Двухфакторная	Система, которой требуется два компонента для того, чтобы предоставить доступ пользователя к системе, такие как владение физическим маркером плюс знание секрета
		Трехфакторная	Добавляет еще один фактор идентификации, такой как биометрический или измеренную характеристику человеческого тела
		Смарт-маркеры	Устанавливает заслуживающие доверия идентификаторы с помощью особой схемы в устройстве, например смарт-карте

Окончание таблицы 4

1	2	3	4
Контроль доступа	Авторизация	На ролевой основе	Механизмы санкционирования, которые управляют доступом пользователя к соответствующим ресурсам системы, основанные на присвоенной роли
		На основе правил	Механизмы санкционирования, которые управляют доступом пользователя к соответствующим ресурсам системы, основанные на особых правилах, связанных с каждым пользователем, независимо от его роли внутри организации
Целостность системы	Антивирус	Методы подписи	Защищает от злонамеренного компьютерного кода, такого как вирусы, черви и Троянские кони, используя их кодовые подписи
		Методы поведения	Проверяет текущие программы на несанкционированное поведение
	Целостность	Обнаружение вторжения	Может использоваться для предостережения системных администраторов о возможности происшествий, связанных с безопасностью, таких как дискредитация файлов на сервере
Аудит и мониторинг	Обнаружение	Обнаружение вторжения	Сравнивает поток сети и элементы регистрации в узле для подбора данных о подписях, которые являются указаниями на хакеров
	Предотвращение	Предотвращение вторжения	Обнаружение атак на сеть и проведение мероприятий, как определено организацией, для смягчения этих атак. Подозрительные действия запускают сигналы тревоги администратора и другие реконфигурируемые отклики
	Регистрация	Инструменты регистрации	Ведет текущее наблюдение и сравнивает поток в сети и элементы регистрации в узле для подбора данных о подписях и профилях адресов в узле, которые являются указаниями на хакеров
Управление	Управление сетью	Управление конфигурацией	Учитывает контроль и конфигурацию сетей и аварийный функциональный набор.
		Управление внесением неисправностей	Устанавливает самые последние обновления, подстраивает к устройствам сети.
	Политика	Принуждение	Дает возможность администраторам вести мониторинг и принудительно проводить политики безопасности

ВЫВОДЫ

Прослежены эволюционные этапы развития терминологии; выявлено, что быстрое развитие системы кибербезопасности информационных технологий и смены парадигм приводит к укрупнению и усложнению терминологии, а также к введению новых терминов. Предложена замена терминов таких как: “dimensions” и “services” интерпретировать общим понятием “услуги” и “методы”.

ЛИТЕРАТУРА

1. Захист інформації. Технічний захист інформації. Терміни та визначення : ДСТУ 3396.2-97. – [Чинний від 01.01.1998-12-19]. – К.: Держстандарт України, 1998. – 15 с.
2. НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу [Електронний ресурс] / Затверджено наказом № 22 ДСТСЗІ СБУ від 28.04.1999. – 30 с. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40393&cat_id=38835
3. Бабак В.П. Інформаційна безпека та сучасні мережеві технології: Англо-українсько-російський словник термінів / В.П. Бабак, О.Г. Корченко. – К.: НАУ, 2003. – 670 с.
4. Богуш В.М. Інформаційна безпека: термінологічний навчальний довідник / Богуш В.М., Кривуца В.Г., Кудін А.М.; [за ред. В.Г.Кривуци]. – К.: ТОВ “Д.В.К”, 2004. – 508 с.
5. Рекомендация МСЭ-Т X.800 Архитектура безопасности для взаимной связи открытых систем для CCITT приложений.
6. Рекомендация МСЭ-Т X.805 (10/2003) Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами.
7. Рекомендация МСЭ-Т X.1205 Обзор кибербезопасности. Режим доступа: http://www.itu.int/itu-t/ recommendations /index.aspx?ser=X
8. Рекомендация МСЭ-Т M.3016.2 Безопасность для плоскости управления: услуги по обеспечению безопасности.
9. Рекомендация МСЭ-Т M.3016.3 Безопасность для плоскости административного управления: Механизм безопасности.
10. Рекомендация МСЭ-Т X.1031 Роли конечных пользователей и телекоммуникационных сетей в пределах архитектуры безопасности.
11. Рекомендация МСЭ-Т X.1250 Базовые возможности для улучшенного доверия и функциональной совместимости при глобальном управлении определением идентичности.
12. Рекомендация МСЭ-Т X.1251 Структура осуществляемого пользователем управления в отношении цифровой идентичности.