УДК 654.026

К.Л. Воронков, М.Ю. Шерстюк

СРЕДСТВА КОНТРОЛЯ ФУНКЦИОНИРОВАНИЯ И ЗАЩИЩЕННОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Воронков Кирилл Львович, *специалист в области АСУС, окончил Российский государственный гидрометеорологический институт, факультет океанологии, заочную аспирантуру при Санкт-Петербургском институте информатики и автоматизации Российской академии наук (СПИИРАН). Ведущий специалист ЗАО «Институт инфотелекоммуникаций». Автор ряда статей и учебных пособий в области информационных технологий. [e-mail: vkl@iitc.ru].*

Шерстюк Максим Юрьевич, *специалист АСОИУ, окончил факультет компьютерных технологий и информатики Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. Ульянова (Ленина). Инженер-программист ЗАО «Институт инфотелекоммуникаций». Опубликовал ряд статей в области информационных технологий. [e-mail: viking@iitc.ru].*

Аннотация

В статье описан аналитический подход к решению проблемы противодействия компьютерным атакам на программное обеспечение, функционирующее на телекоммуникационных средствах в рамках сетей связи специального назначения.

Ключевые слова: программная атака, сеть связи, противодействие, анализ данных.

Противоборство государств в области информационных технологий, стремление криминальных структур противоправно использовать информационные ресурсы, необходимость обеспечения прав граждан в информационной сфере, наличие множества случайных угроз вызывают острую необходимость обеспечения защиты информации в телекоммуникационных сетях (ТКС) специального назначения, обеспечения устойчивого управления такими сетями в условиях программных воздействий (атак).

Так, например, в [1] прямо предполагается проведение информационных операций (включая программные атаки (ПА)), в том числе наступательного характера, объектами которых выступают как гражданские ТКС, так и системы связи и боевого управления и иные элементы военной инфраструктуры. Целью таких атак является достижение информационного превосходства [2].

Таким образом, ТКС и их сетевые элементы (СЭ) – коммутаторы, маршрутизаторы, мультиплексоры и т. д. – могут быть такими же объектами ПА, как серверы и рабочие станции вычислительных сетей. Фактически любой СЭ ТКС, имеющий в своем составе вычислительную среду с выполняемым в ней программным обе-

спечением (ПО) и с возможностью сетевого доступа к ней, потенциально является объектом ПА. Осуществление ПА на ТКС – один из эффективных способов достижения информационного превосходства, в результате которого наступает парализация систем связи, а как следствие этого, нарушение управления войсками.

Характерными особенностями ТКС является их иерархичность (технологическая, организационная, территориальная), разнородность, интегральность использования достижений современной микропроцессорной техники. Данные особенности позволяют решать потенциально не ограниченный круг задач в части построения прикладных служб и сервисов в интересах конкретных пользователей. К таким задачам можно отнести создание службы электронной почты, службы обмена сообщениями, веб-сервисов, службы удаленных конференций и др.

Для обеспечения постоянного и непрерывного функционирования ТКС специального назначения и предоставления услуг связи требуемого качества в любой обстановке, в том числе и при проведении войсковых операций и, как следствие, функционирования в условиях проведения ПА, необходимо осуществлять комплекс мероприятий по обеспечению информационной безопасности ТКС. В силу этого требуется обеспечить противодействие возможным ПА и контроль защищенности как собственно ТКС специального назначения, так и автоматизированной системы управления связью (АСУС) данной системы [3, 4, 5].

С учетом особенности ТКС необходимо создание распределенной сетевой системы защиты от компьютерных атак (СЗКА), обеспечивающей различные виды противодействия ПА и восстановление работоспособности ТКС и / или отдельных ее элементов. Основными видами противодействия ПА, которые будет обеспечивать СЗКА, являются противодействие по факту и превентивное противодействие (рис. 1).

Противодействие по факту включает в себя обнаружение текущей или состоявшейся (завершенной) компьютерной атаки и обеспечение противодействия атакующему. При этом противодействие может быть как активным, целью которого является прекращение ПА на свой объект, так и пассивным, заключающимся в изменении внутреннего состояния объекта таким образом, чтобы атака была невозможна или ее последствия были минимальными.

Превентивное противодействие сочетает в себе перспективное и ретроспективное противодействие. Перспективное противодействие заключается в поиске и устранении уязвимостей ПО средств вычислительной техники (СВТ) или средств телекоммуникаций (СТК).

Ретроспективное взаимодействие заключается в анализе ретроспективных данных об обнаруженных ПА, имевших место в ТКС, и анализ этих данных с целью предотвращения ПА.

Таким образом, и перспективное, и ретроспективное противодействие направлено на выработку рекомендаций об изменении внутреннего состояния потенциального объекта ПА, делающего невозможным реализацию характерных для данного объекта угроз. То есть данные виды противодействия являются элементами пассивного противодействия возможным атакам на элементы ТКС.

При рассмотрении противодействий ПА с позиций профилей управления не-

обходимо отметить, что при превентивном противодействии затрагивается в первую очередь система, обеспечивающая управление безопасностью и управление применением ТКС. Управление функционированием в данном случае обеспечивает реализацию мер, направленных на предотвращение возможных ПА. При противодействии по факту совершения компьютерной атаки основную роль играет система управления безопасностью и система управления функционированием, напрямую осуществляющие изменения состояния атакуемого объекта.

В силу вышеизложенного, для обеспечения информационной безопасности (ИБ) ТКС необходимо наличие сетевой автоматизированной службы (системы) защиты от ПА. Служба защиты от компьютерных атак должна обеспечивать пассивное противодействие проведению ПА на всех уровнях функционирования ТКС с использованием средств фактического, прогностического и ретроспективного противодействия ПА. Построение данной службы целесообразно осуществлять на основе программно-аппаратных комплексов, обеспечивающих контроль функционирования ТКС военного назначения (ВН) и отдельных ее элементов.

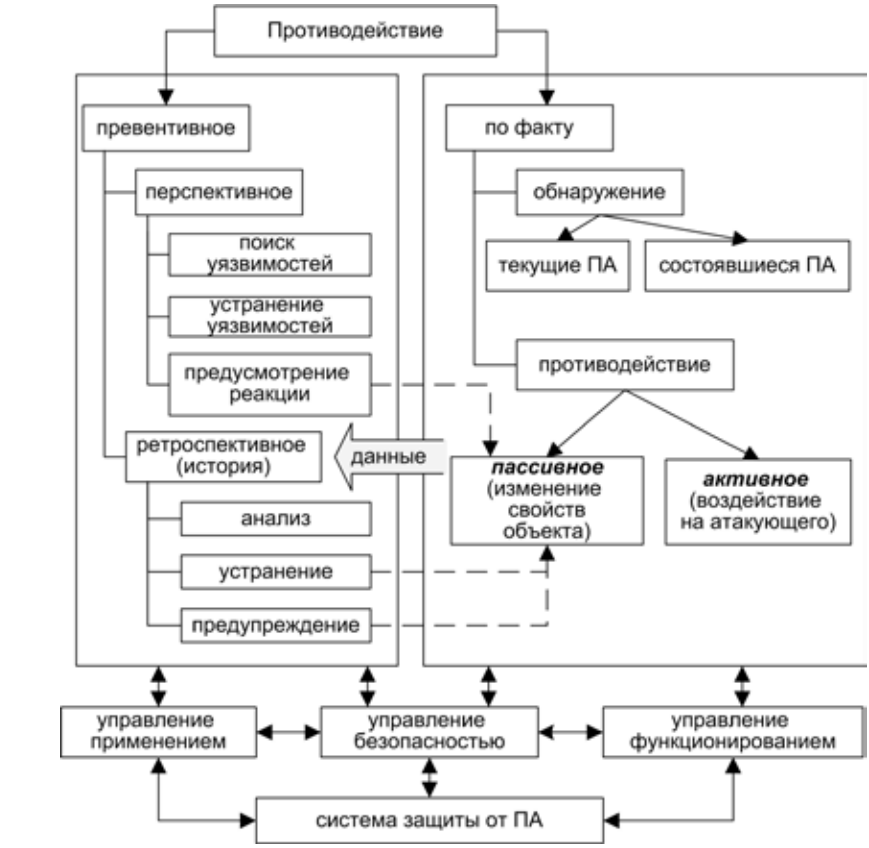

Рис. 1. Виды противодействия

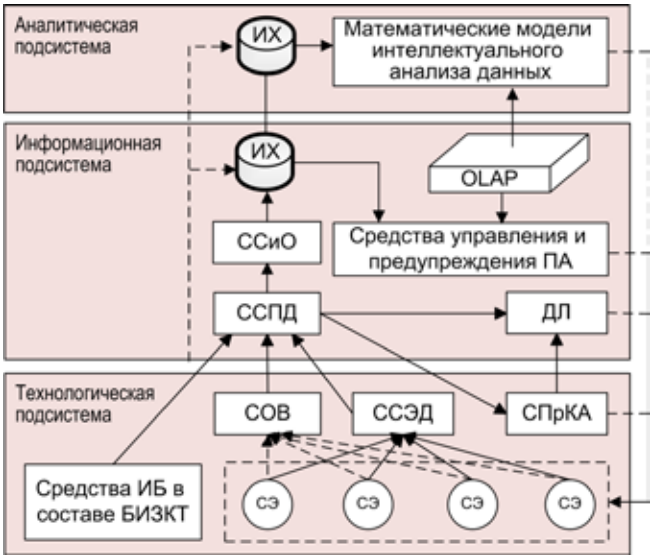

Рис. 2. Функциональные подсистемы

Наличие взаимодействующих комплексов контроля функционирования (ККФ), осуществляющих сбор, обработку и анализ данных, поступающих от элементов ТКС ВН, позволит получать оперативную и непротиворечивую картину состояния сети связи, а наличие средств распознавания ПА и механизмов поддержания эталонного состояния СТК и СВТ – предотвращать и / или минимизировать последствия ПА.

В рамках СЗКА должен функционировать и осуществлять информационное взаимодействие ряд функциональных подсистем, обеспечивающих решение соответствующего перечня задач (рис. 2).

К таким подсистемам следует отнести:

– технологическую подсистему, осуществляющую сбор первичных данных о состоянии СТК, СВТ и ПО, а также обнаружение атак по факту и пассивное противодействие ПА;

– информационную подсистему, в рамках которой осуществляется сбор и хранение данных, поступающих от технологической подсистемы, формирование информационного хранилища (ИХ) данных и проведение оперативного анализа состояния ТКС;

– аналитическую подсистему, оперирующую данными из ИХ и осуществляющую детальный анализ состояния ТКС с помощью различных математических моделей классификационного и прогностического характера.

На уровне технологической подсистемы осуществляется перманентный сбор и обработка информации средствами сбора первичных данных (ССПД). В качестве источников первичных данных могут выступать средства обнаружения вторжений (СОВ), средства сбора эксплуатационных данных (ССЭД) от СЭ, средства ИБ, входящие в состав базовых информационно защищенных компьютерных технологий (БИЗКТ). В случае обнаружения ПА соответствующие сигналы отправляются должностным лицам (ДЛ) узлов связи (УС) и средствам противодействия компьютерным атакам (СПрКА). СПрКА должны обеспечивать пассивное противодействие ПА в автоматическом режиме. ДЛ обеспечивают противодействие ПА с помощью средств управления инфотелекоммуникациями. Все полученные

первичные данные пересылаются информационной подсистеме, обрабатываются средствами сбора и обработки данных (ССиО), а затем заносятся в ИХ. Часть данных может поступать непосредственно в ИХ аналитической подсистемы. ИХ информационной подсистемы является основным источником данных для анализа и прогнозирования возможных и состоявшихся ПА. На его основе могут строиться различные выборки, а также многомерные массивы данных с использованием средств оперативной аналитической обработки (On-Line Analytical Processing (OLAP)). Аналитическая подсистема осуществляет интеллектуальный анализ данных с использованием реляционных и многомерных данных, поступающих от информационной системы. Задачами аналитической подсистемы являются обнаружение ранее не выявленных ПА и прогнозирование возможных атак на элементы ТКС.

ККФ, являющийся основой для построения СЗКА ТКС, должен представлять собой набор программных средств, позволяющих с максимальной оперативностью осуществлять контроль как за состоянием ТКС в целом, так и за отдельными ее компонентами [6, 7], такими как:

– телекоммуникационное оборудование;
– абонентские сети доступа;
– сети передачи данных;
– сетевые сервисы;
– оборудование операторов связи, предоставляющих арендуемые каналы связи;
– потребители услуг;
– системы мониторинга и управления телекоммуникационным оборудованием, сетями и услугами;
– собственные системы управления и сбора данных.

В ТКС с помощью ККФ должны защищаться и контролироваться следующие типы сетевой деятельности:

– управление: защита функций систем управления элементов сети, средств передачи данных, систем поддержки принятия решений и центра данных;
– контроль: защита эффективной передачи информации, сервисов и приложений по сети;
– доступ: доступ абонентов к сетевым ресурсам.

Для обеспечения полного контроля функционирования ТКС ВН необходима интеграция ККФ со всеми компонентами АСУС ТКС. Такая интеграция означает, что сведения о функционировании ТКС поступают со всех функциональных подсистем АСУС и помещаются в единое ИХ данных.

Целью функционирования ККФ ТКС является решение ряда задач, направленных на обеспечение устойчивости ТКС. К таким задачам можно отнести (рис. 3):

– предупреждение возможных ПА;
– обнаружение ПА на элементы ТКС или следов их сокрытия;
– противодействие осуществлению ПА;
– минимизация последствий ПА (восстановление работоспособности системы).

Таким образом, построение СЗКА на базе ККФ позволит повысить оперативную устойчивость функционирования ТКС ВН в условиях постоянного ведения

Рис. 3. Взаимосвязь функциональных задач ККФ

информационной борьбы, т. е. при наличии серьезных дестабилизирующих внешних факторов, влияющих на устойчивость функционирования сетей и систем передачи информации.

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина совместных действий по проведению информационных операций. Наставление объединенного штаба КНШ ВС США 3–13. 1998 (перевод) – М. : ГШ ВС РФ, 1999.

2. Квачков В.В. Спецназ России. Военная литература, 2004.

3. Савельев И.Л., Шерстюк Ю.М. Архитектура службы технологического управления узла связи // Санкт-Петербургская международная конференция «Региональная информатика – 2006», Санкт-Петербург, 24–26 октября 2006 г. : Материалы конференции. – СПб. : СПОИСУ, 2006. – С. 93–94.

4. Шерстюк Ю.М., Зарипов В.Д., Рожнов М.Д., Савельев И.Л. Архитектура средств технологического управления телекоммуникациями // Телекоммуникационные технологии. 2006, вып. 2. – С. 33–40.

5. Савельев И.Л., Шерстюк Ю.М. Построение службы технологического управления узла связи // Санкт-Петербургская международная конференция «Региональная информатика – 2006 (РИ-2006)», Санкт-Петербург, 24–26 октября 2006 г. Труды конференции, секция Телекоммуникационные сети и технологии. – СПб. : СПОИСУ, 2007. – С. 80–88.

6. Воронков К.Л., Шерстюк Ю.М. Формализация содержания процессов управления узлом информационного противодействия // II Международная конференция «Информационная безопасность регионов России», Санкт-Петербург, 26–29 ноября 2001 г. : Материалы конференции. Том 1. – СПб., 2001. – С. 54–55.

7. Воронков К.Л., Шерстюк Ю.М. Оперативность и обоснованность принятия решений подсистемой защиты узла информационного противодействия // VIII Санкт-Петербургская Международная конференция «Региональная информатика – 2002», Материалы конференции в 2-х частях. Часть 1. – СПб., 2002. – С. 102.