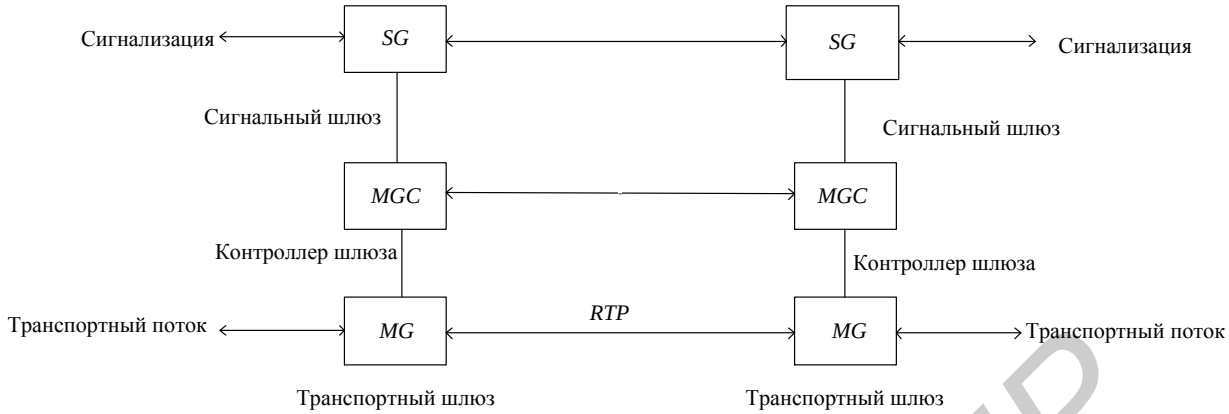

Рисунок 1 – Структурная схема конвертора

Список использованных источников:

[1] Безопасность компьютерных сетей на основе: П. Б. Боккер . – Москва, 1991. – 304 с.

[2] Лукацкий, А. В. Обнаружение атак / А. В. Лукацкий. – СПб. : БХВ-Петербург, 2003. – 608 с.

[3] Высокопроизводительные сети. Энциклопедия пользователя : М. А. Спортак [и др.]. – Диа Софт, 1998. – 432 с.

[4] Руденков, Н. А. Основы сетевых технологий : учеб. пособие / Н. А. Руденков, Л. И. Долинер – Екатеренбург : УрФУ, 2011. – 297 с.

[5] Хорев, *П. Б.* Программно-аппаратная защита информации : учеб. пособие. / П. Б. Хорев – М. : ФОРУМ, 2009. – 351 с.

[6] Мазиков, К. И. Анализ современных сертифицированных средств обнаружения вторжений в информационных сетях / К. И. Мазиков // Вестник ТГУ, т. 19, вып. 2. – 2014. С 661–662.

СИСТЕМА ОБНАРУЖЕНИЯ АНОМАЛИЙ В СЕТИ СВЯЗИ ДОСТУПА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Кухарев В.В.

Утин Л.Л. – к.т.н.

На современном этапе развития ВС РБ наблюдается резкое обострение проблем обеспечения информационной безопасности. Все более обостряются проблемы в обеспечении требуемого уровня защищенности информации, как циркулирующей в автоматизированных системах управления, связи, информационных вычислительных сетей (ИВС), локальных вычислительных сетях (ЛВС) военного назначения. Данные проблемы связаны с одной стороны в обеспечении требуемого уровня безопасности информации, а с другой бурным развитием и широким внедрением во все сферы деятельности, в том числе и в военную, информационных технологий и различного программного обеспечения, всеобщей цифровизацией, вхождением закрытых ведомственных информационных вычислительных сетей в сети общего пользования, активизацией деятельности всех видов разведок противника, в том числе компьютерной.

Как в мирное время, так и в условиях боевых действий наиболее важную роль для армий иностранных государств имеет достоверная разведывательная информация, получаемая по различным каналам. В этих условиях закономерным является его стремление обеспечить получение достоверной информации о системе управления войсками (связью) в том числе по открытым каналам связи и через сети общего пользования. Немаловажную роль в утечке, разглашении секретной информации играет также и внутренний нарушитель безопасности информации – легальный пользователь, администратор АС (ЛВС), зачастую наделенный неограниченными привилегированными правами, который как непреднамеренно, так и преднамеренно может допускать нарушение безопасности информации, циркулирующей в сетях связи военного назначения.

Состояния дел в области защиты информации, показывает, что возможности традиционных средств и способов защиты информации в сетях связи доступа не могут в полной мере обеспечить секретность, доступность и целостность информации в процессе ее обработки, хранения и передачи по сетям связи военного назначения.

Поэтому возникает необходимость повышения эффективности защищенности сетей связи военного назначения. Одной из важнейших подсистем системы защиты информации является система обнаружения аномалий, предназначенная для обнаружения и анализа возможных попыток осуществления несанкционированного доступа и воздействий на информацию, конфиденциальности и интегральной целостности "критических" информационных структур.

В связи с этим, актуальным является решение задачи: разработки подсистемы мониторинга информационного трафика сетей связи доступа военного назначения.

Целью данной работы является совершенствование системы защиты сетей связи, создание защитных барьеров (препятствий) от любого несанкционированного доступа в процесс функционирования системы, а также

попыток хищения, модификации, ознакомления, изменения информации, разрушения и выведения из строя структурно-функциональных элементов и узлов оборудования, специального программного обеспечения, данных и носителей информации.

Список использованных источников:
1. Олифер В.Г., Олифер Н.А. Безопасность компьютерных сетей. 2015. – 500с.
2. Куклачев П.В. Аппаратно-программные средства и методы защиты информации. Владивосток, 2007. – 356с.
3. Увалов К.С. Основы организации адаптивных систем защиты информации. Москва, 2009. – 332с.

ЧИСЛЕННОЕ ОПРЕДЕЛЕНИЕ РИСКОВ БЕЗОПАСНОСТИ СВЯЗИ ДЛЯ ЭЛЕМЕНТА ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Макатерчик А.В.

Маликов В.В – к.т.н., доцент

В настоящее время значительно возрастает роль современных инфокоммуникационных систем специального назначения (ИКС СН). Развитие и совершенствование таких систем ведется в соответствии с общемировыми тенденциями.

Активное внедрение новых средств связи, протоколов и инфокоммуникационных технологий привело к появлению неизученных угроз безопасности связи, возможность реализации которых злоумышленниками негативно влияет на обеспечение информационной безопасности государства и организаций различных форм собственности.

Под угрозой безопасности связи будем понимать совокупность условий и факторов, создающих потенциальную или реально существующую опасность нанесения ущерба системе связи или ее компонентам.

Выделяют следующие виды возможных атак на ИКС СН: пассивная, активная (отказ в обслуживании, модификация потока, создание ложного потока, повторное использование). При этом реализация атаки на ИКС СН включает следующие этапы: сбор информации, выбор метода реализации и типа атаки, реализация выбранного типа атаки, завершение атаки.

На основе проведенного анализа реализации угроз информационной безопасности численное определение рисков безопасности связи для элемента ИКС СН предлагается определять по формуле:

$$R = \frac{\sum_{i=1}^{I}\sum_{j=1}^{J}\sum_{n=1}^{N}(P_i \cdot U_i)\cdot(D_{ij}\cdot V_{ij})\cdot(1-K_{in})}{\sum_{j=1}^{J}\sum_{i=1}^{I}\sum_{n=1}^{N}U_i \cdot V_{ij}}$$

где R – численная величина риска безопасности связи;
I – количество угроз;
J – количество уязвимостей;
N – количество мер по обеспечению безопасности связи;
Pi – весовой коэффициент реализации потенциальной угрозы;
Ui – возможность реализации потенциальной угрозы;
Dij – весовой коэффициент потенциальной уязвимости;
Vij – возможность реализации потенциальной уязвимости;
Kin – возможность нейтрализации угрозы посредством меры по обеспечению безопасности связи.

$$\begin{cases} U_i = \begin{cases} 1 & \text{, если угроза может быть применена к элементу;} \\ 0 & \text{, в противном случае.} \end{cases} \\ V_{ij} = \begin{cases} 1 & \text{, если i-я угроза может быть применена через j-ю уязвимость;} \\ 0 & \text{, в противном случае.} \end{cases} \end{cases}$$

Ограничение условий: