УДК 681.324

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ВОЗДЕЙСТВИЯ НАРУШИТЕЛЯ НА ИНФОТЕЛЕКОММУНИКАЦИОННУЮ СИСТЕМУ

Гужва Д. Ю. – канд. техн. наук, ст. инспектор (ВАС)

В инфотелекоммуникационных системах в целях обеспечения повышенных требований по защите информации возникает необходимость расширения традиционной концептуальной системы нарушителя. Дополнительно учитываемыми способами несанкционированного доступа следует считать программные атаки и компьютерную разведку. Предлагаемая концептуальная модель охватывает эти способы и с необходимой полнотой описывает процесс воздействия нарушителя на инфотелекоммуникационную систему.

In info telecommunication systems, there is a need to expand the traditional concept of wrongdoing in order to ensure increased requirements for data protection. Computer software attack and computer intelligence should be considered as ways for unauthorized access. The proposed conceptual model covers these ways and with the necessary completeness describes the impact of the wrongdoing on an infotelekommunication system.

Ключевые слова: защита информации, несанкционированный доступ, инфотелекоммуникационная система, информационный конфликт, программная атака, нарушитель.

Синтез эффективных систем защиты информации (СЗИ) от несанкционированного доступа (НСД) любых автоматизированных систем (АС), включая современные и перспективные инфотелекоммуникационные системы (ИТКС), требует разработки соответствующих моделей нарушителя. На концептуальном уровне относительно ИТКС такая модель излагается ниже.

В соответствии с руководящими документами ФСТЭК [1, 2] в качестве нарушителя, действия которого направлены на НСД к информации, обрабатываемой в АС, рассматривается субъект, имеющий доступ к работе со штатными средствами системы. Выделяются следующие четыре уровня функциональных возможностей нарушителя, причем более высокий уровень включает в себя функциональные возможности предыдущего:

1) уровень *ведения диалога* в АС, т.е. запуска задач (программ) из фиксированного набора, реализующего заранее предусмотренные функции по обработке информации;

2) уровень *создания и запуска собственных программ*, обладающих новыми функциями по обработке информации;

3) уровень *управления функционированием* АС;

4) уровень *проектирования, реализации и ремонта* технических средств АС, включая собственные технические средства с новыми функциями по обработке информации.

Для каждого уровня нарушитель является специалистом высшей квалификации, знающим все об АС и, в частности, о системе и средствах ее защиты.

Руководящими документами определены способы НСД:

1) *непосредственное обращение* к объектам доступа (ОД), регламентируемое *правилами разграничения доступа*;

2) *создание программных и технических средств*, выполняющих обращение к объектам доступа в обход средств защиты;

3) *модификация средств защиты*, позволяющая нарушителю осуществить НСД к информации;

4) *внедрение* программных и технических *механизмов*, нарушающих структуру и функционирование АС.

Применение подобной модели нарушителя в отношении к ИТКС, функционирующей в условиях информационного конфликта, имеет, на наш взгляд, следующие ограничения:

1) в условиях информационного конфликта в качестве нарушителя наряду с авторизованными или «внутренними» субъектами доступа (СД), действующими в интересах противоборствующей стороны, могут выступать «внешние» злоумышленники, не обладающие в начальный момент времени правами СД и решающие путем программных атак задачу получения таких прав;

2) цели нарушителя в условиях информационного конфликта могут изменяться в зависимости от результатов взаимодействия с СЗИ и быть направлены на НСД как к оперативной, так и к технологической информации, обрабатываемой в ИТКС, для ее программного подавления;

3) реализация НСД к информации в ИТКС осуществляется противоборствующей стороной путем последовательных фаз сбора и анализа данных о структуре и параметрах СЗИ и включает этапы компьютерной разведки, преодоления СЗИ и непосредственного НСД, реализуемого в форме нарушения конфиденциальности, целостности или доступности информации как составляющих информационной безопасности;

4) программные атаки являются основной формой воздействия на ИТКС и осуществляются в виде планомерных, взаимосвязанных, распределенных и скоординированных воздействий;

5) взаимодействие СЗИ ИТКС и нарушителя по своей природе является динамическим процессом.

Перечисленные факторы определяют необходимость расширения традиционной концептуальной модели нарушителя. Для отражения в модели возможностей «внешнего» воздействия на ИТКС и СЗИ ИТКС посредством программных атак предлагается ввести нулевой уровень – сетевого взаимодействия нарушителя с АС. Кроме того, дополнительно к перечисленным выше способам НСД необходимо ввести следующие способы нарушения безопасности информации, соответствующие понятиям «компьютерная разведка» и «программное подавление»:

1) сбор данных о структуре и параметрах ИТКС и СЗИ ИТКС для реализации на их основе программных атак, обеспечивающих возможность получения НСД к информации в приемлемые сроки;

2) нарушение работоспособности ИТКС и СЗИ ИТКС путем генерации сетевого трафика, подавляющего защищенный обмен данными между удаленными узами или абонентами ИТКС.

Концептуальная модель воздействий нарушителя на ИТКС в общем случае включает следующие компоненты:

1) систему классификации программных атак;

2) модель зависимости мощности совокупности программных атак от уровня информированности нарушителя;

3) принципы реализации воздействий нарушителя на информационные ресурсы ИТКС;

4) граф состояний и переходов системы информационных воздействий нарушителя (СИВН);

5) множество характеристик описания процесса воздействий нарушителя, потенциально доступных для наблюдения.

Система классификации программных атак представлена на рис. 1.

В качестве признаков классификации выступают:

цель воздействия (реализация одной или нескольких угроз нарушения безопасности информации);

размещение источника атаки по отношению к ИТКС;

принадлежность к этапу реализации НСД;

характер взаимодействия с объектом атаки;

компонентная направленность воздействия;

тип связи с источником атаки;

тип средств обеспечения атаки.

Предложенная система объединяет как известные [3–6], так и новые классификационные признаки. В качестве примера рассмотрим классифика-

ционную характеристику программных атак сетевого сканирования как наиболее распространенного в ИТКС типа.

Атаки сетевого сканирования относятся к этапу компьютерной разведки. Их результат может быть использован для осуществления любой из угроз нарушения безопасности информации. Реализация подобных атак связана с использованием сервиса сетевых служб и протоколов и зондированием объекта атаки (посылкой запросов и анализом результатов их выполнения). Они относятся к классу удаленных, активных атак с каналом обратной связи, воздействующих на сетевую составляющую ИТКС.

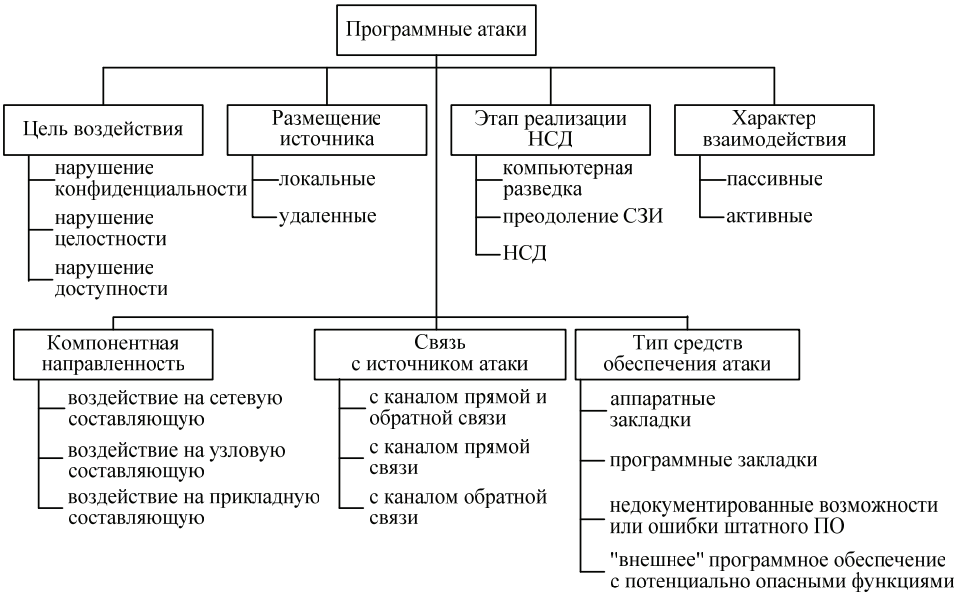

Рис. 1 Система классификации программных атак

Анализ известных прецедентов нарушений безопасности в ИТКС позволяет сделать вывод, что наиболее вероятными и результативными являются комплексные воздействия, включающие совокупность атак различных классов, объединенных единым сценарием, выполнение которого предполагает последовательное воздействие на различные компоненты ИТКС. В качестве последних, основываясь на связи классов атак с уровнями эталонной модели взаимодействия систем, могут быть выделены сетевые, узловые и прикладные компоненты.

Проведение атаки того или иного вида на один из выделенных компонентов предполагает определенный уровень знаний нарушителя о структуре и параметрах ИТКС, включая СЗИ. Кроме того, необходимо наличие некоторого минимального уровня знаний о коммуникационной среде и протоколах физического и канального уровней. Получение такой дополнительной ин-

формации связано с последовательным пассивным или активным воздействием на компоненты ИТКС, т.е. с проведением атак компьютерной разведки. С позиций теории информации это означает, что эффективность очередного этапа комплексной атаки определяется апостериорной информацией, полученной на предыдущих этапах, и **мощностью множества программных атак**, реализуемых при данном уровне информированности СИВН (рис. 2).

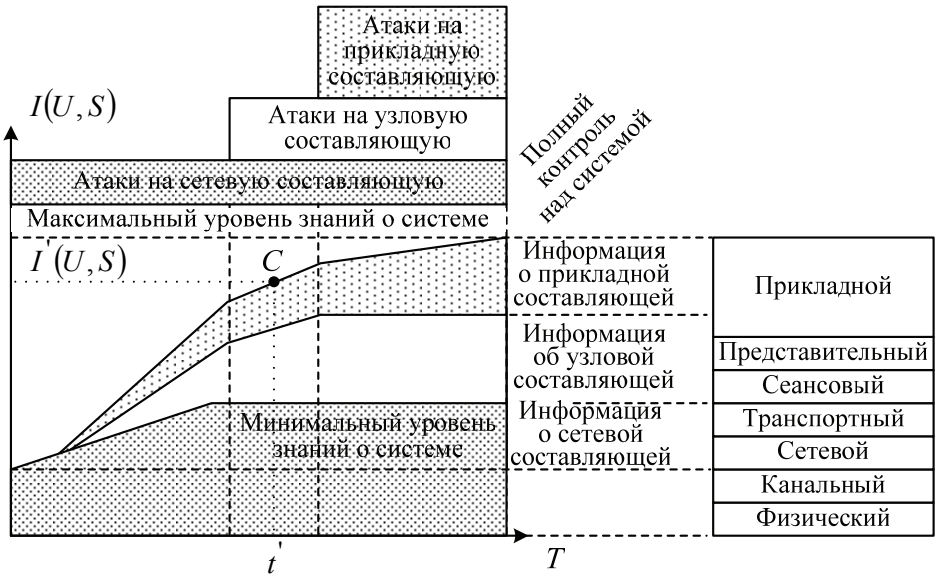

Рис. 2. Модель зависимости мощности множества программных атак от уровня информированности нарушителя

Проведенный анализ и классификация программных атак позволяют выделить следующие **принципы реализации воздействий нарушителя** на ресурсы ИТКС:

1) поэтапное проведение;

2) информационная связность;

3) компонентная направленность;

4) целевая, информационная, временная и структурная оптимальность общей стратегии воздействия;

5) соответствие требуемых ресурсов выбранной стратегии воздействия ее потенциальным результатам.

На рис. 3 показан **граф состояний и переходов** СИВН в процессе информационного конфликта, в соответствии с которым выделены состояния ведения компьютерной разведки, преодоления СЗИ и осуществления НСД в форме непосредственного доступа к защищаемой информации или программного подавления ИТКС.

Времена пребывания СИВН в каждом из состояний и вероятности переходов в другие состояния в ходе конфликтного взаимодействия должны изменяться. В результате матрицы вероятностей переходов графа могут существенно отличаться друг от друга в различные моменты времени.

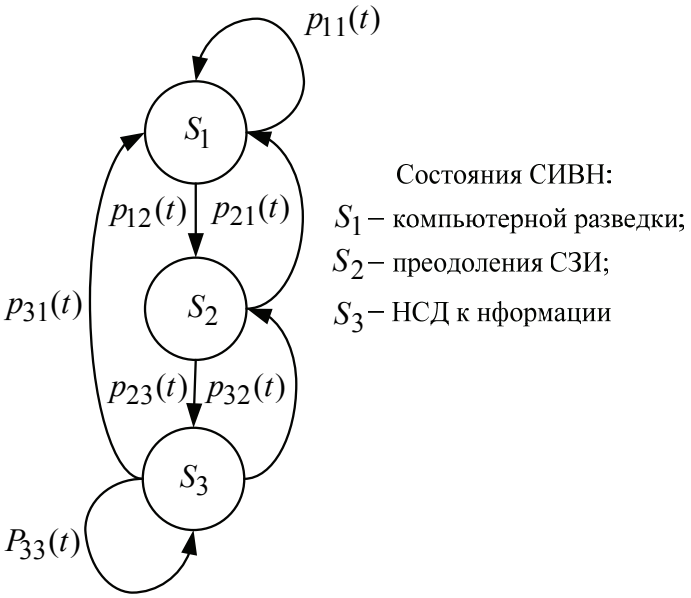

Рис. 3. Граф состояний и переходов СИВН в процессе конфликта

Множество характеристик описания процесса воздействий нарушителя предлагается представить в виде

$$U = \left\{(u_1^{\text{кр}},...,u_{N_{\text{кр}}}^{\text{кр}}),(u_1^{\text{пз}},...,u_{N_{\text{пз}}}^{\text{пз}}),(u_1^{\text{нсд}},...,u_{N_{\text{нсд}}}^{\text{нсд}})\right\},$$

где $u_1^{\text{кр}},..., u_{N_{\text{кр}}}^{\text{кр}}$, $u_1^{\text{пз}},...,u_{N_{\text{пз}}}^{\text{пз}}$, $u_1^{\text{нсд}},..., u_{N_{\text{нсд}}}^{\text{нсд}}$ – подмножества характеристик программных атак различных классов; $N_{\text{кр}}, N_{\text{пз}}, N_{\text{нсд}}$ – число типов атак компьютерной разведки, преодоления СЗИ и НСД соответственно.

В свою очередь, каждое подмножество $u_i \in U$ имеет следующие характеристики:

$\hat{\tau}_i$ – оценка интервала времени между последовательным наблюдением значений признаков идентификации атаки i-го типа;

$\hat{T}_i$ – оценка времени реализации атаки i-го типа;

$\hat{V}_i$ – оценка величины потенциального "ущерба" пользователям ИТКС в случае реализации атаки i-го типа.

Вероятностный характер информационного конфликта обусловливает случайный характер $\hat{\tau}_i$, $\hat{T}_i$ и $\hat{V}_i$, что приводит к необходимости использовать для их описания вероятностные характеристики. В качестве последних могут выступать законы распределения или моменты соответствующих величин.

Задача определения типа и характеристик наблюдаемого воздействия нарушителя решается в процессе идентификации состояний ИТКС с помощью СЗИ и может быть сформулирована в рамках теории распознавания образов. Для описания программных атак как объектов распознавания введем пространство признаков Ω как множество, включающее в себя следующие элементы:

– алфавит признаков $R_\Omega = \{r_1,...,r_j,..., r_{N_R}\}$, где r_j – j-й признак идентификации типа атаки, N_R – число признаков;

– алфавит значений признаков $\mathrm{A}_\Omega = \{\alpha_1,...,\alpha_j,...\alpha_{N_R}\}$, где α_j – диапазон (множество возможных значений) j-го признака.

Главной особенностью процесса идентификации состояний ИТКС в условия информационного конфликта является возможность получения СЗИ неполной или непротиворечивой информации о характеристиках наблюдаемых воздействий. Это обусловлено наличием фактора неопределенности при принятии решении о текущем состоянии ИТКС. В качестве основных причин неопределенности могут выступать:

– отсутствие априорных данных о возможных типах и параметрах воздействий;

– ошибки, вызванные недостаточными техническими возможностями СЗИ, приводящие к неполноте, неточности или противоречивости регистрации данных о наблюдаемом воздействии;

– модификация алгоритмов реализации программных атак или маскирование их под легальные процессы с целью обхода КСЗ.

Таким образом, предложенная в настоящей статье концептуальная модель нарушителя с необходимой полнотой описывает процесс его воздействия на ИТКС. При этом данный процесс следует рассматривать как процесс последовательного наблюдения признаков, несущих определенное количество информации о типе воздействия (программных атаках).

Библиографические ссылки

1. *Концепция* защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. М., 1992.

2. *Временное* положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционирован-

ного доступа в автоматизированных системах и средствах вычислительной техники // Сборник руководящих документов по защите информации от несанкционированного доступа. М., 1998.

3. *Алгулиев Р. М.* Угрозы корпоративным сетям и формализация их отношений с системами защиты. Баку, 2000.

4. *Гриняев С. Н.* Интеллектуальное противодействие информационному оружию. М., 1999.

5. *Зима В. М., Молдовян А. А., Молдовян Н. А.* Безопасность глобальных сетевых технологий. СПб., 2000.

6. *Лукацкий А. В.* Обнаружение атак. СПб., 2001.