УДК 004.056.53

Михова А.И
Міхова А.І.
Mikhova A.I.

РАЗРАБОТКА АРХИТЕКТУРЫ КИБЕРБЕЗОПАСНОСТИ СИСТЕМЫ УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМОЙ

РОЗРОБКА АРХІТЕКТУРИ КІБЕРБЕЗПЕКИ СИСТЕМИ УПРАВЛІННЯ ТЕЛЕКОМУНІКАЦІЙНОЮ СИСТЕМОЮ

DEVELOPMENT OF CYBERSECURITY ARCHITECTURE MANAGEMENT TELECOMMUNICATION SYSTEM

Аннотация. Рассмотрена структура сети TMN с управляемой сетью телекоммуникаций, архитектура кибербезопасности ТКС. Также соотношение услуг и угроз безопасности. Разработана архитектура кибербезопасности TMN.

Анотація. Розглянута структура мережі TMN з керуючою мережею телекомунікацій, архітектура кібербезпеки ТКС. Також співвідношення послуг та загроз безпеки. Розроблена архітектура кібербезпеки TMN.

Summary. The structure network TMN with managed network telecommunications, architecture of cybersecurity TCS were considered. Also relation of services and security threats was considered. Architecture cybersecurity TMN was developed.

Анализ статистики случаев несанкционированного проникновения в государственные и частные сети показал следующее. Наряду с резким увеличением инцидентов, связанных с несанкционированным доступом к информации, появилась проблема расширения диапазона взламываемых компьютерных сетей. Действия злоумышленников наносит не только коммерческий ущерб, но могут быть источником политических и военных кризисов.

В сложившейся ситуации государственные институты, ведущие промышленные и финансовые организации мира вынуждены расходовать на обеспечение кибербезопасности от 5 до 8 % своего бюджета. Основная часть расходуемых средств выделяется на программно-аппаратные комплексы систем защиты.

На основе стандартов, утверждённых Международным союзом электросвязи, существуют системы безопасности сети. Анализ уязвимости систем безопасности показал, что у всех присутствует существенный недостаток. В половине случаев проникновения риск становится угрозой.

При разработке стандартов и рекомендаций за основу обычно берутся более эффективные и универсальные методы, которые внедрены в продукты крупных фирм. В ходе такой стандартизации была создана концепция для построения систем управления сетями связи, разработанная и утверждённая Международным Союзом Электросвязи. Она определяет принципы создания единой системы управления для сетей разных уровней и масштабов, предоставляющих различные типы услуг. Эта система управления телекоммуникациями – Telecommunication Management Network (TMN) представляет собой отдельную сеть с целью стандартизации подходов к управлению сетями с различными типами оборудования для создания единой системы управления вне зависимости от производителей отдельных сетевых элементов. Данная сеть имеет интерфейсы с телекоммуникационной сетью (ТКС) в обусловленных точках стыка. Эти интерфейсы служат для обмена информацией управления и приема-передачи управляющих команд между системами управления и сетями связи. Также осуществляет управление их работой (рис. 1). Объектами управления сети TMN являются телекоммуникационные и сетевые ресурсы [1, 2].

Анализ рекомендаций МСЭ-Т [1…6] показал, что в них представлены уровни кибербезопасности (КБ) ТКС, уровни TMN, однако уровней КБ TMN нет.

Цель статьи – разработка архитектуры кибербезопасности системы управления телекоммуникационной системой, согласованной с архитектурой безопасности ТКС.

Для достижения данной цели поставлены и решены следующие задачи:

– рассмотреть структуру взаимодействия сети TMN с телекоммуникационной сетью;

– рассмотреть описание архитектуры кибербезопасности ТКС;

– соотнести услуги и угрозы безопасности;

– составить сравнительную таблицу уровней кибербезопасности ТКС и управления сетью телекоммуникаций – TMN;

– построение архитектуры кибербезопасности TMN.

Объектом исследования является КБ сложной системы управления телекоммуникациями.

Операционные системы осуществляют обработку всей информации, необходимой для выполнения функций управления. Рабочие станции обеспечивают пользовательский интерфейс, посредством которого обслуживающий персонал взаимодействует с сетью управления. Сеть передачи данных предназначена для организации связи между сетевыми элементами, операционными системами и другими компонентами TMN.

Система управления сетью строится иерархически и имеет следующие уровни: административного (бизнес) управления (BML – Business Management Layer); управление обслуживанием или услугами (SML – Service Management Layer); управление сетью (NML – Network Management Layer); управление элементами (EML – Element Management Layer); сетевые элементы (NEL – Network Element Layer) [1, 2].

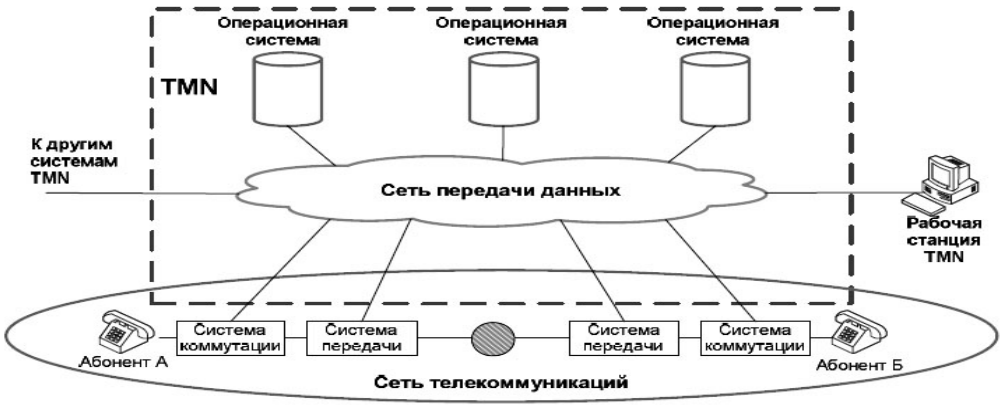

Рисунок 1 – Структурная схема взаимодействия сети TMN с сетью телекоммуникаций

TMN охватывает такие широкие области управления, как эффективность, восстановление, конфигурирование, тарификация и кибербезопасность.

Существуют три основных этапа формирования требований к безопасности. С помощью определения рисков устанавливаются угрозы для активов, оцениваются уязвимости и вероятность их появления, а также потенциальные внешние воздействия. Вторым этапом являются юридические, уставные, нормативные и договорные требования, которые должны быть удовлетворены организацией, ее торговыми партнерами, контрагентами и поставщиками услуг, а также социокультурная среда данных сторон. Третий етап – формирование специфического набора принципов, целей и требований бизнеса к обработке информации, разрабатываемый организацией для поддержания своей деятельности.

«*Киберсреда* включает пользователей, сети, устройства, все программное обеспечение, процессы, сохраненную или транзитную информацию, приложения, услуги и системы, которые могут быть прямо или косвенно соединены с сетями. *Кибербезопасность* – это набор средств, стратегии, принципы обеспечения безопасности, гарантии безопасности, руководящие принципы, подходы к управлению рисками, действия, профессиональная подготовка, практический опыт, страхование и технологии, которые могут быть использованы для защиты киберсреды, ресурсов организации и пользователя. Ресурсы организации и пользователя включают подсоединенные компьютерные устройства, персонал, инфраструктуру, приложения, услуги, системы электросвязи и всю совокупность переданной и/или сохраненной информации в киберсреде. Кибербезопасность состоит в попытке достижения и сохранения свойств безопасности у ресурсов организации или пользователя, направленных против соответствующих угроз безопасности в киберсреде. Общие задачи обеспечения безопасности включают следующее: доступность; целостность, которая может включать аутентичность и неотказуемость; конфиденциальность [4]».

1. Описание архитектуры кибербезопасности ТКС. Для эффективного обеспечения безопасности в сети рекомендуется реализовать мероприятия безопасности; чем их больше введено, тем более эффективно обеспечивается безопасность. Этот метод построения безопасности сети включает средства сетевого администратора, физической безопасности, мониторинга, программного обеспечения ТКС, инструментов обеспечения безопасности, аудита безопасности.

Аудит безопасности сети включает тестирование устойчивости сети к физическим атакам ее системы безопасности, а также предусматривает установку брандмауэра для обеспечения межсетевой защиты. Сетевой администратор выполняет основные задачи конфигурации сетевой безопасности и является более эффективным дорогого брандмауэра.

Физическая безопасность направлена на обеспечение безопасности как изнутри, так и снаружи. Управление доступом к сетям, в отношении допустимого использования паролей и установки программного обеспечения, должно производиться в соответствии с политикой организаций.

Мониторинг. С целью остановки атак системному администратору следует прочитывать журнал регистрации его главной машины каждый день.

Программное обеспечение телекоммуникационной сети. Для учёта недостатков системы безопасности системный администратор должен изучить, какие порты будет использовать приобретаемое программное обеспечение, с какими пользовательскими счетами будет взаимодействовать программа, и какие разрешения доступа к каталогу требует программа.

Согласно [4] для системы передачи данных включены следующие угрозы:

– уничтожение информации и/или других ресурсов;

– искажение или изменение информации;

– кража, перемещение или потеря информации и/или других ресурсов;

– раскрытие информации;

– прерывание обслуживания.

Угроза – потенциальное нарушение защиты.

Так же в соответствии с [3] угрозы делятся на случайные и преднамеренные, также они могут быть активными и пассивными. *Случайные* – возникают без предварительного умысла. *Пассивные* – при их реализации нет изменения информации.

В табл. 1 представлено схематическое соотношение услуг по обеспечению безопасности применительно к угрозам безопасности, определённые в Рек. МСЭ-Т X.805 [3]. Соотношение идентично для каждой области защиты. «Да» в ячейке, сформированной пересечением столбцов и строк таблицы, означает, что конкретной угрозе безопасности противостоит соответствующий механизм защиты.

Таблица 1 – Соотношение услуг и угроз безопасности

Услуги безопасности	Угрозы безопасности				
	Уничтожение информации или других ресурсов	Искажение или изменение информации	Кража, удаление или потеря информации и других ресурсов	Раскрытие информации	Прерывание обслуживания
Контроль доступа	ДА	ДА	ДА	ДА	
Аутентификация			ДА	ДА	
Отказоустойчивость	ДА	ДА	ДА	ДА	ДА
Конфиденциальность данных			ДА	ДА	
Безопасность связи			ДА	ДА	
Целостность данных	ДА	ДА			
Доступность	ДА				ДА
Секретность				ДА	

В МСЭ-Т X.805 [3] плоскость безопасности – это определенный тип действия сети, защищенный с помощью услуг по обеспечению безопасности. В [3] определено три плоскости безопасности для представления трех типов защищенных действий, которые происходят в сети. Плоскостями безопасности являются: плоскость менеджмента, плоскость контроля (сигнализации) и плоскость конечного пользователя.

«Эти плоскости безопасности предназначены для конкретных нужд безопасности, связанных с деятельностью управления сетью, контроля сети или деятельностью по передаче сигналов и деятельностью конечного пользователя соответственно. Предлагается разрабатывать сети таким образом, чтобы события на одной плоскости безопасности хранились изолированно от других плоскостей безопасности [4]».

На рис. 2 показана архитектура кибербезопасности в ТКС общего пользования, включающая услуги по обеспечению безопасности в каждой плоскости КБ [4].

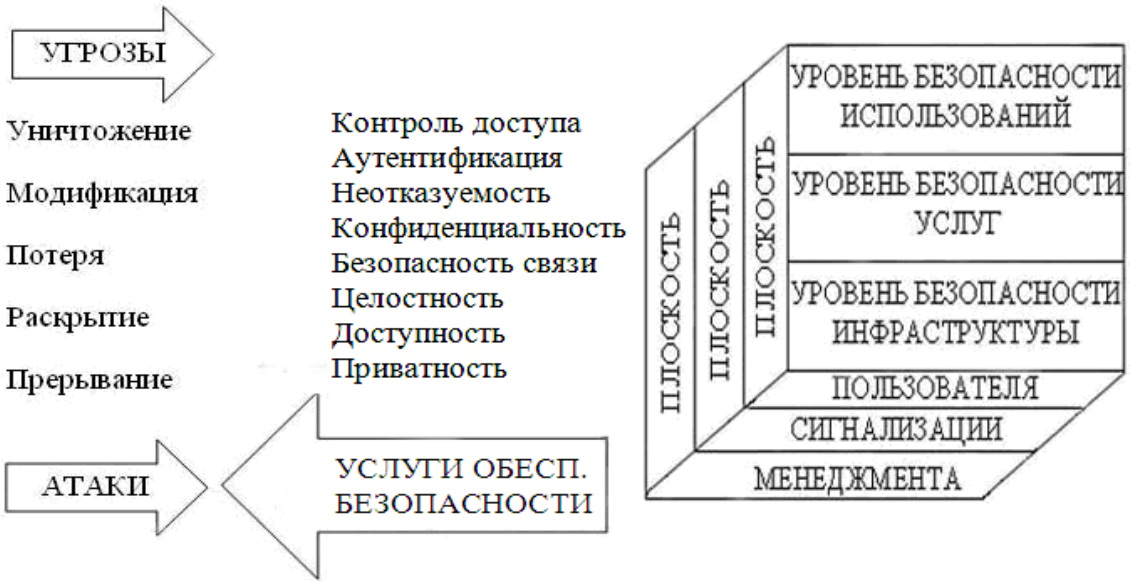

Рисунок 2 – Архитектура кибербезопасности ТКС передачи информации

При отсутствии слабого места в системе или если оно не используется угрозой, потенциальная угроза не всегда вредна. Однако при каждой угрозе существует риск. Оценка риска может быть разделена на оценку вероятности каждой угрозы и оценку воздействия, которое может иметь угроза. Оценки угрозы и риска должны быть частями итеративного процесса: появление новых угроз возможно, например, при принятии мер угрозы криптографическим ключем возникают в результате реализации криптографических мер.

Архитектура кибербезопасности системы управления обеспечивает механизм, позволяющий реализовать информационную безопасность. Для инициирования и контролирования процесса обеспечения информационной безопасности, необходимо создать в организации соответствующую структуру управления.

2. Архитектура кибербезопасности TMN. В табл. 2 предложены взаимосвязи уровней управления сетью TMN и кибербезопасностью, также предложены уровни кибербезопасности TMN. Они похожи с уровнями системы управления сетью TMN, но нет сетевых элементов, так как они присутствуют в самой системе и соответственно защищаются.

На рис. 3 показана архитектура кибербезопасности TMN в соответствии с табл. 2.

При помощи плоскостей безопасности есть возможность установить различия в конкретных аспектах безопасности, которые связаны с определенными видами деятельности, так же дает возможность независимым образом обращаться к ним.

Отличием архитектуры КБ ТКС от архитектуры КБ TMN является различие в угрозах и методах КБ, а также в уровнях и плоскостях архитектуры.

Таблица 2 – Сравнение уровней управления сетью TMN и кибербезопасности ТКС

Уровни КБ ТКС	Уровни системы управления сетью TMN	Уровни КБ TMN
Инфраструктуры	Административного управления	Административного управления
Услуг	Управления услугами	Управления услугами
Управления	Управления сетью TMN	Управления TMN
	Управления элементами	Управления элементами TMN
	Сетевых элементов	

Рисунок 3 – Архитектура кибербезопасности TMN

Данные плоскости предназначены для определенных нужд безопасности, связанных с деятельностью менеджмента TMN и безопасность транспортировки информации как внутри сети, так и за ее пределами. Исходя их того, что в этой системе нет пользователя, следовательно, в данной архитектуре только плоскость менеджера и транспорта.

Выводы. В статье представлены уровни КБ TMN, составлена и представлена архитектура КБ системы управления телекоммуникационной системой, согласованная с архитектурой безопасности ТКС.

Литература

1. ITU-T Recommendation M.3010. Principles for a telecommunications management network. (Принципы системы управления телекоммуникациями) – Женева, 1992.–70с. Режим доступа: http://www.itu.int/ITU-T/recommendations/index.aspx?ser=M
2. Telecommunication Management Network, TMN (Система управления сетями операторов электросвязи). – Режим доступа: http://ru.wikipedia.org/wiki/TMN
3. Рекомендация МСЭ-Т X.805 Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами. – Женева, 2003. – 28 с.
4. Рекомендация МСЭ-Т X.1205 Обзор кибербезопасности. – Женева, 2008. – 64 с.
5. Рекомендация МСЭ-Т M.3016.2 Безопасность для плоскости управления: услуги по обеспечению безопасности. – Женева, 2005. – 16 с.
6. Рекомендация МСЭ-Т M.3016.3 Безопасность для плоскости административного управления: Механизм безопасности. – Женева, 2005. – 30 с.
7. Управление на сетях связи по стандартам TMN. – Режим доступа: http://ruzhnikov.ru/wp-content/uploads/2010/02/tmn-lect.pdf
8. *Гребешков А. Ю.* Управление сетями электросвязи по стандарту TMN: учеб. пособ. / Гребешков А.Ю.– М.: Радио и связь, 2004 . – 155 с. ISBN 5-256-01730-6.
9. Архитектура интеллектуальной системы управления. – Режим доступа: http://kpiarticle.com/kpiarticle.com/www/wp-content/uploads/2010/04/Архитектура-интеллектуальной-системы-управления.pdf).
10. Безопасность в электросвязи и информационных технологиях, июнь, 2006. – Режим доступа: http://www.itu.int/dms_pub/itu-t/opb/hdb/T-HDB-SEC.03-2006-PDF-R.pdf.