УДК 621.391

МОДЕЛИ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

К. Е. Легков, заместитель начальника кафедры АСУ Военно-космической академии им. А. Ф. Можайского, к.т.н.; constl@mail.ru
А. Н. Буренин, доцент кафедры АСУ ВКА им. А. Ф. Можайского, к.т.н.; konferencia_asu_vka@mail.ru

Показано, что функционирование современных инфокоммуникационных сетей специального назначения с высокими качественными показателями может быть обеспечено только при решении комплекса задач управления их безопасностью. Приводятся различные модели, описывающие возможные варианты реализации атакующих действий противника с учетом его первоначального положения, уровня знаний и навыка, конфигурации самой инфокоммуникационной сети, а также реализуемой политики безопасности. На основе этих моделей анализируется уровень защищенности инфокоммуникационной сети, определяются «узкие» места сети, даются рекомендации по устранению обнаруженных «дыр» безопасности, предлагаются модели встроенных в архитектуру системы управления программных комплексов, позволяющих выявлять характер и интенсивность информационных воздействий на критически важные элементы сетей.

Ключевые слова: *инфокоммуникационная система, качество обслуживания, управление, услуги, эффективность.*

Введение. В настоящее время в составе выделенных систем связи специального назначения создается ряд телекоммуникационных сетей, в совокупности образующих инфокоммуникационную сеть, которая фактически является информационным и телекоммуникационным ядром соответствующей системы связи и предоставляет пользователям требуемые услуги связи [1, 2].

Функционирование таких выделенных инфокоммуникационных сетей с высокими качественными показателями в условиях достаточно жестких требований, предъявляемых со стороны пользователей информационных систем и автоматизированных систем управления (АСУ), возможно только при решении целого комплекса задач обеспечения информационной безопасности. При этом решающая роль в этом вопросе отводится АСУ инфокоммуникационной сетью [3].

Возросшая сложность телекоммуникационных сетей, входящих в состав выделенной инфокоммуникационной сети (абонентские сети, сети доступа, транспортная сеть, сети услуг каждого уровня сети), и механизмов их защиты, увеличение количества уязвимостей, потенциальных ошибок в использовании различных средств телекоммуникаций, в предоставлении услуг и управления, а также усиление возможностей потенциального нарушителя по реализации различного рода атак — все это делает необходимой разработку мощных автоматизированных подсистем анализа атак и управления безопасностью выделенной инфокоммуникационной сети. Эти подсистемы, в свою очередь, существенно повышают защищенность элементов сети и призваны выполнять задачи по обнаружению состоявшихся фактов информационных воздействий и существующих ошибок в конфигурировании каждой сети, по выявлению возможных атакующих действий различных категорий нарушителей и определению критичных сетевых ресурсов, а также подготовить данные по выбору адекватной программы управления безопасностью.

Модели управления безопасностью инфокоммуникационных сетей. При решении задач управления информационной безопасностью выделенной инфокоммуникационной сети используются понятия модели атак, модели нарушителя, объекта атак (инфокоммуникационная сеть, элементы сети) и т.д. [4–6].

Модель атак служит для описания возможных действий противника и формирования сценариев реализации этих действий. Как правило, она имеет вид иерархической структуры [4–6]. Верхними уровнями являются комплексный и сценарный.

Комплексный уровень определяет множество высокоуровневых целей процесса анализа защищенности (анализ на нарушение основных аспектов информационной безопасности: целостности, конфиденциальности, доступности) и множество анализируемых (атакуемых) объектов. На комплексном уровне может быть обеспечено согласование нескольких сценариев, которые реализуются группой нарушителей противника.

Сценарный уровень учитывает *модель нарушителя* (противника), определяет конкретный атакуемый объект выделенной инфокоммуникационной сети (автоматизированные рабочие места (АРМ) должностных лиц (ДЛ) пунктов управления (ПУ), сервер и т.д.) и цель атаки (например, «определение типа операционной системы АРМ», «реализация атаки отказа в обслуживании» и т.п.). Он содержит определенные этапы сценария, множество которых состоит из групп элементов: разведка, внедрение (первоначальный доступ к объекту атаки), повышение привилегий, реализация угрозы, сокрытие следов, создание потайных ходов.

Элементы сценарного уровня, расположенные ниже, служат для детализации целей, достигаемых реализацией данного сценария. Нижний уровень в иерархии концептуальной модели компьютерных атак описывает низкоуровневые атакующие действия нарушителя.

Модель нарушителя (противника) тесно связана с моделью атак. Их взаимосвязь состоит в том, что в модели атак содержится максимально полное описание возможных способов компрометации объектов выделенной инфокоммуникационной сети, а модель противника конкретизирует, кто, какими средствами и с использованием каких знаний может реализовать данные угрозы и нанести ущерб тому или иному объекту сети. При этом сама модель должна учитывать основные параметры противника:

- первоначальное положение (внутренние и внешние нарушители);
- уровень знаний и умений, определяющий возможности противника по реализации атакующих действий (зада-

ется перечнем известных противнику уязвимостей выделенной инфокоммуникационной сети, средств реализации атаки и т.п.);

- первичные знания об атакуемой выделенной инфокоммуникационной сети (например, в виде перечня АРМ ДЛ ПУ, коммутаторов, маршрутизаторов, серверов, пользователей и т.п.);
- метод генерации сценария (используется ли оптимизация сценария для достижения заданной цели).

Для более подробного описания сценариев различных атак часто применяется *модель формирования общего графа атак*. Она служит для построения графовой модели, описывающей всевозможные варианты реализации атакующих действий противника с учетом его первоначального положения, уровня знаний и навыка, конфигурации выделенной инфокоммуникационной сети, реализуемой в ней политики безопасности. На основе графа атак производится анализ защищенности выделенной инфокоммуникационной сети, определяются «узкие» места сети — эти данные помогают выработать рекомендации по устранению обнаруженных уязвимостей (с учетом уровня критичности) и по управлению безопасностью.

В общем случае, при успешной реализации противником разведывательных действий, нарушения конфиденциальности, целостности и доступности информационных ресурсов выделенной инфокоммуникационной сети не происходит. Однако возможно нарушение конфиденциальности, например, в случае, когда политикой безопасности в сети установлено, что информация о топологии той или иной внутренней сети выделенной инфокоммуникационной сети является закрытой. При успешном получении противником прав локального пользователя возможности выполнения действий, направленных на нарушение конфиденциальности, целостности и доступности или на получение прав администратора, увеличиваются, так как он может, в частности, нарушить конфиденциальность, целостность и доступность некоторой совокупности объектов сети, имея только права пользователя. При успешном получении прав администратора на определенном АРМ или сервере противник может полностью нарушить конфиденциальность, целостность, доступность всех объектов данного узла выделенной инфокоммуникационной сети или даже ее фрагмента.

Модели программных комплексов. По мере усложнения выделенной инфокоммуникационной сети все ее объекты обычно упорядочиваются следующим образом: элементы сети → атакующие действия → трассы атак → угрозы → общий граф атак.

После реализации каждого из сценариев, принадлежащих множеству сценариев разведки, производится проверка условий выполнения атакующих действий, использующих уязвимости программного и аппаратного обеспечения элементов выделенной инфокоммуникационной сети. При успешной реализации атакующих действий заданной группы, приводящих к получению противником прав локального пользователя или администратора на атакованном АРМ или сервере, осуществляется проверка необходимости перехода противника (нарушителя) на данный элемент сети. В случае реализации перехода эта же последовательность действий повторяется для нового положения противника.

Модель выделенной инфокоммуникационной сети служит для представления используемого в данной сети программного и аппаратного обеспечения, распознавания действий нарушителя и определения реакции сети на реализуемые противником атакующие действия. Для спецификации аппаратного и программного обеспечения обычно используется некий специализированный язык, использующий основные объектно-ориентированные технологии структурирования и концептуализации. При этом производится описание выделенной инфокоммуникационной сети на уровне ее топологии и сетевых сервисов. Сетевая топология определяется классами физических элементов сети, связанных физическими линиями (цифровыми каналами, трактами), а сетевые сервисы — классами «электронная почта», «файловый обмен», «диалоговый режим» и т.д.

В модель выделенной инфокоммуникационной сети обычно встраивается *общая модель распознавания действий противника*, которая позволяет осуществлять преобразование низкоуровневого представления атакующих действий (последовательности «ложных» сетевых пакетов или «ложных» команд для операционной системы) в высокоуровневые идентификаторы атак. Как правило, в основу этой модели положен механизм, реализующий сигнатурный метод: поступающая на вход модели выделенной инфокоммуникационной сети последовательность (поток) атакующих действий сравнивается с заранее определенными сигнатурами и в случае обнаружения сходства определяется высокоуровневый идентификатор атаки.

Другой моделью, используемой при решении задач обеспечения информационной безопасности выделенной инфокоммуникационной сети, является *модель оценки уровня защищенности*, которая охватывает определенную систему различных метрик безопасности и правил, применяемых для их расчета и оценки. При этом множество всех метрик безопасности строится на основе уже рассмотренного сформированного общего графа атак. Метрики безопасности, обычно характеризующие защищенность как базовых, так и составных объектов графа атак, классифицируются по разделению объектов общего графа атак на базовые и составные — в соответствии с порядком вычислений, а также с тем, используются ли метрики для определения общего уровня защищенности выделенной инфокоммуникационной сети. Примерами метрик безопасности являются критичность конкретного АРМ, сервера, коммутатора, маршрутизатора, размер ущерба при реализации угрозы, количество трасс атак на графе и т.д.

Технология интеллектуальных мультиагентных систем. Во многих случаях для оценки уровня защищенности выделенной инфокоммуникационной сети может быть применен упрощенный экспресс-метод так называемой интеллектуальной системы анализа [5], который состоит из следующих этапов:

- определение уровня критичности элементов выделенной инфокоммуникационной сети по упрощенной трехуровневой шкале (высокий, средний, низкий);
- определение критичности атакующих действий;
- определение размера ущерба, вызванного успешной реализацией атакующего действия и зависящего от уровней критичности действия и атакуемого элемента сети; определение размера ущерба для всех угроз;
- определение метрик сложности в доступе для всех атакующих действий во всех трассах с учетом значений данного показателя для каждого из действий, составляющих трассу, и всех угроз с учетом значений данного показателя для всех трасс, составляющих угрозу;
- определение степени возможности реализации угрозы на основе показателя сложности в доступе;
- определение общего уровня защищенности выделенной инфокоммуникационной сети на базе полученных оце-

нок степени реализации угрозы и размера ущерба, вызванного ее успешной реализацией.

Традиционные методы защиты телекоммуникационных сетей ориентированы преимущественно на защиту от конкретных (известных или прогнозируемых) видов угроз и атак и реализуются в виде набора программных и аппаратных компонентов, функционирующих относительно независимо. Существующие системы защиты обычно имеют централизованную структуру, характеризуются неразвитыми адаптационными возможностями, пассивными механизмами обнаружения атак, большим процентом ложных срабатываний при обнаружении вторжений, значительной деградацией трафика целевых информационных потоков из-за значительного объема ресурсов, выделяемых на защиту, и т.п. Поэтому в последнее время появился другой перспективный подход к построению комплексных систем защиты информации в выделенных инфокоммуникационных сетях, позволяющий преодолеть некоторые из перечисленных недостатков. В его основу положена технология интеллектуальных мультиагентных систем, которая позволяет существенно, по сравнению с традиционными методами, повысить эффективность защиты информации, в том числе ее адекватность, отказоустойчивость, устойчивость к деструктивным действиям, универсальность, гибкость и т.д.

Данный подход предполагает, что компоненты систем защиты информации в выделенной инфокоммуникационной сети, специализированные по типам решаемых задач, тесно взаимодействуют друг с другом с целью обмена информацией и принятия согласованных решений, адаптируются к изменению трафика, реконфигурации аппаратного и программного обеспечения, а также к новым видам атак. При этом компоненты мультиагентной системы защиты информации представляют собой интеллектуальные автономные программы (агенты защиты), реализующие определенные функции защиты с целью обеспечения требуемого класса защищенности. Они позволяют реализовать комплексную надстройку над механизмами безопасности используемых сетевых программных средств, операционных систем и приложений, повышая защищенность сети до требуемого уровня. Согласно этой технологии процесс создания мультиагентных систем для любой предметной области, в том числе для защиты информации в выделенной инфокоммуникационной сети, предполагает решение двух высокоуровневых задач:

- создание «системного ядра» мультиагентной системы;
- клонирование программных агентов и отделение сгенерированной мультиагентной системы от «системного ядра».

Математическое описание информационных воздействий. В формальной модели и прототипе агентно-ориентированной системы моделирования атак распределенные скоординированные атаки на выделенную инфокоммуникационную сеть должны рассматриваться в виде последовательности совместных действий агентов-противников, выполняемых с различных элементов сети, в которые они заранее внедрены. Агенты противника координируют свои действия согласно какому-то общему сценарию. На каждом шаге сценария атаки они пытаются реализовать некую частную подцель.

Важное значение для решения задач обеспечения информационной безопасности выделенной инфокоммуникационной сети при воздействиях противника имеет математическое описание потоков информационных воздействий. Так как информационные воздействия противника на элементы выделенной инфокоммуникационной сети могут происходить в произвольные, случайные моменты времени, интервалы между воздействиями в общем случае также являются случайными величинами, последовательность информационных воздействий может быть математически описана моделью стохастического потока атак. Наиболее общим видом потока является рекуррентный поток, отличающийся тем, что интервалы времени между двумя информационными воздействиями независимы и имеют одинаковые произвольные функции распределения $F(t)$. Так, простейший поток является частным случаем рекуррентного потока, у которого $F(t) = 1 - e^{-\lambda t}$.

Запишем вероятность того, что в интервале времени длительностью Δt поступит ровно k воздействий:

$$P_k(\Delta t) = \int_0^{\Delta t} P_{k-1}(\Delta t - x)\, dF(x). \qquad (1)$$

Ясно, что $P_0(0) = 1 - F(\Delta t)$.

Математическое ожидание числа требований рекуррентного потока информационных воздействий на выделенную инфокоммуникационную сеть, приходящихся на интервал длиной Δt, определяется формулой

$$m(\Delta t) = \int_0^{\Delta t} [1 + m(\Delta t - x)]\, dF(x) = \\ = F(\Delta t) + \int_0^{\Delta t} m(\Delta t - x) dF(x). \qquad (2)$$

Если вероятность нулевой длительности промежутка между информационными воздействиями противника недостаточно мала, замена такого интервально-рекуррентного потока простейшим приведет к заметным ошибкам. Интервально-рекуррентный поток с функциями распределения промежутков времени между двумя требованиями «хуже» пуассоновского, поэтому интенсивность эквивалентного потока при управлении безопасностью выделенной инфокоммуникационной сети можно увеличить на значение, полученное на основе моделирования.

Заключение. Математическое описание потоков информационных воздействий позволяет обоснованно осуществлять в контуре системы управления выделенной инфокоммуникационной сетью моделирование программно-аппаратных атак в соответствии с предполагаемыми угрозами, имеющимися в арсенале потенциального противника и известными создателям и обслуживающему персоналу сети. При этом моделирование атак удобно проводить в рамках агентов системы управления, реализованных во всех без исключения элементах выделенной инфокоммуникационной сети (в АРМ, серверах, коммутаторах, маршрутизаторах и др.), наделяя их дополнительными функциями по генерированию образов программных агентов, поддерживающих различные компоненты программно-аппаратных атак. Менеджеры же системы управления будут выступать в качестве агентов, имитирующих организацию комплексов атак.

Эти же компоненты системы управления будут выполнять функции компонентов мультиагентной системы обеспечения информационной безопасности сети, каждый из которых реализует вполне конкретные функции защиты. При этом множество многомерных векторов состояния контролируемых параметров после имитационного (тестового)

воздействия периодически сравнивается с реально фиксируемым вектором состояния во время функционирования выделенной инфокоммуникационной сети.

ЛИТЕРАТУРА

1. **Легков К. Е.** О некоторых подходах к повышению эффективности системы управления в рамках изменения подхода к автоматизации и информации/К. Е. Легков // Мобильные телекоммуникации (Mobile Communications).— 2013.— № 7.— С. 48.
2. **Легков К. Е.** Основные теоретические и прикладные проблемы технической основы системы управления специального назначения и основные направления создания инфокоммуникационной системы специального назначения/К. Е. Легков // T-Comm: Телекоммуникации и транспорт.— 2013.— Т. 7, № 6.— С. 42–46.
3. **Легков К. Е.** Вероятность потери пакета в беспроводных сетях со случайным множественным доступом к среде передачи/ К. Е. Легков, А. А. Донченко//T-Comm: Телекоммуникации и транспорт.— 2011.— Т. 5, № 5.— С. 32–33.
4. **Легков К. Е.** Современные технологии беспроводного широкополосного доступа 802.16E и LTE: перспективы внедрения на транспорте/К. Е. Легков, А. А. Донченко, В. В. Садовов // T-Comm: Телекоммуникации и транспорт.— 2010.— Т. 4, № 2.— С. 30–32.
5. **Легков К. Е.** Беспроводные MESH сети специального назначения/К. Е. Легков, А. А. Донченко // T-Comm: Телекоммуникации и транспорт.— 2009.— Т. 3, № 3.— С. 36–37.
6. **Легков К. Е.** Анализ систем передачи в сетях беспроводного доступа/К. Е. Легков, А. А. Донченко // T-Comm: Телекоммуникации и транспорт.— 2009.— Т. 3, № 2.— С. 40–41.

Получено 30.10.14

ИНФОРМАЦИЯ

«НАУКА И АСУ-2014»: НАДЕЖНОСТЬ, МОБИЛЬНОСТЬ, ОТВЕТСТВЕННОСТЬ

На Всероссийской научно-технической конференции «Наука и АСУ-2014», состоявшейся 30 октября 2014 года в Московском техническом университете связи и информатики (МТУСИ), рассматривались теоретические и прикладные проблемы развития и совершенствования автоматизированных систем управления (АСУ).

Тон обсуждению задал председатель конференции **Б. П. Смирнов** — главный конструктор АСУ МР, руководитель ЗАО «НПЦ ИРС». Он остановился на вопросах автоматизации всех типов учета, отчетности и других процессов, исполняющихся в разноуровневом порядке.

Научный руководитель ОАО «ГСКБ «Алмаз-Антей» **Я. В. Безель,** говоря об основных принципах построения АСУ реального времени жестко регламентированным циклом, подчеркнул ответственность специалистов, которые занимаются программированием, поскольку все АПК предъявляют высокие требования к вычислительной среде.

Начальник научно-технического отдела ЦНИРТИ им. академика А. И. Берга **Б. В. Хлопов** посвятил выступление разработке нормативных документов для аппаратуры стирания информации с электронных носителей (магнитных, оптических, жестких дисков и пр.), в том числе регулирующих вопросы экстренного уничтожения информации.

Заместитель генерального директора ООО «АйКомИнвест» по инновационным технологиям **В. О. Тихвинский** определил новую парадигму развития ИКТ как эру мобильной передачи данных, мобильного контента, услуг дистанционного управления. При этом, естественно, меняются бизнес-модели производства. Макроэкономический прогноз от В. О. Тихвинского: к 2050 г. ожидается 100%-ная роботизация производства. Миллиарды машин потребуют дистанционного управления технологическими процессами, и решить эти задачи призваны сети M2M, которые являются драйвером развития сетей 5G. Сдерживающий момент — отсутствие нормативной базы, регулирующей внедрение в России сетей M2M.

Практическим опытом автоматизации процессов сетевого технологического управления объектами инфокоммуникационной инфраструктуры для Олимпиады-2014 в Сочи поделился главный научный сотрудник ОАО «НТЦ ВСП «Супертел ДАЛС» **Г. В. Сызранцев**. «СУПЕРТЕЛ» был ответственным поставщиком оборудования при строительстве волоконно-оптических линий передачи Анапа–Джубга, Джубга–Сочи с ответвлением от Джубги до Краснодара. Ситуация осложнялась тем, что основные объекты связи для обеспечения управления подготовкой и проведением зимних Олимпийских и Паралимпийских игр находятся в горном кластере, где своего оптического кабеля не было проложено, так что приходилось арендовать волокна в кабельных линиях связи, принадлежащих различным владельцам. Пусконаладочные работы сдерживались погодными условиями, действиями других строительных организаций, которые нередко повреждали магистральный оптический кабель.

Строительная готовность олимпийского сегмента сети связи была достигнута всего за несколько месяцев до начала Игр. Предварительные испытания, имитация аварийных ситуаций и расчеты структурной надежности построенной сети связи показали, что выполнить требования Олимпийского комитета по устойчивости работы всей системы связи весьма проблематично. Повысить мобильность резервирования основного оборудования сети связи и устойчивость работы сети в целом помогли некоторые организационно-технические меры, такие как доработка встроенного программного обеспечения оборудования на базе технологии NGSDH, обеспечившая резервирование основных информационных потоков без использования дополнительного оборудования связи, организация резервных трасс к базовым станциям стандарта TETRA основных олимпийских объектов, резервирование информационных потоков по альтернативным трассам связи с использованием оборудования с функциями автоматического резервирования технологии NGPDH и др.

Первичные мультиплексоры технологии NGPDH обеспечивали переключение информационных потоков на любую из имеющихся трасс связей при обрыве основной трассы автоматически. Специальное встроенное ПО этих мультиплексоров в совокупности с сетевым ПО «Супертел-NMS v3» позволяет строить автоматические первичные сети связи, что и было применено для повышения оперативности функционирования систем управления практически всеми службами на Олимпиаде.

За время работы службы управления связью, которую возглавлял Г. В. Сызранцев, были разработаны новые формы документов для этапов планирования связи и эксплуатационного обеспечения, а также новые формы и методы обеспечения эксплуатационной надежности функционирования опорно-транспортной сети связи. Среди них известные (эшелонирование мобильных групп линейных надсмотрщиков, несущих круглосуточное дежурство и распределенных по трассам связи, причем время прибытия на самый удаленный объект ответственности не превышало 10 мин) и новые, основанные на особенностях построения топологии сети связи и высокой управляемости информационными потоками как на программном уровне, так и на физическом. Все это позволило провести Олимпиаду без претензий со стороны оргкомитета к службам обеспечения и предоставления услуг связи.

Доработка опорно-транспортной сети связи была осуществлена «олимпийской командой» ОАО «НТЦ ВСП «Супертел ДАЛС» с 20 января по 5 февраля 2014 г. Возможности аппаратуры связи и принятые меры повышения устойчивости функционирования сети связи обеспечили значения этого показателя к 5 февраля, когда состоялся первый хоккейный матч, на уровне 0,96.

В ходе Олимпийских и Паралимпийских игр отмечалось несколько аварийных ситуаций, вызванных погодными и техническими условиями. Достаточный уровень структурной надежности сети связи, в том числе методами автоматизации отдельных функций системы сетевого технологического управления, обеспечил высокую устойчивость к авариям, последствия которых никак не отразились на функционировании системы связи в целом.

Подробнее см. http://www.elsv.ru/news/?id=478