9. Building an Information Risk Management Toolkit [Электронный ресурс]. – Режим доступа: https://www.coursera.org/course/inforisk

10. Designing and Executing Information Security Strategies [Электронный ресурс]. – Режим доступа: https://www.coursera.org/course/infosec

С.П. Горелик, В.С. Шумилин

ЗАЩИТА СЕТЕЙ СВЯЗИ В УСЛОВИЯХ ПРОГРАММНЫХ ВОЗДЕЙСТВИЙ

(Академия ФСО России, г. Орел)

С развитием информационных и телекоммуникационных технологий, становится актуальным процесс развития сетей связи, путем цифровизации и интеграции их в общемировое телекоммуникационное пространство, что в свою очередь, существенно увеличивает возможности нарушителей по идентификации, вскрытию и воздействию на их элементы.

Анализ элементов сети связи осуществляется нарушителем посредством ведения несанкционированного мониторинга (рисунок 1).

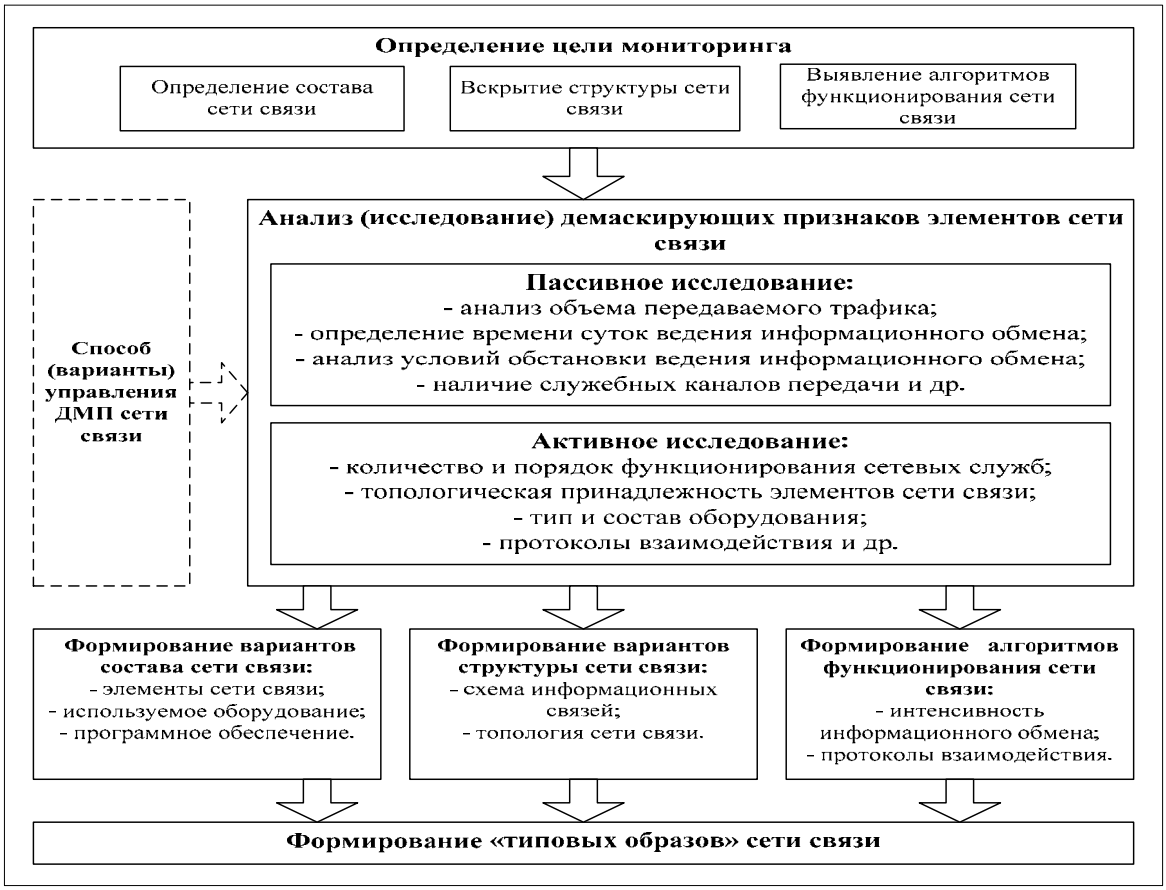

Рис. 1. Обобщенный порядок проведения несанкционированного мониторинга элементов сети связи (вариант)

Из рисунка 1 видно, что процесс ведения несанкционированного мониторинга элементов сети связи осуществляется поэтапно. Сначала определяются цели мониторинга (необходимость определения состава сети связи, вскрытие структуры сети связи либо выявление алгоритмов функционирования сети связи). Далее анализируются (исследуются) демаскирующие признаки (ДМП) элементов сети связи и процессов их функционирования. Процесс анализа демаскирующих признаков элементов сети связи реализуется двумя подсистемами: активной и пассивной [1].

Пассивное исследование осуществляет сбор типовых демаскирующих признаков элементов сети связи. К типовым демаскирующим признакам элементов сети связи относятся: форма огибающей сигнала; спектр сигналов; вид излучения, вид модулирующего сигнала; значения параметров сигнала; мощность излучения; количество излучаемых фиксированных частот, взаимные удаления элементов, площадь размещения элементов и др. [2].

Активное исследование предполагает использование комплексных программных воздействий, наиболее часто реализуемыми из которых являются: анализ сетевого трафика, сканирование сети, отказ в обслуживании и др. После анализа демаскирующих признаков переходят к формированию множества вариантов сетей связи, которое включает в себя отображение параметров по демаскирующим признакам, их обобщение и интеллектуальный анализ, что позволяет сформировать «типовые образы» сети связи, отражающие ее функциональные особенности [3].

Анализ существующих средств и методов защиты позволил определить, что демаскирующие признаки элементов сети связи, выявляемые активным исследованием, могут быть скрыты методами разграничения доступа и криптографического закрытия семантической составляющей информационного обмена [4, 5]. Однако существующие методы защиты не всегда учитывают особенности изменения параметров демаскирующих признаков и не имеют возможности управления данными параметрами в зависимости от характера воздействий со стороны злоумышленника. В связи с этим возникает необходимость разработки научно-технических предложений, позволяющих осуществлять формирование защищенной сети связи, путем управления (ослабления, устранения) ее демаскирующими признаками. В качестве предложения по защите разработан способ управления демаскирующими признаками сети связи [6]. Обобщенная схема, поясняющая способ управления демаскирующими признаками сети связи представлена на рисунке 2.

Суть способа заключается в варьировании значениями управляемых демаскирующих признаков по соответствующим правилам и в заданных пределах, в результате чего, злоумышленник вводится в заблуждение относительно структуры сети связи и параметров её функционирования,что приводит к повышению устойчивости сети связи в условиях деструктивных программных воздействий. В качестве исходных данных задают множество контролируемых параметров демаскирующих признаков сети связи.

В результате измерения значений данных контролируемых параметров, в ходе выполнения цикла анализа, формируют группы контролируемых параметров демаскирующих признаков и задают коэффициенты важности для каждой группы. Дополнительно определяется количество управляемых и неуправляемых демаскирующих признаков. Перед развертыванием, разрабатываются варианты ложного функционирования сети связи.

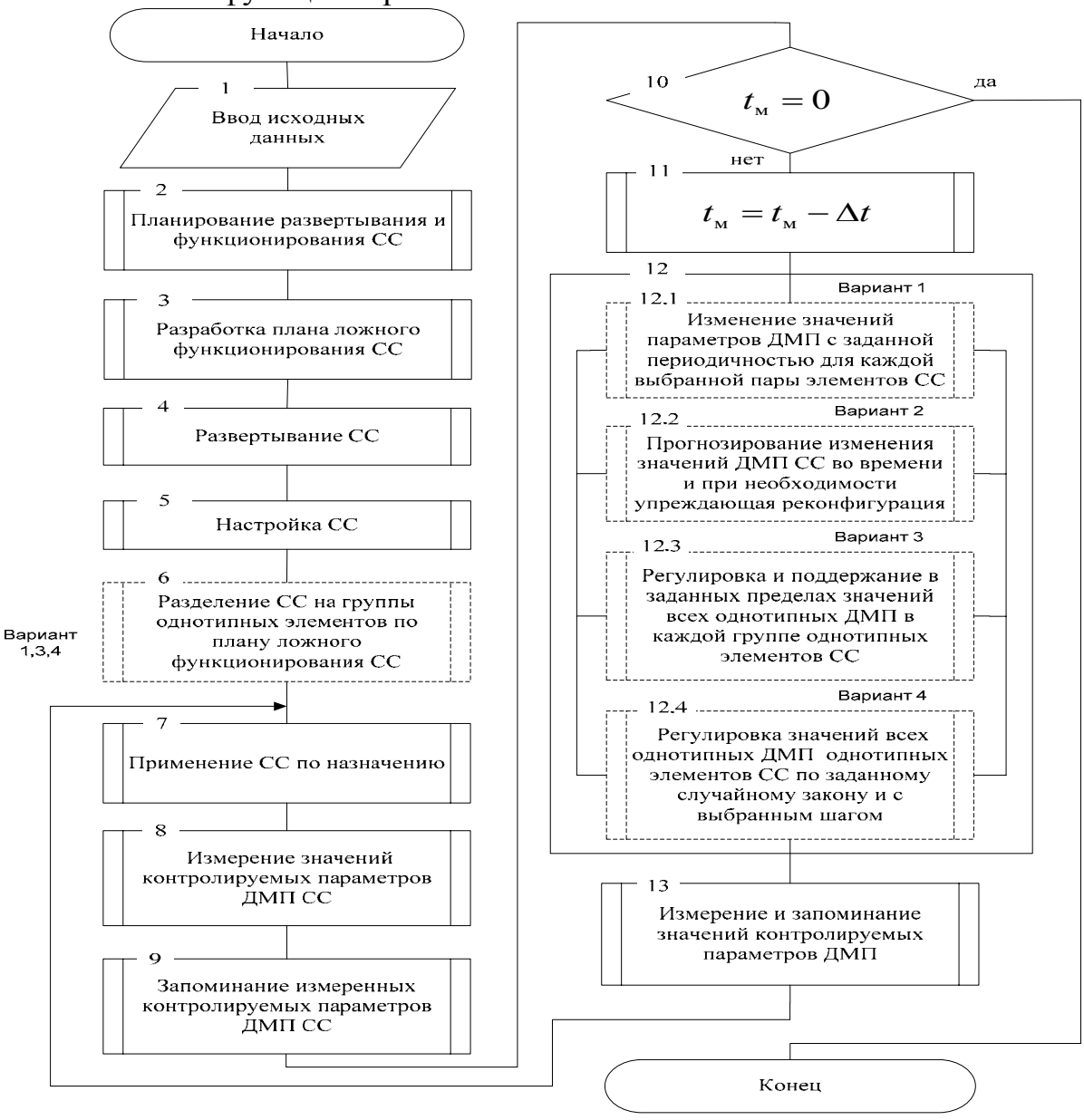

Рис. 2. Обобщенная схема способа управления демаскирующими признаками сети связи

После этого осуществляют развертывание сети связи, настраивают основные параметры и применяют ее по назначению. На функционирующей сети связи производят измерение значений контролируемых параметров демаскирующих признаков и запоминают их с целью дальнейшего использования.

Способ предполагает управление защищенностью сетей связи по

нескольким направлениям.

В первом варианте злоумышленник вводится в заблуждение относительно структуры сети связи и ее параметров за счет периодического (по необходимости корректируемого) взаимного изменения демаскирующих признаков на выбранных парах элементов сети связи.

Во втором варианте злоумышленник вводится в заблуждение относительно структуры сети связи и ее параметров на основе прогнозирования значений показателей демаскирующих признаков и, при необходимости, упреждающей реконфигурации сети связи.

В третьем варианте заявленного способа злоумышленник вводится в заблуждение относительно структуры сети связи и ее параметров за счет принудительной регулировки (с заданной периодичностью) и поддержания в установленных пределах на однотипных элементах сети связи значений всех однотипных признаков.

В четвертом варианте злоумышленник вводится в заблуждение относительно структуры сети связи и ее параметров за счет одновременного изменения всех однотипных параметров демаскирующих признаков в каждой группе всех однотипных элементов сети связи по заданному случайному закону и шагу с заданным периодом так, чтобы параметры демаскирующих признаков элементов сети связи попали в заданный интервал значений.

Таким образом, использование способа управления демаскирующими признаками сети связи, с возможностью корректировки значений управляемых демаскирующих признаков ее элементов в заданных значениях и упреждающей реконфигурации, позволяет снизить эффективность ведения несанкционированного мониторинга элементов сети связи. Кроме того, полученные результаты могут использоваться при проведении исследований по разработке методов и способов защиты сетей связи в условиях внешних деструктивных программных воздействий, а также при проэктировании систем защиты сетей связи в рамках определения защитного ресурса.

Литература

1. Зима В. М., Молдовян А. А., Молдовян Н. А. Безопасность глобальных сетевых технологий. СПб.: БХВ - Петербург, 2003. – 368 с: ил.

2. Меньшаков Ю. К. Защита объектов и информации от технических средств разведки. – М. : Российск. гос. гуманит. ун-т, 2002. – 399 с.

3. Петренко С. А. Методы информационно-технического воздействия на киберсистемы и возможные способы противодействия. – Труды ИСА РАН, том 41, 2009., 104-146 с.

4. Пат. 2419153 Российская федерация, МПК G06N 5/00. Способ контроля демаскирующих признаков системы связи / Е. В. Гречишников [и др.] ; заявитель и патентообладатель Академия ФСО России. – № 2009125131/08 ; заявл. 30.06.09 ; опубл. 20.05.11, Бюл. № 1. – 22 с. : ил.

5. Пат. 2422892 Российская федерация, МПК G06F 21/20. Способ защиты вычислительной сети / Е. В. Гречишников [и др.] ; заявитель и

патентообладатель Академия ФСО России. – № 2010114785/08 ; заявл. 13.04.10; опубл. 27.06.11, Бюл № 18 – 9 с. : ил.

6. Пат. 2450337 Российская федерация, МПК G06F 15/00. Способ (варианты) управления демаскирующими признаками системы связи / Е. В. Гречишников [и др.] ; заявитель и патентообладатель Академия ФСО России. – № 2011117814/08 ; заявл. 03.05.11 ; опубл. 10.05.12, Бюл. № 13. – 19 с. : ил.

Д.В. Кириллов

ПРОБЛЕМЫ АВТОМАТИЗАЦИИ УПРАВЛЕНИЯ КОНТРОЛЕМ ДОСТУПА НА ОСНОВЕ РОЛЕЙ

(Самарский государственный университет)

Для достижения цели автоматизации управления контролем доступа на основе ролей в автоматизированных системах управления предприятием (АСУП) необходимо решить задачу замыкания компонентов и отношений подсистемы реализующей политику безопасности (ПБ) и объектов и отношений уровня бизнес-логики системы (БЛ), содержащей достаточно большой объем данных о субъектах необходимых для принятия решений о назначений или отзыве полномочий, либо для выполнения других операций [1].

В простейшем случае, когда в организации используется только одна система, и управление доступом реализуется в ней же, задача с формальной точки зрения является тривиальной - необходимо обогатить систему недостающими компонентами и отношениями [2]. Простая модель данных характерная для систем, использующих ролевую политику безопасности представлена на рисунке 1.

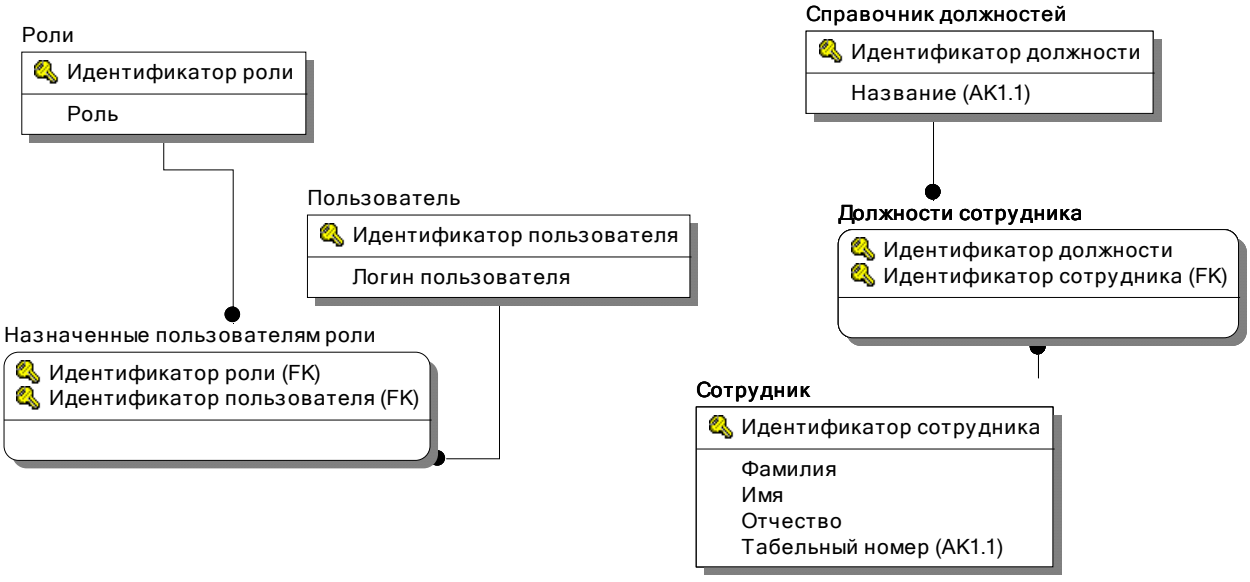

Рис. 1. Простейшая модель данных некоторых компонентов и отношений подсистемы разграничения данных
и соответствующих им объектов уровня бизнес-логики