МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

РАЗРАБОТКА СТРУКТУРЫ ЗАЩИЩЕННОЙ ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ ОБЪЕКТА

Методические указания к выполнению курсового проекта по дисциплине «Проектирование защищенных телекоммуникационных систем» для студентов специальности 10.05.02

Курск 2017

УДК 004.725.7

Составители: А.Л. Марухленко

Рецензент
Кандидат технических наук, доцент *А.Г. Спеваков*

Разработка структуры защищенной телекоммуникационной системы объекта: методические указания к выполнению курсового проекта / Юго-Зап. гос. ун-т; сост. А. Л. Марухленко Курск, 2017.-17 с.

Содержат сведения по вопросам проектирования и разработки защищенной телекоммуникационной системы объекта Указывается порядок выполнения курсового проекта, правила оформления.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по направлению подготовки 10.05.02 и предназначены для изучения дисциплины «Технология обеспечения информационной безопасности объекта».

Текст печатается в авторской редакции

Подписано в печать 01.11.2017. Формат 60х84 1/16.
Усл.печ. л. 1,0. Уч.-изд.л. 0,9. Тираж 30 экз. Заказ _____. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Современная инфокоммуникационная система представляет собой универсальную многоцелевую сеть, предназначенную для передачи речи, изображений и данных с использованием технологии коммутации пакетов. Концепция создания такой системы предусматривает поддержку неограниченного набора услуг с гибкими возможностями по их управлению, реализацию универсальной транспортной мультипротокольной сети с распределенной коммутацией, интеграцию с традиционными сетями связи.

Фундаментом любой инфокоммуникационной системы является мультипротокольная/мультисервисная транспортная сеть связи на основе пакетной передачи данных, обеспечивающая перенос разнородного трафика с использованием различных протоколов передачи. На более высоких уровнях модели OSI инфокоммуникационная система открывает массу возможностей построения наложенных сервисов поверх универсальной транспортной среды - от почтовых сервисов до пакетной телефонии (VoIP), передачи изображений, видеоконференцсвязи и т.п. Инфокоммуникационная система обеспечивает доступность услуг вне зависимости от местоположения пользователя и используемых им интерфейсов.

С появлением подобных систем остро встали вопросы информационной безопасности ИТ-инфраструктуры организации, использующей ее услуги, оценки защищенности ИТ-инфраструктуры. Возникла необходимость выявлять и классифицировать различные угрозы информационной безопасности и разрабатывать соответствующие модели защиты. Необходимыми стали разработка и внедрение комплексных технических решений по защите информации при инфокоммуникационном взаимодействии, как внутри организации, так и с другими организациями и внешними информационными ресурсами.

Задача создания комплексных решений по защите информации подобных систем представлена на рисунке 1.

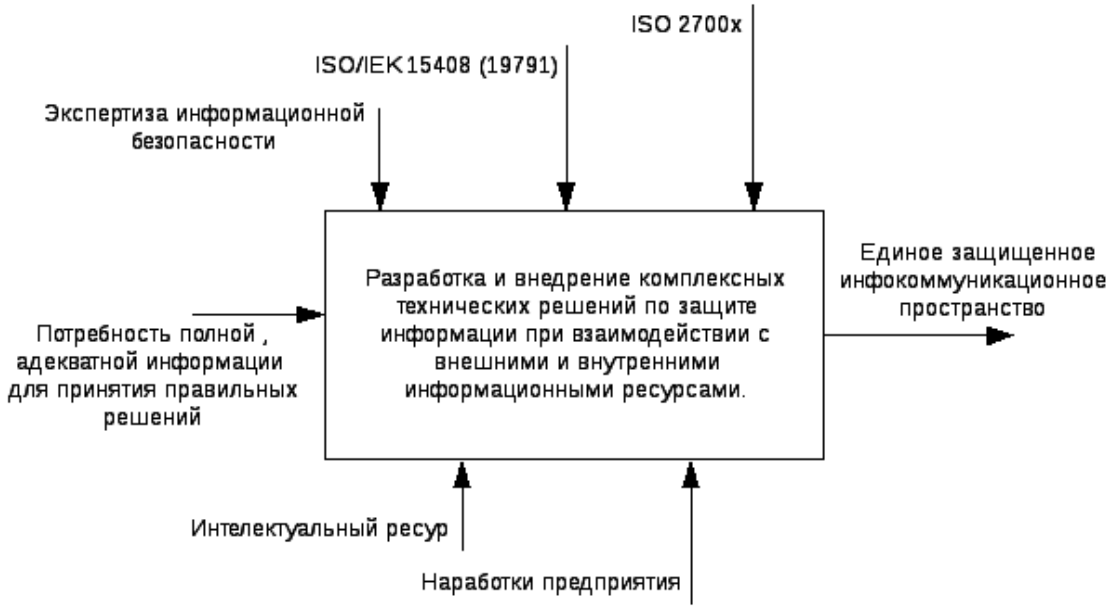

Рисунок 1 – Создание комплексных решений по защите информации

Пользователями защищенных телекоммуникационных систем (ЗТКС) могут являться:

- коммерческие организации;
- органы государственной власти;
- ведомства (управления) силовых структур.

При этом, для потребителей системы обеспечивается:

- защита информации;
- технология обеспечения безопасности голосовой связи, встроенная в инфраструктуру сети;
- технология обеспечения безопасности, которая охватывает инфраструктуру, управление вызовами, оконечные устройства и уровень приложений;
- предоставление гарантированного качества переноса трафика.

Основными технико-экономическими задачами построения и поддержания функционирования систем защиты информации (СЗИ)

являются задачи проектирования оптимальных СЗИ, поиска способов сокращения расходов на создание СЗИ при сохранении уровня защищенности информации и разработки методологии рационального управления СЗИ в процессе их функционирования.

Проектирование СЗИ, оптимальных по технико-экономическим показателям, полностью вписывается в методологию проектирования больших систем, разработанной в классической теории систем. В качестве же основы для построения оптимизирующего алгоритма могут быть использованы зависимости между уровнем защищенности информации и ресурсами, вкладываемыми в осуществление каждой из функций защиты полного их множества. Наиболее перспективным способом снижения расходов на создание СЗИ является типизация и стандартизация их компонентов или целых систем.

1. ЖИЗНЕННЫЙ ЦИКЛ ЗТКС

Разработка проектов больших ТКС связанна с работой коллективов в несколько десятков, а то и сотен человек из нескольких организаций. Организация такой работы возможна только при наличии нормативно-методических документов, регламентирующих различные аспекты процессов деятельности заказчика, разработчиков, поставщиков и строительно-монтажных организаций.

Комплекс таких документов называется нормативно-методическим обеспечением (НМО). Эти документы регламентируют:

- порядок разработки, внедрения, сопровождения ТКС (Устав);
- общие требования к составу ТКС, связям между ее компонентами, а также к ее качеству – техническое задание (ТЗ);
- виды, состав и содержание проектной и рабочей документации (Стандарт).

Все документы НМО классифицируются по следующим признакам:

- виды регламентации (Стандарт, РД, положение, инструкция и т.д.);
- статус регламентирующего документа (международный, отраслевой, предприятия);
- области действия документов (заказчик, подрядчик);
- объекту регламентации или методического обеспечения (ТКС, бизнес-процесс).

Нормативной базой НМО являются:

- международные стандарты ISO/IEC (International organization of standardization/international electrotechnical commision);
- стандарты РФ (ГОСТ Р);
- стандарты организаций (СТ/П) – стандарт предприятия.

Процессы создания любой автоматизированной системы (АС), в том числе и телекоммуникационной системы, регламентированы стандартами:

- ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;
- ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;
- ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем».

Жизненный цикл ТКС (ЖЦ ТКС) определяется как период времени, который начинается с момента принятия решения о необходимости создания ТКС и заканчивается в момент ее полного изъятия из эксплуатации.

Основным нормативным документом, регламентирующим состав процессов ЖЦ ТКС, является международный стандарт ISO/IEC 12207:1995 он определяет структуру ЖЦ, содержащую процессы, действия и задачи, которые должны быть выполнены во время создания ТКС (его российский аналог ГОСТ Р ИСО/МЭК 12207-99 введен в действие в июле 2000 г.). В данном стандарте процесс определяется как совокупность взаимосвязанных действий, преобразующих некоторые входные данные в выходные. Каждый процесс характеризуется определенными задачами и методами их решения, исходными данными, полученными от других процессов, и результатами.

Каждый процесс разделен на набор действий, каждое действие - на набор задач. Каждый процесс, действие или задача инициируется и выполняется другим процессом по мере необходимости, причем не существует заранее определенных последовательностей выполнения (естественно, при сохранении связей по входным данным).

2. СТРУКТУРНЫЙ ПОДХОД К АНАЛИЗУ И ПРОЕКТИРОВАНИЮ ТКС

Основной проблемой, которую приходится решать при создании больших систем любой природы является проблема сложности. Правильная декомпозиция системы является главным способом преодоления сложностей больших систем. Понятие правильно по отношению к декомпозиции означает следующее:

– количество связей между отдельными подсистемами должно быть минимальным.

– связанность отдельных частей внутри каждой подсистемы должно быть максимальным.

Структура системы должна быть такой, чтобы все взаимодействия между ее подсистемами укладывались в ограничения:

– каждая подсистема должна инкапсулировать своё содержимое;

– каждая подсистема должна иметь четко определенный интерфейс с другими подсистемами.

В проектировании телекоммуникационных систем применяются два основных подхода к декомпозиции систем.

Функционально-модульный (структурный подход) – в основу положен принцип функциональной декомпозиции, при которой структура системы описывает в терминах иерархии ее функций и передачей информацией между отдельными функциональными элементами.

Объектно-ориентированный подход – использует объектную декомпозицию, при которой структура системы описывается в терминах объекта и связей между ними, а поведение системы описывается в терминах обмена сообщениями между объектами.

3. ОСОБЕННОСТИ ПРОЕКТИРОВАНИЯ НА СОВРЕМЕННОМ УРОВНЕ И СИНТЕЗ КСИБ

Выделяют следующие подходы к проектированию:

1) Использование типовых СЗИ.

Выбирается один из имеющихся типовых проектов полной СЗИ. Осуществляется привязка типового проекта к условиям конкретной ТКС.

Целесообразно применять, когда: требования к ЗИ не очень высокие, строго определенная структура ТКС, архитектура ТКС близка к одной из типовых, требования и условия защиты во всех однотипных структурных компонентах (ТСК) однородны.

2) Использование типовых структурно-ориентированных компонентов (ТСК) СЗИ.

Для каждого ТСК ТКС выбирается один из типовых проектов компонента СЗИ. Осуществляется привязка проектов к условиям ТСК. Производится объединение всех компонентов в СЗИ.

Целесообразно применять, когда: требования к ЗИ не очень высокие, строго определенная структура ТКС, архитектура ТКС близка к одной из типовых, требования и/или условия защиты в различных ТСК различны.

3) Использование функционально-ориентированных компонентов СЗИ.

Для каждой группы компонентов ТКС выбираются по одному из типовых функционально ориентированных компонентов СЗИ. Осуществляется привязка проектов к условиям группы. Производится объединение компонентов в подсистему СЗИ. Все подсистемы объединяются в СЗИ.

Целесообразно применять, когда: требования к ЗИ не очень высокие, в ТКС выделяются компактно расположенные компоненты, требования и условия защиты в различных частях ТКС различны.

4) Разработка индивидуального проекта СЗИ, для реализации которого создаются индивидуальные средства защиты.

Разрабатывается проект индивидуальной СЗИ. Разрабатываются средства для реализации проекта. Осуществляется наладка СЗИ.

Целесообразно применять, когда: требования к ЗИ очень высокие, защищаемая информация имеет особую важность, ТКС является уникальной.

5) Разработка индивидуального проекта с использованием типового проекта (ТПР) по средствам защиты.

Разрабатывается проект индивидуальной СЗИ, для реализации которого используются ТПР по основным средствам защиты.

Целесообразно применять, когда: требования к ЗИ очень высокие, ТКС имеет ярко выраженные особенности.

6) Использование ТПР по многорубежной модели.

На плане территориального размещения ТКС намечаются рубежи защиты. Для каждого рубежа выбирается один из типовых проектов подсистемы СЗИ. Осуществляется привязка проектов к условиям каждого реального рубежа. Все подсистемы объединяются в СЗИ.

Целесообразно применять, когда: требования к ЗИ не слишком высокие, компоненты ТКС распределены на значительной территории, ТКС имеет сильно распределенную структуру, требования и условия защиты в различных компонентах ТКС различны.

4. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОБЛЕМЫ СИНТЕЗА СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ИС, АС, ТКС

Оценки параметров СЗИ в условиях высокой степени неопределенности условий ее функционирования должны вычисляться с использованием не одной математической модели, а согласованного семейства моделей, адаптивно конструирующихся одна из другой и, таким образом, непрерывно совершенствующихся на основе оптимального выбора исходных данных.

При синтезе оптимальных систем защиты исходными должны явиться следующие два положения:

– выбор математически вычисляемого критерия оптимальности в соответствии с архитектурой системы защиты и технологией обработки информации на объекте;

– четкая математическая формулировка задачи, учитывающая все априорные сведения и позволяющая решить ее в соответствии с принятым критерием.

Итогом решения задачи синтеза оптимальной системы защиты и его конечной целью должны быть четыре содержательных результата:

– архитектура системы защиты;

– количественная оценка качества ее функционирования;

– оценка практической чувствительности разработанных моделей к отклонениям от априорных данных;

– физическая реализуемость синтезируемых систем защиты в современных системах обмена данными (соответствие технологии обработки информации уровню ее защиты).

Под эффективностью систем защиты информации будем понимать эффективность ее использования в качестве активного средства в операции обеспечения конфиденциальности обработки, хранения и передачи

информации. При этом, оценка эффективности операции заключается в выработке оценочного суждения относительно пригодности заданного способа действий специалистов по защите информации или приспособленности средств защиты к решению задач.

Введение показателя эффективности требует также определения критерия эффективности, как правила, позволяющего сопоставлять стратегии, характеризующемся различной степенью достижения цели, и осуществлять выбор стратегий из множества допустимых.

Теоретические основы построения оптимальных систем защиты исключительно сложны и, несмотря на интенсивность исследований в этой предметной области, еще далеки от совершенства.

Таким образом, проектирование и оценка реализации проекта защищенной телекоммуникационной системы становится очень трудоемким процессом. На практике применяются подходы, которые позволяют уменьшить трудоемкость разработки и использующие собственные или заимствованные наработки. Но это не дает возможности сколь-нибудь значительно уменьшить трудоемкость процесса оценки защищенности. Хотя здесь не утверждается, что этот (последний) процесс не поддается автоматизации. В любом случае очень важным является опыт работника/организации.

Курсовой проект позволяет, в рамках изучения дисциплины приблизиться к практической стороне проектирования защищенной телекоммуникационной системы. Для выполнения необходимо самостоятельно систематизировать информацию, как по объекту проектирования, так и по методикам проектирования и оценки защищенности телекоммуникационной системы.

5. ПОЯСНЕНИЕ К ТЕХНИЧЕСКОМУ ЗАДАНИЮ К КУРСОВОМУ ПРОЕКТУ

В рамках курсового проекта предлагается разработать типовое проектное решение защищенной телекоммуникационной системе в рамках одного из сегментов существующей сети, предназначенной для работы с информацией ограниченного доступа. Для этого необходимо:

- выбрать вариант, в котором представлена отрасль предприятия. Номер варианта соответствует номеру в списке группы (Приложение А);
- приступить к выбору средств защиты;
- показать выбор одного из средств с использованием инструмента системного подхода к сложным проблемам принятия решений;
- составить полный перечень необходимого комплекта средств защиты информации;
- рассчитать стоимость типового проектного решения.

6. КРИТЕРИИ ОЦЕНКИ ПРОЕКТА

Работа считается выполненной (оценки – удовлетворительно или хорошо), если:

- в ней есть структура сегментов сети рассматриваемого предприятия, при этом однотипные сегменты достаточно представить единожды;
- хотя бы кратко описаны технологии, примененные в рамках реализации концепции ИБ предприятия или выбранные технические средства телекоммуникационной системы.

Полнота описания влияет на результирующую оценку. При защите проекта задаются вопросы по каждому из этапов выполнения проекта, чтобы оценить самостоятельность выполнения и уровень понимания сути работы. В случае верного ответа на 80%-90% вопросов преподавателя – ставится оценка «отлично».

7. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1) Шувалов В.П., Величко В.В., Субботин Е.А., Ярославцев А.Ф. Телекоммуникационные системы и сети. Том 3. Мультисервисные сети (2005)

2) Петраков А.В. Основы практической защиты информации. 2-е изд. Учебн. пособие. – М.: Радио и связь. 2000. – 368 с.

3) Цифровые и аналоговые системы передачи: Учебник для вузов/ В.И.Иванов, В.Н.Гордиенко, Г.Н.Попов и др.; Под ред. В.И.Иванова. – 2-е изд. – М.: Горячая линия – Телеком, 2003. – 232 с.

4) Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. Сети связи: Учебник для ВУЗов. - СПб.: БХВ-Петербург, 2010. - 400 с.

5) Буч Г. Объектно-ориентированный анализ и проектирование. – М.: Вильямс, 2008.

6) А.В. Росляков. Виртуальные частные сети. Основы построения и применения. - М.: Эко-Трендз, 2006. - 242 с.

7) Выпускная квалификационная работа: Методические рекомендации по технологии разработки, оформлению и защите выпускной квалификационной работы студентами. Состав. Ткаченко А.В., КГТУ, Курск, 2008.

ПРИЛОЖЕНИЕ А

1) Разработка структуры защищенной телекоммуникационной системы для предприятий нефтегазовой отрасли.

2) Разработка структуры защищенной телекоммуникационной системы для органов местного самоуправления.

3) Разработка структуры защищенной телекоммуникационной системы для предприятий банковской сферы.

4) Разработка структуры защищенной телекоммуникационной системы для муниципальных предприятий.

5) Разработка структуры защищенной телекоммуникационной системы для машиностроительной отрасли.

6) Разработка структуры защищенной телекоммуникационной системы для энергетической отрасли.

7) Разработка структуры защищенной телекоммуникационной системы для военизированной отрасли.

8) Разработка структуры защищенной телекоммуникационной системы для строительной отрасли.

9) Разработка структуры защищенной телекоммуникационной системы для металлургической отрасли

10) Разработка структуры защищенной телекоммуникационной системы для жилищно-коммунальное хозяйства.