УДК 519

Г.Н. Гудов[1], О.С. Купач[2]
([1]РГГУ, [2]4 ЦНИИ МО России; e-mail: goodov4747@mail.ru)

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ДЕЙСТВИЙ "НАРУШИТЕЛЯ" ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Проведена формализация процесса обеспечения информационной безопасности на основе анализа действий "нарушителя".

Ключевые слова: безопасность информации, источники угроз, нарушитель.

G.N. Gudov, O.S. Kupach

A MATHEMATICAL MODEL OF ACTIONS "OFFENDER" OF INFORMATION SECURITY

The formalization of process ensuring of information security based on the analysis of actions of "offender".

Key words: information security, sources of threats, the offender.

Статья поступила в редакцию Интернет-журнала 27 февраля 2014 г.

Основной подход к обеспечению информационной безопасности сложной системы – интеллектуализация такой системы, то есть оснащение системы элементами интеллекта, создание у неё специального информационно-программного окружения, обеспечивающего информационную безопасность этой системы на протяжении всего её жизненного цикла [1]. Такое оснащение должно обеспечивать постоянную адаптацию сложной системы к изменяющимся внутренним и внешним условиям, проводить диагностику, контроль, анализ и синтез отдельных составляющих системы и функционирования системы в целом [2].

Как показывают данные, приводимые в технической литературе, большинство угроз безопасности информации (до 70-80 %) исходят от человека [3]. Криминальные структуры, фирмы-конкуренты активно вербуют работников предприятий. Согласно опубликованным статистическим данным, более 70 % утечек информации приходится на долю персонала, имеющего к ней непосредственный доступ [3]. Это свидетельствует о том, что в современных условиях одним из главных направлений по обеспечению безопасности информации должна быть работа с персоналом, который имеет доступ к защищаемой информации.

В технической литературе приводятся работы по моделированию поведения нарушителей безопасности информации описательного характера или с использованием математической модели возникновения нарушений безопасности информации [4, 5].Обобщение результатов моделирования по данной тематике позволяет сделать следующие выводы:

- описываются нарушения информационной безопасности, которые могут возникнуть на рассматриваемом объекте;

- описываются методы, способы и технические средства нарушения информационной безопасности, а также методы, способы и технические средства защиты от этих нарушений без учёта классификации нарушителя и последовательности возникновения нарушений и жизненного цикла системы безопасности информации;

- математические модели описывают вероятность возникновения нарушений применительно к определённому типу объекта (то есть с определённой технической конфигурацией).

Ниже рассматривается система, состоящая из технической подсистемы, подсистемы персонала, внешней среды.

Объект исследования: возникновение (совершение) нарушения безопасности информации в зависимости от состоянии защищённости объекта.

Предмет исследования: зависимость поведения нарушителя от параметров, влияющих на состояние системы информационной безопасности.

Цель исследования: оценка эффективности системы защиты информации или достаточности принятых мер для исключения нарушений информационной безопасности.

Задачи:

1. Определить основные этапы нарушений (как последовательность событий);

2. Определить вероятность перехода нарушителя с одного этапа на другой при нарушениях информационной безопасности (для определения слабого звена в системе обеспечения безопасности);

Вероятность совершения событий на каждом этапе должна зависеть от типа нарушителя и состояния системы защиты информации на объекте.

Для решения вышеуказанных задач исследованы:

- последовательность событий при нарушениях безопасности информации;
- вероятность перехода нарушителя с этапа на этап;

Рассмотрен пример результатов анализа состояния защиты информации на объекте.

Представленная модель нарушений информационной безопасности является универсальной и одинакова для описания событий совершения нарушений как для должностных лиц, имеющих допуск к защищаемой информации, так и для иных лиц, не имеющих допуска к защищаемой информации, с учётом типа нарушителя и состояния защиты информации на объекте.

Нарушителями будем называть персонал, который своими действиями или бездействием случайно или преднамеренно нарушил состояние информационной безопасности. Любое правонарушение совершается не сразу и состоит из последовательности событий, которые между собой связаны определенной зависимостью.

Можно выделить три этапа нарушений безопасности информации:

1. Предпосылки к возникновению нарушений (дестабилизирующие факторы) – на нарушителя действуют факторы, подталкивающие его на совершение правонарушения;

2. Нарушения состояния информационной безопасности – нарушитель осознанно или неосознанно нарушает требования режима конфиденциальности и защиты информации ведомственных нормативных документов или законодательных нормативных актов;

3. Ликвидация последствий нарушений (восстановление состояния информационной безопасности) – проводится расследование по выявлению нарушителя, определяются места взлома (обхода) средств защиты, способы, методы нарушений, принимаются меры по уменьшению ущерба от нарушений, производится восстановление элементов системы защиты информации.

I. *Этап предпосылки к нарушению безопасности информации*

На этом этапе возможна следующая последовательность событий:

- ***возникновение причин*** (мотивов), побуждающих (толкающих) к совершению правонарушений;

- ***наличие обстоятельств,*** которые создаёт сам "нарушитель";

- ***создание условий***, которые существуют на объекте защиты или создаются должностными лицами по незнанию или осознанно, влияющих на нарушение безопасности.

II. *Этап нарушения безопасности информации*

Данный этап является основным в действиях нарушителя, который требует более детального описания его составляющих. Здесь выделяется следующая последовательность совершения подэтапов событий.

1. *Появление угрозы*

На данном подэтапе нарушителя будем называть злоумышленником.

Злоумышленник – человек, намеренно идущий на нарушение из корыстных побуждений и/или, выполняющий чьи-либо преступные указания, который еще не совершил действий, приведших к нарушению характеристик информационной безопасности, но имеет намерения и подготавливается к совершению преступления или готовит к совершению иных лиц. Нарушитель не нарушил требований закона Российской Федерации и/или требований ведомственных нормативных документов общества, организаций. Злоумышленник проводит предварительный анализ своих возможностей, с учётом ожидаемой выгоды, готовит преступление. Например, злоумышленник добывает сведения об организации, характере производственной деятельности, его возможности по производству и реализации продукции, расположение зданий, планировку территории поэтажного плана и т.п.

2. ***Подготовка нарушения безопасности информации***

На этом подэтапе будем называть правонарушителем.

Правонарушитель – лицо, выполняющее конкретные действия, которые нарушают требования нормативных документов или законодательных актов либо должностное лицо своими действиями или бездействиями совершает правонарушения (ошибочно, случайно, по незнанию или иным причинам). На данном подэтапе правонарушитель ищет возможные пути нарушения безопасности инфорррмации. Основное усилие его направлено на сбор сведений о защите объекта, выявление слабых мест (с учётом имеющихся знаний и опыта), планирование действий (выбор способов и методов реализации замысла).

3. ***Нарушение безопасности информации***

На этом подэтапе нарушитель делает конкретные противоправные действия для преодоления средств защиты. Если нарушителю удаётся реализовать замысел, что нанесло ущерб безопасности информации, он (по решению суда) признаётся ***преступником*** и ему определяют меру наказания.

III. ***Этап ликвидации последствий происшествий***

На этом этапе происходит последовательность событий, направленных на восстановление состояния информационной безопасности, с наименьшим возможным ущербом для объекта защиты.

Описанную последовательность событий можно представить в виде математической модели дискретного марковского случайного процесса с непрерывным временем. Систему можно представить в формализованном виде (рис. 1).

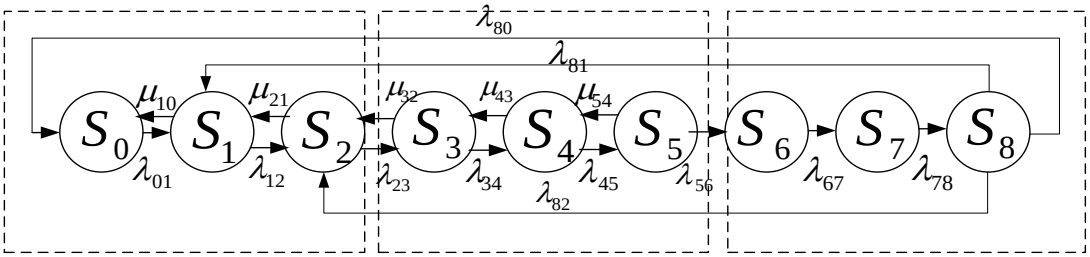

Рис. 1. Формализованная схема этапов реализации угрозы безопасности информации:

S_i, $i = \overline{0, 8}$ – это состояния системы, соответствующие схеме этапов нарушения безопасности информации;

λ_{ij}, μ_{ji} – интенсивности переходов из одного состояния в другое

После решения системы уравнений (учитывая ограничение – сумма вероятностей состояний системы должна быть равной единице) получим финальные вероятности нахождения системы в одном из состояний. Физический смысл интенсивностей переходов заключается в количестве совершённых действий за промежуток времени (например, количество преступлений за год).

Интенсивность перехода мы определяем для конкретного объекта в зависимости от состояния системы защиты информации.

Вероятность нахождения системы на определённом этапе нарушения информационной безопасности мы определяем с использованием уравнения Колмогорова.

Изменяя интенсивности переходов, система будет изменять вероятности состояний, в которых она находится.

Пример решения уравнений Колмогорова в среде Mathcadc заданными коэффициентами интенсивности перехода (λ_{ij}, μ_{ji}) в случаях непреднамеренных действий внутренним нарушителем – блокировка доступа к информации:

1. Проводится анализ правонарушений и преступлений на каждом этапе нарушения безопасности информации.

2. Определяется коэффициент интенсивности перехода λ, μ для каждого этапа нарушения безопасности информации.

3. Коэффициент интенсивности переходов для рассматриваемого объекта определяется на основании оценки экспертов (специалистов в области информационной безопасности) в зависимости от совершенного события, явления, фактора на каждом этапе.

4. Вероятность нахождения системы на определённом этапе определяем с использованием уравнения Колмогорова

Изменение интенсивности переходов будет изменять вероятность состояния, в котором она находится.

Для практического применения эвристических математических моделей поведения нарушителя необходимо конкретизировать исходные данные и уточнить методику сбора и обработки исходных данных для защищаемого объекта.

Выводы

1. Математическое моделирование поведения нарушителя в социотехнической системе, является важным инструментом в решении теоретических и прикладных задач при создании системы защиты информации.

2. Предложенная в данной работе формализация последовательности событий в виде математической модели дискретного марковского случайного процесса с непрерывным временем позволит описывать поведение нарушителя с расчётом вероятностей событий в зависимости от состояния защищенности объекта.

3. Использование разработанной математической модели при уточнении исходных данных и коэффициентов перехода позволяет определить вероятность правонарушения (преступления) на объекте защиты.

4. Предлагаемый подход к формализации проблемной области позволит прогнозировать события на этапах нарушения безопасности, выявлять слабое звено в системе безопасности информации на объекте.

Литература

1. ***Чечкин А.В., Пирогов М.В.*** Активаторы и регуляторы среды радикалов // Нейрокомпьютеры: разработка, применение. 2012. № 5.

2. ***Чечкин А.В., Пирогов М.В.*** Метод интеллектуализации критических систем с использованием таблиц радикалов // Нейрокомпьютеры: разработка, применение. 2012. № 2.

3. ***Васильев С.Н., Жерлов А.К., Федосов Е.А., Федунов Б.Е.*** Интеллектное управление динамическими системами. М.: Физматлит, 2000. 352 с.

4. ***Петросян Д.С.*** Концептуальные и математические модели поведения человека как экономического агента // Аудит и финансовый анализ. 2009. № 1.

5. ***Бабкин В.В.*** Модель нарушителя информационной безопасности – превенция появления самого нарушителя // Управление в кредитной организации. 2006. № 5.

6. ***Рожнов А.В., Белавкин П.А., Купач О.С., Лобанов И.А.*** Обоснование метода построения рациональной иерархии и стратифицированной модели проблемно-ориентированной системы управления в условиях неполноты исходных данных // Шестая всероссийская мультиконференция по проблемам управления. 2013. Т. 4.

7. ***Язык*** схем радикалов: методы и алгоритмы / Под ред. А.В. Чечкина и А.В. Рожнова. Коллективная монография. Ч. I. М.: Радиотехника, 2008.

8. ***Герасименко В.А.*** Защита информации в автоматизированных системах обработки данных. М.: Энергоиздат, 1994. 400 с.

9. ***Кривоножко В.Е., Рожнов А.В., Лычев А.В.*** Построение гибридных интеллектуальных информационных сред и компонентов экспертных систем на основе обобщённой модели анализа среды функционирования // Нейрокомпьютеры: разработка, применение. 2013. № 6.