Киберустойчивость информационно-телекоммуникационной сети

Коцыняк
Михаил Антонович,
профессор 32 кафедры
Военной академии связи им. С.М. Буденного,
д.т.н., профессор

Коцыняк
Михаил Михайлович,
заместитель начальника кафедры
Военной академии связи им. С.М. Буденного

Лаута
Олег Сергеевич,
преподаватель 32 кафедры
Военной академии связи им. С.М. Буденного

Лаута
Александр Сергеевич,
курсант Военной академии связи им. С.М. Буденного

Практика многих конфликтов современности позволяет рассматривать «цветные» революции в качестве важной составляющей войн нового типа, которые чаще всего определяются как гибридные войны. При подготовке гибридной войны ее участники заблаговременно объединяются в сеть, которая охватывает столицу, другие крупные города, а также регионы, имеющие природные ресурсы, и их воздействие первоначально направлено на информационно-телекоммуникационную сеть (ИТКС).

Гибридная война включает реализацию комплекса воздействий различного типа: дипломатические, экономические, военные и информационные операции.

В настоящее время воздействия на ИТКС военные специалисты США рассматривают как специфическую форму информационных операций (ИО). В соответствии с доктриной «Информационные операции» (JP 3–13) составляющими ИО являются: техническая разведка (ТР); сетевые операции (СО); радиоэлектронная борьба (РЭБ); огневое поражение (ОП); введение в заблуждение (ВвЗ) и психологические операции (ПсО), общая направленность которых свидетельствует о резком смещении акцентов на достижение интеллектуального и информационного превосходства над противником в рамках ведения информационного противоборства (ИП) [5].

Использование в ИТКС технологий, средств связи и программного обеспечения иностранного производства, интеграция ИТКС с сетью связи общего пользования (ССОП), а ССОП — с мировым информационным пространством, предопределили смещение акцентов на достижение превосходства над противником на основе применения компьютерных атак (КА).

Результатом воздействия КА являются блокирование управляющей информации и внедрение ложной информации, нарушение установленных регламентов сбора, обработки и передачи информации в автоматизированных системах управления, отказы, сбои в работе ИТКС, а также компрометация передаваемой (получаемой) информации. В этом случае, КА — один из основных факторов, определяющих устойчивость ИТКС.

По оценке зарубежных экспертов, эффект воздействия КА на ИТКС сравним с эффектом применения оружия массового поражения. По их мнению, эффективность таких воздействий прямо пропорциональна уровню технологического развития и масштабам использования компьютерной техники в системах управления государством и ВС. Влияние на ИТКС последствий применения противником КА при ведении ИП, а также отказов и сбоев аппаратно-программных средств по этой причине, приведет к существенному снижению устойчивости и, вследствие этого, к снижению эффективности информационного обмена между органами управления.

Прогнозируемый характер воздействия КА на ИТКС обусловливает необходимость рассмотрения четвертой составляющей устойчивости — кибер-устойчивости и совокупности новых требований, которым должны соответствовать показатели устойчивости ИТКС.

Под киберустойчивостью ИТКС понимается способность ИТКС поддерживать управление в условиях воздействия КА.

Учитывая требования нормативно-правовых документов, а также другие условия и факторы, влияющие на устойчивость ИТКС, можно сделать вывод о необходимости поиска новых подходов к оценке устойчивости ИТКС в условиях КА, т. е. киберустойчивости.

В настоящее время отсутствуют методики, позволяющие оценить киберустойчивость ИТКС. Для устранения этого пробела предлагается методика оценки киберустойчивости ИТКС, позволяющая определить показатели, характеризующие киберустойчивость ИТКС.

В качестве показателя, характеризующего киберустойчивость ИТКС, в методике используется коэффициент исправного действия ИТКС по киберустойчивости ($K_{\text{икуИТКС}}$), который показывает, какую часть времени от всего учитываемого ИТКС функционирует исправно.

С целью определения коэффициента исправного действия по киберустойчивости ИТКС сначала находятся коэффициент исправного действия по киберустойчивости j-го маршрута в условиях воздействия КА и вероятность воздействия на него. Для этого необходимо рассмотреть процесс функционирования ИТКС в условиях воздействия системы КА (рис. 1).

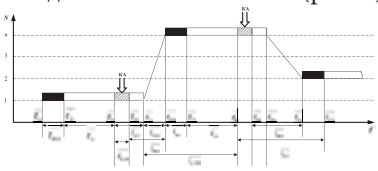

Рис. 1. Процесс функционирования ИТКС в условиях воздействия КА

В обобщенном виде процесс функционирования ИТКС в условиях воздействия КА можно представить следующим образом.

Для осуществления передачи оперативной информации ($\bar{t}_2$, $\bar{t}_7$, $\bar{t}_{12}$ и т.д.) сначала операторы ИТКС входят в связь ($\bar{t}_1$), на что затрачивается среднее время $\bar{t}_{\text{вх}}$.

С некоторого времени ($\bar{t}_3$, $\bar{t}_8$ и т.д.) система информационного воздействия реализует КА за среднее время $\bar{t}_{\text{КА}}$, которую оператор ИТКС сможет обнаружить ($\bar{t}_4$, $\bar{t}_9$ и т.д.) за среднее время $\bar{t}_{\text{ро}}$.

Обнаружив воздействие КА, оператор ИТКС будет принимать меры по восстановлению связи ($\bar{t}_5$, $\bar{t}_9$ и т.д.) за среднее время $\bar{t}_{\text{пер}}$.

После этого операторы ИТКС входят в связь ($\bar{t}_6$, $\bar{t}_{11}$ и т.д.), на что затрачивается некоторое среднее время $\bar{t}_{\text{вх}}$, и передача оперативной информации возобновляется.

Среднее время, затрачиваемое на принятие мер защиты, вхождение в связь, характеризует реакцию системы управления на воздействие системы КА, то есть $\bar{t}_{\text{рсу}}=\bar{t}_{\text{имз}}+\bar{t}_{\text{вх}}=\bar{t}_{\text{пер}}+\bar{t}_{\text{ро}}+\bar{t}_{\text{вх}}$.

Среднее время от момента принятия мер по восстановлению связи до момента воздействия системы КА назовем временем реакции комплекса компьютерной разведки (КР) ($\bar{t}_{\text{ркр}}$).

Тогда выражение для определения коэффициента исправного действия по киберустойчивости j-го маршрута можно записать

$$K_{\text{икуМ}j}=\frac{\bar{t}_{nj}}{\bar{t}_{nj}+\bar{t}_{\text{КА}j}}, \qquad (1)$$

а вероятность воздействия КА

$$P_{\text{возд}j}=1-\frac{\bar{t}^{2}_{\text{рКР}j}}{(\bar{t}_{\text{рКР}j}+\bar{t}_{\text{вх}j})\cdot(\bar{t}_{\text{рКР}j}+\bar{t}_{\text{пмз}j})}, \qquad (2)$$

где $K_{\text{иМ}j}$ — коэффициент исправного действия по киберустойчивости j-го маршрута;

$P_{\text{возд}}$ — вероятность воздействия КА на j-ый маршрут.

Так как маршрут передачи информации состоит из нескольких интервалов связи, то коэффициент исправного действия по киберустойчивости j-ого составного маршрута равен произведению коэффициентов исправного действия его интервалов

$$K_{\text{икуСМ}j}=\prod_{j=1}^{O}K_{\text{икуМ}j}, \qquad (3)$$

где $K_{\text{икуСМ}j}$ — коэффициент исправного действия по киберустойчивости j-го составного маршрута;

O — общее количество интервалов связи на j-ом маршруте.

Воздействие КА ($P_{\text{возд}}$) на отдельные маршруты направлений связи (НС) повлечет нарушение их функционирования и принятие мер по восстановлению нарушенных связей. С этой целью осуществляется поиск обходных маршрутов. Возможности по установлению соединений и передаче сообщений в случае выхода из строя элементов или целых участков характеризует связность НС и ИТКС ($K_{\text{св}}$), т.е. структурную живучесть. Одним из наиболее простых и удобных для оценки структурной живучести является линейный показатель связности, который определяется по формуле [3]

$$K_{\text{свНС}i}=\sum_{i=1}^{N}\alpha_{j}\cdot\left(\frac{H_j}{N+O}+\frac{O}{N}\right) \qquad (4)$$

где $K_{\text{свНС}i}$ — коэффициент связности i-го НС;

N — число маршрутов в НС;

H_j — ранг j-го маршрута;

$$\alpha_{ij}=\begin{cases}\dfrac{\gamma^{j}}{\gamma^{i}_{sum}} & \text{— вес } j\text{-го маршрута в информационном обмене } i\text{-го НС;}\\ \dfrac{\gamma^{i}_{sum}}{\gamma_{sum}} & \text{— вес } i\text{-го НС в информационном обмене ИТКС.}\end{cases}$$

Совокупность маршрутов образуют НС, а НС и средств вычислительной техники — ИТКС. Коэффициент исправного действия по киберустойчивости i-го НС может характеризоваться вероятностью сохранения на НС хотя бы одного маршрута и определяется по формуле

$$K_{\text{икуНС}i}=K_{\text{свНС}i}\cdot\left(1-\prod_{j=1}^{N}((1-K_{\text{икуСМ}j})\cdot P_{\text{возд}j})\right), \qquad (5)$$

где $K_{\text{икуНС}i}$ — коэффициент исправного действия по киберустойчивости i-го НС.

Учитывая, что ИТКС состоит из М НС, коэффициент исправного действия по киберустойчивости ИТКС определяется из выражения

$$K_{\text{икуИТКС}}=K_{\text{свИТКС}}\cdot\left(1-\prod_{i=1}^{M}(1-K_{\text{икуНС}i})\right), \qquad (6)$$

где $K_{\text{икуИТКС}}$ — коэффициент исправного действия по киберустойчивости ИТКС;

$$K_{\text{свИТКС}}=\sum_{i=1}^{M}\alpha_{i}\cdot\left(\frac{G_i}{M+N}+\frac{N}{M}\right)$$

G — ранг i-го НС;

M — количество НС в ИТКС.

Таким образом, для определения коэффициента исправного действия ИТКС первоначально требуется определить среднее время воздействия системы КА и комплекса компьютерной разведки, т.е. их вероятностно-временные характеристики (ВВХ). Для этого предлагается использовать профильные модели КА и метод топологического преобразования стохастических сетей (ТПСС). Примеры и порядок расчета ВВХ КА приведены в [1, 2, 4].

Используя эти вероятностно-временные характеристики, была получена зависимость коэффициента исправного действия по киберустойчивости ИТКС от количества маршрутов, представленная на рис. 2. В качестве исходных данных использовались следующие данные: α_i=1; $\bar{t}_{\text{вх}}$=3 мин; $\bar{t}_{\text{пер}}$=1 мин; $\bar{t}_{\text{ро}}$=2 мин; $\bar{t}_{\text{р КР}}$=10 мин; $\bar{t}_{\text{КА}}$=13 мин.

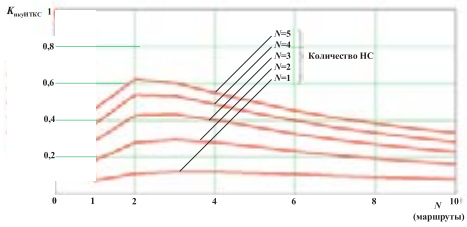

Рис. 2. Зависимость коэффициента исправного действия ИТКС от количества маршрутов и НС

Полученная зависимость коэффициента исправного действия по киберустойчивости ИТКС от количества маршрутов позволяет определить рациональный диапазон количества потребных маршрутов при воздействии КА. Анализ показал, что коэффициент исправного действия принимает оптимальное значение при использовании для передачи информации от 2 до 5 маршрутов в зависимости от количества направлений связи в ИТКС, что показывает необходимость перехода от распределенной структуры ИТКС к «звезде». Кроме того, маршруты, образованные радиосредствами, обладают наибольшей оперативностью, в связи с чем коэффициент исправного действия принимает максимальное значение.

Таким образом, предлагаемая методика позволяет оценивать киберустойчивость ИТКС. Результаты оценки позволят обосновать требования к топологии ИТКС и к выбору средств и способов ее защиты от системы КА.

Список используемых источников:

1. Лаута О.С., Коцыняк М.А., Кулешов И.А. Вероятностно-временные характеристики компьютерной атаки типа «Перенаправление пакетов данных».// Труды XII Российской научно-технической конференции Калуга, 2013 – Калуга: Изд. ООО «Новосфера», 2013, С. 149-154.
2. Лаута О.С., Коцыняк М.А., Осадчий С.А. Вероятностно-временные характеристики компьютерной атаки типа «Анализ сетевого трафика».// Юбилейный журнал «Информация и космос», 2014, С. 56-61.
3. Колесников А.А. Оптимизация структур сетевых моделей - Л.: ВАС, 1987. – 101 стр.
4. Коцыняк М.А., Кулешов И.А., Лаута О.С. Устойчивость информационно-телекоммуникационных сетей– С-Пб.: Издательство Политехнического университета, 2013 – 93 стр.
5. Joint Publication JP 3-13 – Information Operation. Joint Chiefs of Staff. 13 February 2006.