УДК 355.1

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СВЯЗИ И ИНФОРМАЦИИ ПРИ СЕТЕЦЕНТРИЧЕСКОМ УПРАВЛЕНИИ ВОЙСКАМИ И РАЗЛИЧНЫХ СЦЕНАРИЯХ НАПАДЕНИЯ НА ТЕЛЕКОММУНИКАЦИОННУЮ СЕТЬ

Ю.А. СЕМАШКО, В.М. КАЛИНИН, В.Н. ШЕПТУРА

Военная академия Республики Беларусь
Минск-57, 220057, Беларусь

Поступила в редакцию 24 мая 2012

Определяется место и роль телекоммуникационной сети как основы формирования единого информационного пространства при ведении сетецентрических боевых действий. Анализируется аспект уязвимости телекоммуникационных сетей в плане обеспечения безопасности связи и защиты информации. Рассматриваются наиболее вероятные сценарии нападения на сеть и их последствия. Формулируются основные требования к безопасности связи и защите информации. Предлагается общее решение проблемы создания устойчивой к атакам телекоммуникационной сети.

Ключевые слова: информация, телекоммуникационная сеть, безопасность информации, легитимный узел, скомпрометированный узел, нападение на сеть, сценарий нападения, сетевая атака.

Введение

В настоящее время проблема ведения военных действий в едином информационном пространстве приобретает особую актуальность, поскольку при реализации сетецентрического принципа управления войсками (силами) информация играет ключевую роль в обеспечении анализа ситуации в реальном масштабе времени и принятия обоснованного решения. С помощью информационных и телекоммуникационных технологий можно мгновенно собрать, обработать и распространить информацию (или дезинформацию) в любой точке зоны ответственности группировки войск (сил) [1].

Анализ проблемы обеспечения безопасности информации, постановка задачи создания устойчивой к нападениям телекоммуникационной сети

В едином информационном пространстве рассредоточенные воинские формирования могут вести совместные действия, динамически перераспределять ответственность, задачи и адаптироваться к изменениям обстановки. Для этого необходимо наличие высокоэффективной информационной инфраструктуры, которая обеспечит все элементы группировки войск (сил) полноценным доступом к общему информационному ресурсу. Информационные и телекоммуникационные системы и сети посредством сбора, обработки, анализа и распределения информации обеспечивают реализацию информационной технологии поддержки принятия решений и виртуализацию управленческих процессов [2]. При этом отпадает привычная необходимость присутствия в одном месте в одно и то же время должностных лиц, участвующих в выработке элементов решения, поскольку система обеспечивает обмен информацией между ними независимо от их местоположения. Единое информационное пространство позволяет лицу, принимающему решения, понять и оценить ситуацию в реальном масштабе времени, определить порядок действий и довести его до подчиненных.

По мере возрастания информационно-технологического прогресса возможности группировок войск (сил) по ведению военных действий в едином информационном пространстве будут возрастать. Поэтому самыми уязвимыми компонентами инфраструктуры являются телекоммуникационные сети, а обеспечение их информационной безопасности должно стать одним из приоритетных направлений военного строительства и строительства Вооруженных Сил единого государства Российской Федерации и Республики Беларусь [3, 4].

Телекоммуникационные сети военного назначения, являясь основой для формирования единого информационного пространства, должны использовать открытые (гражданские и коммерческие) стандарты, в том числе IP-технологии, поскольку предполагают сопряжение и взаимодействие с государственными и ведомственными сетями, развернутыми в зоне ответственности группировки войск (сил) и (или) региональной группировки Вооруженных Сил Союзного Государства. При этом с целью выполнения требований по безопасности связи необходим пересмотр и повышение надежности существующих IP-протоколов (в плане их имитостойкости).

В настоящее время Интернет является в основном статическим, проводным и работает в изначально невраждебной окружающей среде. В военное время среда информационного обмена кардинально меняется и трансформируется во враждебную, характеризуемую широким спектром угроз несанкционированного доступа к информации. Практика показывает, что в таких условиях простое добавление правил безопасности в существующие протоколы не является решением проблемы по существу, поскольку даже в мирное время, независимо от наличия множества доступных решений для обеспечения конфиденциальности коммерческой и личной информации, локальные сети и персональные компьютеры пользователей до сих пор остаются весьма уязвимыми для хакерских атак и нападений. В военное время данная проблема еще более обострится и, если безопасность телекоммуникационной сети не будет гарантированно обеспечена, она станет бесполезной как инструмент для принятия управленческих решений.

При нарастании военной угрозы и в военное время обеспечение безопасности телекоммуникационной сети для органов государственного и военного управления становится сложной и многогранной проблемой. Это обуславливается бескомпромиссностью информационной войны и антагонизмом преследуемых ею целей, динамичностью информационной среды, широким применением ранее считавшихся запрещенными приемов и методов разрушения информации или ее подмены ложной. Динамичность заключается в том, что требования к безопасности информации, военной связи и разведывательной защищенности телекоммуникационной сети будут меняться вследствие существенного увеличения числа мобильных сетевых узлов, их частого перемещения и повышения удельного веса беспроводных линий связи в их общем количестве. Вследствие резкого увеличения размерности сети и ее реконфигурации за счет добавления к стационарным большого числа подвижных (мобильных) пользователей невозможно установить одинаковые требования к безопасности информации и связи для всех узлов. Следовательно, всякий раз при изменении конфигурации сети нужно устанавливать новые требования к ее разведывательной защищенности, безопасности информации и связи. Практика показывает, что традиционные протоколы этого профиля становятся слишком громоздкими для их практического применения в условиях, когда ресурсы сети недостаточны, а узлы слишком быстро или часто перемещаются [5, 6].

Беспроводные сети не только уязвимы для атак, но и содержат явные и вторичные разведпризнаки пользователей, что позволяет противнику добывать важную информацию о сети, принадлежности пунктов управления и намерениях органов управления. Скрытие такой сети, как и полное исключение ее разведывательной доступности, фактически невозможно. Кроме того, антагонистическая окружающая сетевая среда предполагает новые информационные угрозы, которые ранее не были свойственны телекоммуникационным сетям – например, компрометация узлов связи. Скомпрометированный узел – это свой узел, которым управляет противник. Следовательно, против атак, исходящих изнутри сети, все традиционные решения проблемы ее безопасности неприемлемы. Использование криптографической защиты в этих условиях не имеет смысла, поскольку скомпрометированный узел имеет доступ к ключам и шифрам [7].

Таким образом, телекоммуникационные сети, с одной стороны, позволяют должностным лицам обмениваться информацией независимо от их местоположения, что устраняет фак-

торы места и времени, которые ранее вынуждали вести военные действия на ограниченных пространствах. С другой стороны, если безопасность сети нарушена, противник способен вмешаться в процесс выработки и принятия решения. Информация может быть перехвачена, задержана или изменена, следовательно, нарушается ситуационная осведомленность и адекватное восприятие обстановки. В конечном счете, если информация будет противоречить объективно сложившейся обстановке, принимаемые в соответствии с ее оценкой решения будут либо неправильными, либо необоснованными, либо отсроченными, что может позволить противнику получить определенные преимущества.

Отметим несколько специальных понятий и терминов, относящихся к безопасности телекоммуникационной сети, функционирующей в едином информационном пространстве [8].

Термины и определения

Термин правильные пакеты означает, что в сети может осуществляться передача только тех пакетов, которые не проявляют каких-либо признаков нарушения их формата, содержания и отправлены легитимными (определенными маршрутно-адресной таблицей) узлами. Пакеты, которые разбиты на фрагменты (субпакеты), должны прибыть к своему месту назначения без задержек по времени доставки и нарушений их целостности в пути. Крайне важно гарантировать, чтобы пакеты вовремя доставлялись адресатам и сшивались до наступления момента времени потери актуальности содержащейся в них информации. В маршрутизации могут участвовать только легитимные узлы сети. Если узел становится скомпрометированным, он больше не должен быть допущен к сетевым операциям. Служебная информация, циркулирующая между узлами сети, должна обеспечивать защиту таблиц маршрутизации от искажений. Крайне важна и ее конфиденциальность, поскольку сеть всегда передает информацию о своей структуре, местоположении узлов, условиях их функционирования и т. д., по которой разведка противника может получать сведения о группировке войск (сил), ее состоянии, действиях и возможных намерениях. Однако следует понимать, что достижение полной конфиденциальности является чрезвычайно трудной задачей, особенно при обмене информации по беспроводным сетям.

Специальные требования предъявляются и к технической надежности средств и комплексов управления, связи и автоматизации. Эксплуатационные отказы в обслуживании не должны приводить к превышению установленных временных задержек доставки пакетов, вызванных перегруженностью сети, или, в худшем случае, деградацией ее состояния либо полным разрушением (развалом) структуры [9].

Условно можно выделить три уровня безопасности информации при сетецентрическом управлении группировкой войск (сил): безопасность содержания информации, безопасность коммуникации и безопасность сети.

Безопасность содержания информации предполагает непосредственную защиту содержания информационного обмена между двумя абонентами (пользователями). При этом в качестве пользователей могут выступать как должностные лица, так и компьютерные процессы, имеющие возможность проверить источник информации.

Безопасность коммуникации охватывает защиту данных, которые передаются по сети от источника к получателю. Оконечные точки в этом случае – компьютерные узлы, имеющие несколько пользователей.

Главное различие между этими двумя видами безопасности заключается в том, что при безопасности содержания информации оконечными точками являются истинные пользователи, а при безопасности коммуникации – компьютеры, передающие и принимающие данные. Корреспондирующие узлы должны иметь возможность проверить легитимность друг друга до коммуникации. Кроме того, передаваемые данные должны быть защищены от расшифровки и модификации с целью исключения ввода ложной информации и недопустимой задержки.

Безопасность сети имеет самое непосредственное отношение к выполнению задач по своевременной пересылке правильных (легитимных) пакетов в нужном информационном направлении, не нарушая приоритетов и (или) установленных категорий срочности. Этот уровень безопасности отличается от двух предыдущих тем, что его главная задача состоит в передаче информации от источника к получателю, не затрагивая ее содержания.

Пример практического решения проблемы обеспечения безопасности содержания информации – протокол типа PGP. Приемлемые решения для безопасности коммуникации протоколы IPSec (защиты IP трафика), TLS (транспортного уровня между абонентом и сервером) и SSH (удаленных абонентов) [9, 10].

Безопасность сети, в свою очередь, имеет несколько аспектов и уровней. Физическая безопасность охватывает защиту линий и узлов сети (например, защиту маршрутизаторов различными средствами управления доступом). В целом же уровень сетевой безопасности решает вопросы защиты связей между двумя узлами. Цель сетевой безопасности в беспроводной сети состоит в том, чтобы обеспечить такую же степень безопасности, как и в проводной сети. Как правило, безопасность сети включает установление подлинности абонента (его идентификацию) и шифрование (кодирование). Кроме того, протоколы безопасности сети должны обеспечить защиту от преднамеренного изменения ее структуры или нарушения управления сетью.

Возможные сценарии нападения на сеть и их последствия

Нападение на структуру телекоммуникационной сети может быть внешним или внутренним. В первом случае незаконный узел внедряется в сеть как законный (легитимный). Во втором случае легитимный узел скомпрометирован, т. е. попал под влияние противника, управляется им и маскируется под легитимный, чтобы использоваться в дальнейшем для нападения на сеть. Результатом такого нападения может стать:

– отказ в обслуживании, когда узел потребляет ресурсы сети, вызывая ее перегрузку. Особенно это опасно в беспроводных сетях, где и сетевые ресурсы, и ресурсы узлов имеют ограниченную мощность, не достаточную для компенсации потерь;

– разрушение передачи служебной информации протоколов, когда узел участвует в передаче служебной информации протокола и в состоянии изменить структуру маршрутизации;

– разрушение трафика сети, когда узел способен снизить скорость передачи или задержать пакеты. Это касается в основном функций протоколов высших уровней. В результате узел генерирует ненужный служебный трафик, вызывает перегрузку и, в конечном счете, разрушает целостность сети;

– анализ трафика, когда узел отслеживает трафик сети и на основе анализа раскрывает ее структуру, определяя местоположение узлов, их роль, назначение, принадлежность и т. д.;

– распространение дезинформации, когда узел распространяет в сети ложную, но достаточно правдоподобную информацию. Например, узел может действовать как датчик и передавать ошибочные данные во время сбора сведений об обстановке.

Сценарии нападения на телекоммуникационную сеть могут быть различными. Например, на рис. 1 представлен сценарий нападения на сеть двух узлов противника (E_1 и E_2).

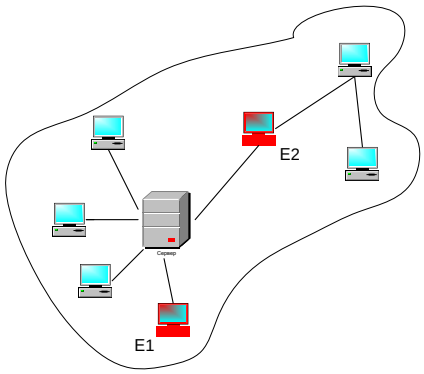
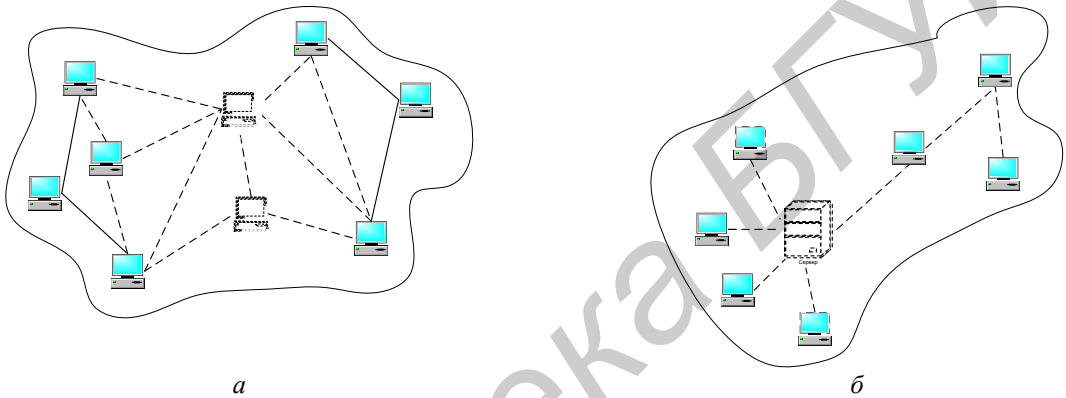


Рис. 1. Сценарий нападения на телекоммуникационную сеть двух узлов противника

Узел E_1 замаскировался под легитимный и предоставляет серверу дезинформацию. Сервер собирает данные из различных источников и составляет представление об окружающей среде путем объединения данных. Однако, поскольку некоторые из собранных данных ошибочны, заключительная картина будет отличаться от реальной и являться искаженной. Затем эта ложная картина распространяется по сети и может, в конечном счете, привести к ошибочному решению, основанному на неверном ситуативном понимании.

Узел E_2, с другой стороны, проводит атаки на сеть с целью получить в ее центре отказ в обслуживании. Получая пакеты от сервера, он дублирует их и передает к следующему узлу сети. Атака с целью отказа в обслуживании распространяется вплоть до узла назначения, который выявляет пакеты-двойники и отказывается от них. Если сеть беспроводная, эти атаки особенно серьезны по своим последствиям для узлов, начиная с соседних с E_2, и до тех, через которые проходит информация к узлу-получателю. Чтобы хоть как-то воспрепятствовать нарастанию перегрузки сети, спровоцированной узлом E_2, нельзя допускать, чтобы легитимные узлы своими действиями ее «ускоряли». С этой целью необходимо осуществлять контроль подлинности всех узлов сети так же, как и всех пакетов. Для исключения подобных атак любой узел должен быть в состоянии проверить, что принимаемые пакеты легитимны, своевременны и уникальны (не содержат дубликатов).

В результате ряда успешных атак сеть может быть физически разрушена, т. е. становится разобщенной и функционально неспособной выполнять свое предназначение. На рис. 2, *а* показана структура частично разрушенной сети, где пунктиром обозначены разрушенные маршрутизаторы и линии связи. В результате предпринятых атак сеть оказалась разделена на две отдельных и утративших взаимосвязь части.



а *б*

Рис. 2. Сценарии нападения на сеть:
а – атака с целью частичного разрушения структуры; *б* – избирательная атака

Особо опасно по своим последствиям физическое разрушение базовой сети, в результате чего специальные сети могут потерять возможность соединения и превратиться в отдельные острова. Мобильные узлы могут потерять способность к перемещению в результате потери связи с узлом связи привязки. Серверы потерявших связность узлов могут выключить некоторые свои функции, что в еще большей степени усложнит обстановку для оставшейся работоспособной части сети. В целях устранения последствий частичных разрушений базовые сети должны иметь функции восстановления и формирования своей структуры, при этом в первую очередь восстанавливаются маршруты и серверы.

На рис. 2, *б* приведен сценарий избирательной атаки на сеть. В ходе избирательной атаки уничтожаются только ключевые узлы. Ключевой узел в данном случае – это маршрутизатор доступа, который является основой локальной сети. Без этого узла у других узлов сети просто нет связи друг с другом и вместо того, чтобы разрушать всю сеть, противнику легче найти ключевые узлы и устранить их.

Полученные результаты и их обсуждение

Общее решение проблемы построения устойчивой к атакам сети состоит не только в том, чтобы не иметь в ней явных точек отказа (как в рассмотренном примере с маршрутизатором доступа) или осуществить многократное дублирование критических элементов структуры. Возможный выход из ситуации, когда в телекоммуникационной сети главный узел группы потерян – передача его функциональных возможностей на другой узел. Такие динамические решения позволяют устранить проблему единственной точки отказа, не осуществляя дублирование. Чтобы решить проблему кардинально и справиться с разрушением, необходимы не только силы и средства для быстрого восстановления утраченных элементов сети, но и динамическое

управление оставшимися с целью перераспределения оказываемых ими услуг на другие узлы. Это подразумевает, что каждый узел должен обладать всем набором функций и услуг, которые до определенного момента не используются, а активируются в нужное время.

Если узел в результате атаки не разрушен, а лишь скомпрометирован, то противник, используя его возможности, может в дальнейшем предпринять множество атак, сценариями которых могут быть, например:

– нападения, предпринимаемые узлами противника;

– компрометация других узлов и постепенный захват всей сети;

– вскрытие систем безопасности беспроводных сетей (алгоритмы псевдослучайной перестройки частот, широкополосного сигнала и т. д.) с целью их подавления;

– получение доступа ко всем услугам и информации, которые получают легитимные узлы, с использованием последних для ввода ложной информации, поскольку каждый узел сети наделен правом изменять информацию;

– целенаправленное деструктивное изменение поведения сети посредством распространения дезинформации.

Если в результате атак на сеть скомпрометированные узлы станут превосходить по численности легитимные, то на сервере пункта управления группировки войск (сил) или информационно-технического центра появится большой объем ложной информации. В этом случае, если отсутствует надлежащий трастовый механизм обработки информации, сервер доверяет большинству поступивших на него данных, т. е. данным, предоставленным противником. Следовательно, созданная в результате объединения обработанных данных информационная картина складывающейся обстановки окажется искаженной в соответствии с замыслом противника. Кроме того, сервер может совершать и ошибки второго рода, признавая легитимные узлы незаконными и выдавая им сертификат недоверия, особенно если скомпрометированные узлы выборочно блокируют сообщения от легитимных узлов.

Основная проблема в борьбе со скомпрометированными узлами заключается в том, что традиционные решения для обеспечения безопасности, основанные на криптографии, не могут быть применены. Скомпрометированные узлы обходят криптографическую защиту, поскольку индивидуальные ключи становятся известны противнику, а других способов отличить скомпрометированный узел от легитимного, кроме контроля его поведения, просто не существует. При этом и сам контроль поведения узла, подозреваемого в потере легитимности, не является тривиальным. Например, легитимный узел может распространять ошибки из-за временного сбоя, а скомпрометированный узел может вести себя без какого-либо подозрения (сомнения в легитимности) в течение достаточно длительного периода времени или передавать ошибки, которые нелегко обнаружить.

Анализ рассмотренных сценариев сетевых атак противника показывает, что кардинальным решением проблемы выявления скомпрометированных узлов является постоянное наблюдение за сетевым трафиком, который может использоваться для получения решающей информации о состоянии любого узла, даже если содержание трафика неизвестно.

Структура сети легко раскрывается ее транспортным потоком. Для противника узлы, передающие и принимающие большие объемы данных, являются наиболее значимыми. При этом средствам разведки легче обнаружить узел передачи, чем узел приема, особенно если получатель не посылает подтверждения. Сетевая структура способна отображать структуру размещения войск (сил), облегчая противнику решение задачи обнаружения мест размещения командных пунктов и их уничтожения. Анализ трафика вполне может раскрыть намерения командования группировки войск (сил), а также уровень боевой готовности воинских формирований. Например, традиционно перед началом активных действий интенсивность обмена на информационных направлениях увеличивается, а слабо обученный персонал имеет тенденцию к более активному обмену.

Анализ и обобщение полученных результатов позволяет определить наиболее важные критерии безопасности телекоммуникационной сети:

– сеть должна быть в состоянии выполнить свои задачи, даже если она частично разрушена или подверглась нападению;

– если сеть частично разрушена, в резерве должны быть средства быстрого ее восстановления, исключающие полную потерю функциональных возможностей сети;

– сеть должна иметь трастовое управление, чтобы скомпрометированные узлы были своевременно обнаружены и исключены из информационного обмена;

– сеть не должна передавать информацию нелегитимным пользователям;

– сеть должна обеспечивать конфиденциальность, уровень которой гарантирует сохранение в тайне от противника сведений о боевом составе группировки войск (сил), ее действиях и намерениях, структуре системы управления. Противник может «видеть» сеть и даже иметь доступ к ней с целью перехвата информации, но при этом извлекать только минимум разведпризнаков, которые не влияют на структурную целостность системы управления.

Заключение

Телекоммуникационные сети весьма уязвимы для атак противника, а разные сценарии нападения на них отличаются по степени опасности и последствиям. Следует понимать, что информационные сети и системы военного назначения имеют свою специфику, которая обусловлена критическим характером и значительным масштабом последствий от снижения уровня защиты информации и безопасности связи.

PROVISION OF COMMUNICATIONS AND INFORMATION SECURITY IN CENTRIC NETWORK TROOPS CONTROL AND VARIOUS SCENARIOS OF ATTACKING TELECOMMUNICATIONS NETWORK

Yu.A. SEMASHKO, V.M. KALININ, V.N. SHEPTURA

Abstract

Place and role of telecommunications network as the basis of creating unique informative space in conducting centric network warfare is determined. Aspect of vulnerability of telecommunications networks to provide communications security and information protection is analyzed. The most scenarios of attacking network and their consequences are considered. The main requirements to communications security and information protection are formulated. General solution of the problem of creating stable to the attacks telecommunications network is suggested.

Список литературы

1. *Паршин, С. А., Горбачев Ю.Е., Кожанов Ю.А.*Современные тенденции развития теории и практики управления в вооруженных силах США. – М., 2009.

2. Теория управления в системах военного назначения / под ред. *И.В. Котенко.* М., 2001.

3. *Косачев И.М., Хижняк А.В.* // Вестн. Воен. акад. Респ. Беларусь. 2010. № 2 (27).

4. *Копытко В.К., Шептура В.Н.* // Военная Мысль. 2011. № 10. С. 16–26.

5. *Candolin C.* Securing military decision making in a Network-centric environment / Doctoral Dissertation, Helsinki University of Technology Department of Computer Science and Engineering Laboratory for Theoretical Computer Science. 2005.

6. *Candolin C., Kari H.* A security architecture for wireless ad hoc networks // In Proceedings of IEEE Milcom, Anaheim, California, USA. – 2002. – October 2002.

7. *Паршин С.А., Горбачев Ю.Е., Кожанов Ю.А.* Кибервойны – реальная угроза национальной безопасности? М., 2011.

8. *Alberts D., Garstka J., Stein F.* Network centric warfare – developing and leveraging information superiority. CCRP, 2-nd edition, 2000.

9. Новые сетевые технологии в системах управления военного назначения / Под ред. *Н. И. Буренина.* СПб., 2000.

10. *Белянский П.В.* Англо-русский словарь терминов и сокращений в современной военной технике связи. М., 2006.