МЕТОДИКА ОЦЕНКИ УПРАВЛЯЕМОСТИ ФРАГМЕНТА СЕТИ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ С УЧЕТОМ ВЛИЯНИЯ МНОЖЕСТВЕННОСТИ ЦЕНТРОВ УПРАВЛЕНИЯ И ДЕСТРУКТИВНЫХ ПРОГРАММНЫХ ВОЗДЕЙСТВИЙ

Бегаев А.Н.[1], Стародубцев Ю.И.[2], Фёдоров В.Г.[3]

В настоящее время развертывание информационно–телекоммуникационных систем для организации процесса обмена данными между территориально разнесенными подразделениями компаний осуществляется в тесном взаимодействии с сетью связи общего пользования, особенностью которой является ее многооператорность с соответствующим количеством центров управления. Фактор множественности центров управления влечет за собой увеличение цикла управления сетью связи. При функционировании интегрированных сетей создаются условия для осуществления деструктивных программных воздействий. Это означает, что к условиям децентрализованного управления сетью операторами связи добавляется еще фактор деструктивных управляющих воздействий злоумышленника, потенциально имеющего возможность удаленного управления элементом сети в части касающейся. Что также приведёт к изменению цикла управления сетью. Разработана методика, позволяющая определить степень влияния множественности центров управления на управляемость сети связи и оценить защитные свойства заданного фрагмента сети от деструктивных программных воздействий. С помощью методики можно решать задачи по выявлению элементов сети, в отношении которых необходимо осуществлять защитные мероприятия от деструктивных программных воздействий для сохранения заданного режима управления сетью.

***Ключевые слова**: система управления, многооператорность, деструктивные управляющие воздействия.*

DOI: 10.21681/2311-3456-2017-4-32-39

Введение

Система связи общего пользования (ССОП) относится к классу сложных, иерархических, организационно-технических и динамичных систем [1-2]. Ее сложность определяется большим числом взаимосвязанных частей (сетей связи, подсистем сигнализации, синхронизации, тарификации и т. д.) и элементов, многообразием связей между ними, значительной разветвленностью и неоднородностью, а главное высокой динамикой изменения этих характеристик (параметров), которая зависит от количества органов и объектов управления, количества управляемых параметров и реализуемых алгоритмов.

Принимая во внимание то, что развертывание информационно-телекоммуникационных систем для организации процесса обмена данными между территориально разнесенными подразделениями компаний в настоящее время осуществляется в тесном взаимодействии с ССОП, необходимо учитывать сложившиеся принципы ее построения и особенности функционирования [3].

Как и любой сложный технический объект, ССОП требует выполнения различных действий для поддержания ее в рабочем состоянии, анализа и оптимизации ее производительности, защиты от внутренних и внешних угроз. Среди многообразия средств, привлекаемых для достижения этих целей, главное место занимает система управления сетью.

Система управления сетью – это сложный программно–аппаратный комплекс, который контролирует сетевой трафик и управляет коммуникационным оборудованием информационно-телекоммуникационной сети [4, 5].

Для решения задачи управления сетью необходимо иметь возможность управления отдельным элементом (объектом управления) и его параметрами. Как правило для этой цели на каждом элементе устанавливается специализированная автономная программа конфигурирования и управления – программный агент. Такие агенты могут встраиваться в управляемое оборудование либо работать на устройстве, подключенном к интерфейсу управле-

1 Бегаев Алексей Николаевич, кандидат технических наук, ЗАО «Эшелон-СЗ», г. Санкт-Петербург, a.begaev@nwechelon.ru

2 Стародубцев Юрий Иванович, доктор военных наук, профессор, Военная академия связи им. С.М.Будённого, г. Санкт-Петербург, ys@e-nw.ru

3 Фёдоров Вадим Геннадиевич, Военная академия связи им. С.М.Будённого, г. Санкт-Петербург, vadim.fedorov.53@mail.ru.

ния такого устройства. Агент поддерживает связь с центром управления сетью, который посылает ему запросы и команды на выполнение определенных операций. Каждый агент управляет одним или несколькими элементами сети.

Агент может выполнят следующие функции:

- хранить, извлекать и передавать по запросам извне информацию о технических и конфигурационных параметрах устройства (модель устройства, число портов, тип портов, тип ОС и др.);

- выполнять, хранить и передавать по запросу извне характеристики функционирования устройства (число принятых пакетов, число отброшенных пакетов, степень заполнения буфера, состояние порта);

- изменять по командам, полученным извне, конфигурационные параметры (сетевой адрес, идентификатор, географическое положение).

Для каждого управляемого объекта в сети создается и хранится на нем база данных управляющей информации. База данных управляющей информации содержит значения множества различных типов переменных, характеризующих конкретный управляемый объект. Например, база данных маршрутизатора включает такие характеристики, как:

- тип протокола, который поддерживает интерфейс (эта переменная принимает значения всех стандартных протоколов);

- количество портов, их тип, желаемый статус порта (*up* – готов передавать пакеты, *down* – не готов передавать пакеты);

- таблица маршрутизации;

- количество кадров и пакетов протоколов канального, сетевого и транспортного уровней, прошедших через эти порты.

Для изменения этих переменных используется режим удаленного управления, который реализуется специальным протоколом прикладного уровня (*SNMP*, *telnet*, *Secure SHell*), работающим поверх транспортных протоколов, которые связывают удаленный узел с сетью. Режим удаленного управления позволяет центру управления через агента устройства изменять значения какой-либо переменной или списка переменных.

Процесс управления сетью связи, как и любой процесс, происходит во времени, поэтому показателем для оценки управляемости системы связи является средняя продолжительность цикла управления ($\overline{T}_{ЦУ}$).

Цикл управления – полная совокупность периодически следующих друг за другом составляющих процесса управления. Он включает: получение (сбор) управляющим объектом (органом, центром управления) необходимой информации; обработку органом (центром) управления полученной информации в целях выработки соответствующего правильного решения; передачу решения объектам управления для реализации [6].

Это означает, что на основе имеющихся данных о сети (собранных и прогнозируемых) и понимания эффективности ее функционирования органу (центру) управления необходимо принять решение о том, в какое время, какое управляющее воздействие необходимо реализовать.

Для оптимального функционирования системы связи указанные затраты времени не должны превышать требуемые $\overline{T}_{ЦУ} \le \overline{T}_{доп.ЦУ}$. При несоблюдении данного условия реакция системы теряет смысл, т.к. не обеспечивается должная эффективность (опоздание цикла управления к динамике изменения ситуации на сети).

Оптимальным в этой ситуации вариантом построения системы управления является – централизованное управление [7], при котором все функции управления осуществляет один центр управления в предположении, что количество объектов управления и управляемых параметров сбалансировано с возможностями органа управления (рис.1).

Необходимо отметить, что сейчас на телекоммуникационном рынке присутствует значитель-

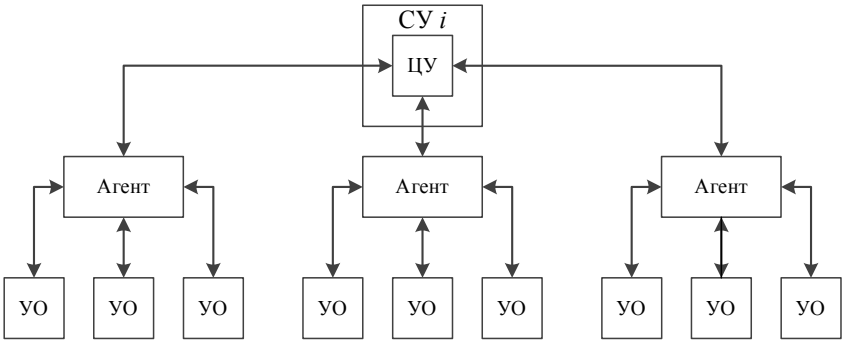

***Рис. 1**. Схема централизованного построения системы управления сетью*

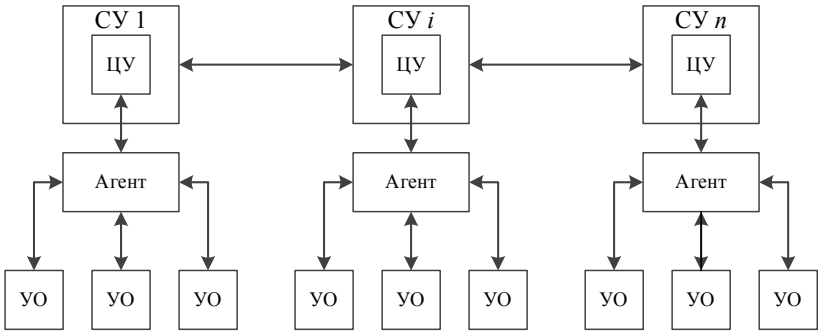

***Рис. 2**. Схема управления сетью с множеством центров (органов) управления*

ное количество операторов связи, каждый из которых в процессе эксплуатации сети связи модернизирует и преобразовывает существующую структуру сети в части касающейся. Вследствие этого особенностью современной ССОП является ее многооператорность, а, следовательно, отсутствие единого центра (системы) управления сетью (рис. 2) [8]. Такая высокая степень децентрализации управления приводит к тому, что любые изменения на фрагменте сети требуют согласованных, в части касающейся, действий всех операторов, предоставляющих услуги. В результате – длительность цикла управления увеличивается.

С точки зрения информационной безопасности немаловажным является тот факт, что при функционировании интегрированных сетей связи, использующих для обмена данными ресурсы ССОП, создаются условия для ведения злоумышленниками компьютерной разведки и осуществления деструктивных программных воздействий (ДПВ) [9]. Учитывая, что передаваемая информация, как правило надежно защищена с криптографической точки зрения, а взаимодействие осуществляется только с «доверенными абонентами», наиболее эффективными являются воздействия, направленные на срыв (блокирование) процесса передачи данными путем захвата некоторых (всех) функций управления на элементах ССОП и осуществления деструктивных управляющих воздействий [10].

Таким образом, в этой ситуации общее число центров управления в ССОП будет складываться из двух компонент. Во-первых, это легитимные центры управления операторов связи предоставляющих услуги, во-вторых могут появиться нелегитимные, которые будут пытаться путем осуществления деструктивных управляющих воздействий изменить определенные параметры управления на элементах сети связи. Это означает, что к условиям децентрализованного управления сетью операторами связи добавляется еще фактор деструктивных управляющих воздействий злоумышленника, потенциально имеющего возможность удаленного управления элементами сети в части касающейся (рис. 3).

Исходя из этого задачей защиты процесса передачи данных при использовании ресурсов ССОП является определение пораженных элементов фрагмента ССОП, при которых распространение влияния ДПВ охватит критическую часть этого фрагмента сети, что приведет к ее деградации и срыву управления (блокаде отдельных элементов сети, снижению их реальной пропускной способности, срыву или блокированию процесса передачи данных). После чего могут быть реализованы защитные мероприятия, направленные на минимизацию количества элементов сети подверженных деструктивным управляющим воздействиям.

Таким образом сложившаяся ситуация вызывает необходимость принципиального изменения

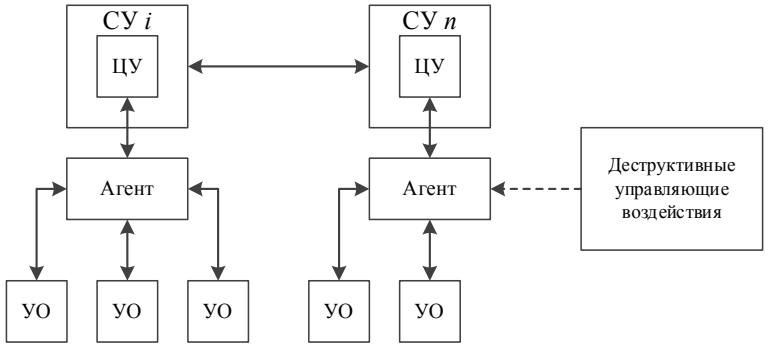

***Рис. 3**. Вариант осуществления деструктивных управляющих воздействий*

подходов к обеспечению защиты информационных ресурсов выделенных сетей, основанные на использовании ресурсов ССОП. С учетом выявленных особенностей функционирования ССОП ставится задача на разработку научно-методического обеспечения по оценке управляемости фрагмента ССОП с учетом влияния множественности центров управления и ДПВ.

Постановка задачи на исследование

Методика относится к области информационной безопасности интегрированных ИТКС. Целью методики является оценка управляемости фрагмента ССОП, заключающейся в изменении длительности цикла управлении, в зависимости от количества легитимных и нелегитимных центров управления.

Основными исходными данными методики являются: границы фрагмента ССОП; общее количество элементов ССОП, функционирующих в указанном фрагменте ($N_{ССОП}$); количество элементов фрагмента ССОП подверженных ДПВ ($N_{ССОП}^{ДПВ}$); количество центров управления на фрагменте ССОП ($N_{ЦУ}$); общее количество параметров управления i-го элемента фрагмента ССОП ($R_i^{УП}$); количество параметров управления i-го элемента фрагмента ССОП подверженных ДПВ ($R_i^{ДПВ}$); среднее время цикла управления сбалансированной системы управления ($\overline{T}_{исхЦУ}$).

Основными ограничениями и допущениями являются: элементы ССОП – это стационарные объекты с общеизвестными координатами, функционирующими в режиме, характерном для систем массового обслуживания; действия ДПВ – захват привилегий и управление параметрами элемента сети; все элементы фрагмента ССОП равновероятно подвержены ДПВ; исходная система управления ССОП функционирует в режиме, при котором количество центров управления и элементов сети сбалансировано и обеспечивается соответствие параметров качества сетевых соединений требуемым значениям.

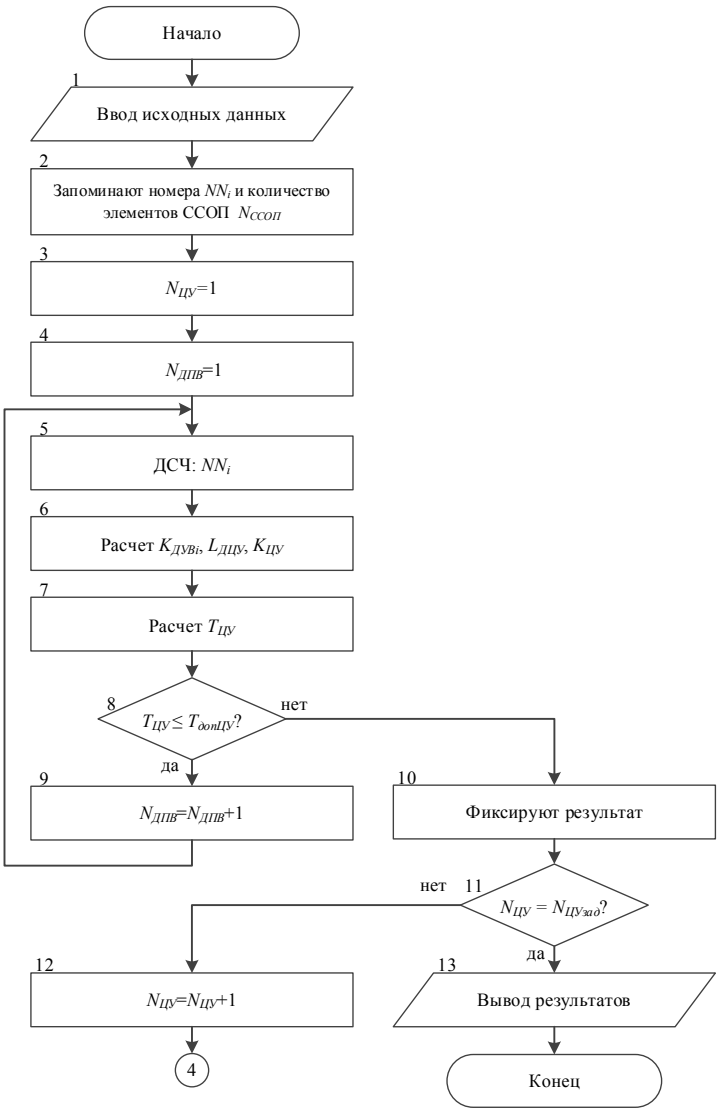

***Рис. 4**. Схема алгоритма оценки управляемости заданного фрагмента ССОП*

Для оценки предложен новый обобщенный показатель: коэффициент децентрализации управления ($K_{ДУ}$). Кроме того, введены частные показатели: доля функций i-го центра управления реализующих деструктивные управляющие воздействия ($K_i^{ДУВ}$); среднее время цикла управления ($\overline{T}_{ЦУ}$).

Критерием оценки управляемости фрагмента ССОП является значение среднего времени продолжительности цикла управления, которое должно быть не больше требуемого $\overline{T}_{ЦУ} \le \overline{T}_{доп.ЦУ}$.

Выходными результатами методики являются: среднее время цикла управления ($\overline{T}_{ЦУ}$) с учетом множественности легитимных и нелегитимных центров управления удовлетворяющее требуемым значениям.

Оценка управляемости фрагмента сети связи общего пользования с учетом влияния множественности центров управления и деструктивных программных воздействий

Обобщенная схема методики оценки управляемости фрагмента сети связи общего пользования с учетом влияния множественности центров управления и ДПВ представлена в виде алгоритма и заключается в следующей последовательности действий (рис.4).

В блоке 1 осуществляют ввод исходных данных.

В блоке 2 запоминают номера (NN_i) и общее количество элементов ССОП, функционирующих в указанном фрагменте ($N_{ССОП}$).

В блоке 3 устанавливают счетчик операторов связи с независимыми центрами управления на фрагменте ССОП в начальное значение $N_{ЦУ}$=1.

В блоке 4 устанавливают счетчик количества элементов фрагмента ССОП подверженных ДПВ злоумышленника в начальное значение $N_{ССОП}^{ДПВ}$=1

В блоке 5 случайным образом, с помощью датчика случайных чисел, генерируют по заданному закону распределения номер элемента фрагмента ССОП подверженного ДПВ.

В блоке 6 производится расчет весового коэффициента деструктивных управляющих воздействий параметрами i-го элемента фрагмента ССОП ($K_i^{ДУВ}$); количества деструктивных центров управления ($L_{ДЦУ}$); коэффициента децентрализации управления ($K_{ДУ}$) по формулам (3-5).

При управлении сетью связи базовыми показателями эффективности функционирования сети являются пропускная способность, своевременность, достоверность и безопасность [11]. Известно, что изменение любой характеристики (параметра) сложной системы приводит к разноуровнему изменению всех показателей, характеризующих основные свойства системы [12, 13].

Исходя из этого, в условиях динамичности состояний ССОП вследствие постоянного и независимого изменения состава, структуры операторами связи, перепадов неконтролируемой информационной нагрузки от множества обслуживаемых абонентов можно предположить, что с увеличением в каком-либо регионе числа операторов со своими центрами управления, время квазистационарного состояния указанного фрагмента сети будет экспоненциально уменьшаться, что однозначно повлечет за собой ухудшение базовых показателей ее функционирования.

Для оценки ситуации, характеризующейся множественностью центров управления и динамическим изменением их количества, используется новый показатель, а именно коэффициент децентрализации управления ($K_{ДУ}$), который позволяет оценить качество функционирования сети связи по базовым показателям.

Коэффициент децентрализации управления отражает зависимость качества функционирования сети связи от количества центров управления и их управляющих воздействий на объекты управления (элементы сети).

Коэффициент децентрализации управления рассчитывается по формуле:

$$K_{ДУ} = 1 - e^{-\frac{N_{ЦУ}}{N_{ССОП}}}, \quad (1)$$

где $N_{ЦУ}$ – количество центров управления в сети связи; $N_{ССОП}$ – количество объектов управления в сети связи.

В случае увеличения центров управления, длительность цикла управления будет определяться:

$$\overline{T}_{ЦУ} = \overline{T}_{исхЦУ} + K_{ДУ}\overline{T}_{исх.ЦУ}, \quad (2)$$

где $\overline{T}_{исхЦУ}$ – среднее время цикла управления сбалансированной системы управления.

Под сбалансированной системой управления в идеальном случае, понимается система, для которой коэффициент децентрализации $K_{ДУ}$ =0. На практике система при $N_{ЦУ}$=1 и $N_{ССОП}$=30, характеризуется $K_{ДУ}$=0,03.

Таким образом с увеличением на фрагменте ССОП количества сетей с независимыми центрами управления, длительность цикла управления будет увеличиваться $T_{ЦУ} \to \max$.

В условиях деструктивных управляющих воздействий коэффициент децентрализации управления рассчитывается по формуле:

$$K_{ДУ} = 1 - e^{-\frac{N_{ЦУ}+L_{ДЦУ}}{N_{ССОП}}}, \quad (3)$$

где $N_{ЦУ}$ – количество легитимных центров управления на фрагменте ССОП; $L_{ДЦУ}$ – условное количество деструктивных центров управления; $N_{ССОП}$ – общее количество элементов ССОП, функционирующих в указанном фрагменте.

При этом учитывается фактор деструктивных управляющих воздействий злоумышленника, потенциально имеющего возможность удаленного управления как всей сетью, так и частью элементов сети или частью параметров управления элемента.

Условное количество деструктивных центров управления рассчитывается по формуле:

$$L_{ДЦУ} = \sum_{i=1}^{N_{ССОП}^{ДПВ}} K_i^{ДУВ}, \quad (4)$$

где $K_i^{ДУВ}$ – доля функций *i*-го центра управления реализующих деструктивные управляющие воздействия.

$$K_i^{ДУВ} = \frac{R_i^{ДПВ}}{R_i^{УП}}, \quad (5)$$

где $R_i^{ДПВ}$ – количество параметров управления *i*-го элемента фрагмента ССОП подверженных ДПВ; $R_i^{УП}$ – общее количество параметров управления *i*-го элемента фрагмента ССОП.

В блоке 7 производится расчет длительности цикла управления заданной системой управления фрагмента ССОП по формуле (2).

В блоке 8 проверяют на выполнение требования по допустимой длительнос ти цикла управления $T_{ЦУ} \le T_{доп.ЦУ}$.

Если условие выполняется, то управление передается блоку 9, в котором увеличивают на 1 значение счетчика количества элементов фрагмента ССОП подверженных ДПВ и далее в цикле управление передается блоку 5.

Если условие не выполняется, то управление передается блоку 10, в котором фиксируют значение коэффициента децентрализации управления ($K_{ДУ}$).

В блоке 11 проверяют достигло ли количество операторов связи с независимыми центрами управления заданного.

Если условие не выполняется, то управление передается блоку 12, в котором увеличивают значение счетчика количества операторов связи с независимыми центрами управления на 1 и далее в цикле управление передается блоку 4.

Если условие выполняется, то результат запоминают и алгоритм заканчивает работу.

Таким образом в работе предложена методика оценки управляемости фрагмента ССОП с учетом влияния множественности центров управления и деструктивных программных воздействий. На основании выходных данных предложенной методики делают вывод при каком количестве центров управления длительность цикла управления будет соответствовать требуемым значениям.

Выводы

Научная новизна разработанной методики заключается в одновременном учете влияния множественности центров управления и деструктивных программных воздействий на качество функционирования системы управления сети связи. Методика позволяет получать зависимости длительности цикла управления системой связи от количества разнородных центров управления и их управляющих воздействий на элементы сети.

Разработанное научно-методическое обеспечение предназначено для научно-исследовательских организаций и ведомств с целью обоснования политики развития, разработки и модернизации систем управления.

Представленное научно-методическое обеспечение является основой для разработки подходов и научно-технических предложений по оценке степени защищенности систем управления сетями от ДПВ, выявлению слабых мест в существующих сетях, по управлению и модернизации сети связи, при планировании развёртывания и эксплуатации сети связи.

***Рецензент**: Цирлов Валентин Леонидович, кандидат технических наук, доцент МГТУ им. Н.Э. Баумана. E-mail: v.tsirlov@cnpo.ru*

Литература:

1. Семенов Ю.В. Проектирование сетей связи следующего поколения. СПб.: Наука и Техника, 2005. 240 с.: ил.
2. Тепляков И.М. Основы построения телекоммуникационных систем и сетей. М.: Радио и связь, 2004. 328 с.
3. Стародубцев Ю.И., Федоров В.Г. Способ обнаружения источника сетевых атак на автоматизированные системы // Проблемы экономики и управления в торговле и промышленности, 2016. № 1. с. 87-92.
4. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. СПб.: Питер, 2010. 944с.
5. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий/Под. ред. А.С.Маркова. М.: ДМК Пресс, 2017. 224 с.

6. Ермишян А.Г. Теоретические основы построения систем военной связи в объединениях и соединениях. Учебник. Часть 1. Методологические основы построения организационно-технических систем военной связи. Санкт-Петербург: Военная академия связи, 2005. 740 с.
7. Дымарский Я.С. Управление сетями связи: принципы, протоколы, прикладные задачи / Я.С. Дымарский и др.; под ред. Г.Г. Яновского. М.: ИТЦ Мобильные коммуникации, 2003. 384 с.
8. Федоров В.Г., Стародубцев Ю.И., Репников А.Ю. Задача разработки модели сети связи общего пользования, включающей двух и более операторов, как ресурса, используемого в интересах заданной системы управления // Региональная информатика и информационная безопасность. Сборник трудов. Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления. 2016. С. 64-66.
9. Стародубцев Ю.И., Федоров В.Г. Способ адаптивной защиты выделенных сетей торгового объекта от воздействия деструктивного трафика сложной структуры // Проблемы экономики и управления в торговле и промышленности. 2015. № 3 (11). С. 57-62.
10. Липатников В.А., Стародубцев Ю.И. Защита информации. СПб.: ВУС, 2001. 348 с.
11. Рейман Л.Д., Варакин Л.Е. Перспективные телекоммуникационные технологии. Потенциальные возможности. М.: МАС, 2001. 256 с.
12. Стародубцев Ю.И., Сухорукова Е.В., Федоров В.Г. Проблема оценки защищенности информационно-телекоммуникационных систем // XIV Санкт-Петербургская международная конференция «Региональная информатика (РИ-2014)». Санкт-Петербург, 29-31 октября 2014 г.: Материалы конференции. 2014. С. 102-103.
13. Стародубцев Ю.И., Бегаев А.Н., Давлятова М.А. Управление качеством информационных услуг. СПб.: Изд-во Политехн. ун-та, 2017. 454 с.

THE METHOD OF ASSESSING THE CONTROLLABILITY OF A FRAGMENT OF THE COMMUNICATION NETWORK OF GENERAL USE TAKING INTO ACCOUNT THE INFLUENCE OF MULTIPLE CENTERS OF CONTROL AND DESTRUCTIVE SOFTWARE IMPACTS

Begaev A.N.[4], Starodubtsev Y.I.[5], Fedorov V.G[6]

Currently, the deployment of information and telecommunication systems for the process data exchange between geographically distributed departments is carried out in close cooperation with the communications network for common use, which feature is its mnogopartiinosti with an appropriate number of control centers. Factor of a plurality of control centers entails an increase in cycle control network. In the operation of integrated networks, the conditions for the exercise of destructive software effects. This means that the conditions of decentralized management network operators added another factor to destructive control actions of the attacker, potentially having the ability to remotely control a network element in the part concerning. As a result of the change management cycle network. A technique is developed to determine the degree of influence of the plurality of control centers to control network and to assess the protective properties of the specified part of the network from the destructive software effects. Using techniques to solve the problem of identification of network elements in respect of which it is necessary to implement protective measures against destructive software impacts to preserve a given mode of network management.

Keywords*: control system, many operators, destructive control actions.*

References:

1. Semenov Yu.V. Proektirovanie setey svyazi sleduyushchego pokoleniya. Spb.: Nauka i Tekhnika, 2005. 240 P.: il.
2. Teplyakov I.M. Osnovy postroeniya telekommunikatsionnykh sistem i setey. M.: Radio i svyaz', 2004. 328 P.

4 Alexey Begaev, Ph.D., CJSC «North-West Echelon», Saint-Petersburg, a.begaev@nwechelon.ru

5 Yuriy Starodubtsev, Dr.Sc., Professor, Federal State Public Educational Institution of Higher Professional Education Military Telecommunication Academy named after the Soviet Union Marshal Budienny S. M., Saint-Petersburg, ys@e-nw.ru

6 Vadim Fedorov, Federal State Public Educational Institution of Higher Professional Education Military Telecommunication Academy named after the Soviet Union Marshal Budienny S. M., Saint-Petersburg, vadim.fedorov.53@mail.ru.

3. Starodubtsev Yu.I., Fedorov V.G. Sposob obnaruzheniya istochnika setevykh atak na avtomatizirovannye sistemy, Problemy ekonomiki i upravleniya v torgovle i promyshlennosti, 2016. No 1, pp. 87-92.
4. Olifer V. G., Olifer N. A. Komp'yuternye seti. Printsipy, tekhnologii, protokoly: Uchebnik dlya vuzov. 4-e izd. SPb.: Piter, 2010. 944 P.
5. Barabanov A.V., Dorofeev A.V., Markov A.S., Cirlov V.L. Sem' bezopasnyh informacionnyh tekhnologij/Pod. red. A.S.Markova. M.: DMK Press, 2017. 224 s.
6. Ermishyan A.G. Teoreticheskie osnovy postroeniya sistem voennoy svyazi v ob"edineniyakh i soedineniyakh. Uchebnik. Chast' 1. Metodologicheskie osnovy postroeniya organizatsionno-tekhnicheskikh sistem voennoy svyazi. Sankt-Peterburg: Voennaya akademiya svyazi, 2005. 740 P.
7. Dymarskiy Ya.S. Upravlenie setyami svyazi: printsipy, protokoly, prikladnye zadachi / Ya.S. Dymarskiy i dr.; pod red. G.G. Yanovskogo. M.: ITTs Mobil'nye kommunikatsii, 2003. 384 P.
8. Fedorov V.G., Starodubtsev Yu.I., Repnikov A.Yu. Zadacha razrabotki modeli seti svyazi obshchego pol'zovaniya, vklyuchayushchey dvukh i bolee operatorov, kak resursa, ispol'zuemogo v interesakh zadannoy sistemy upravleniya, Regional'naya informatika i informatsionnaya bezopasnost'. Sbornik trudov. Sankt-Peterburgskoe obshchestvo informatiki, vychislitel'noy tekhniki, sistem svyazi i upravleniya. 2016, pp. 64-66.
9. Starodubtsev Yu.I., Fedorov V.G. Sposob adaptivnoy zashchity vydelennykh setey torgovogo ob"ekta ot vozdeystviya destruktivnogo trafika slozhnoy struktury, Problemy ekonomiki i upravleniya v torgovle i promyshlennosti. 2015. № 3 (11), pp. 57-62.
10. Lipatnikov V.A., Starodubtsev Yu.I. Zashchita informatsii. SPb.: VUS, 2001. 348 s.
11. Reyman L.D., Varakin L.E. Perspektivnye telekommunikatsionnye tekhnologii. Potentsial'nye vozmozhnosti. M.: MAS, 2001. 256 P.
12. Starodubtsev Yu.I., Sukhorukova E.V., Fedorov V.G. Problema otsenki zashchishchennosti informatsionno-telekommunikatsionnykh system, XIV Sankt-Peterburgskaya mezhdunarodnaya konferentsiya «Regional'naya informatika (RI-2014)». Sankt-Peterburg, 29-31 oktyabrya 2014 g.: Materialy konferentsii. 2014, pp. 102-103.
13. Starodubtsev Yu.I., Begaev A.N., Davlyatova M.A. Upravlenie kachestvom informatsionnykh uslug. SPb.: Izd-vo Politekhn. un-ta, 2017. 454 P.