Алгоритм раннего обнаружения атак на информационные ресурсы АСУП

Л.М. Груздева, М.Ю. Монахов (ВлГУ)

Предложена модель организации защитных механизмов в распределенной информационной системе, реализация которой позволяет улучшить временные и вероятностные характеристики систем защиты. Наряду с этим предложен новый алгоритм обнаружения атак на ресурсы ИС, основанный на понятии критической области угроз.

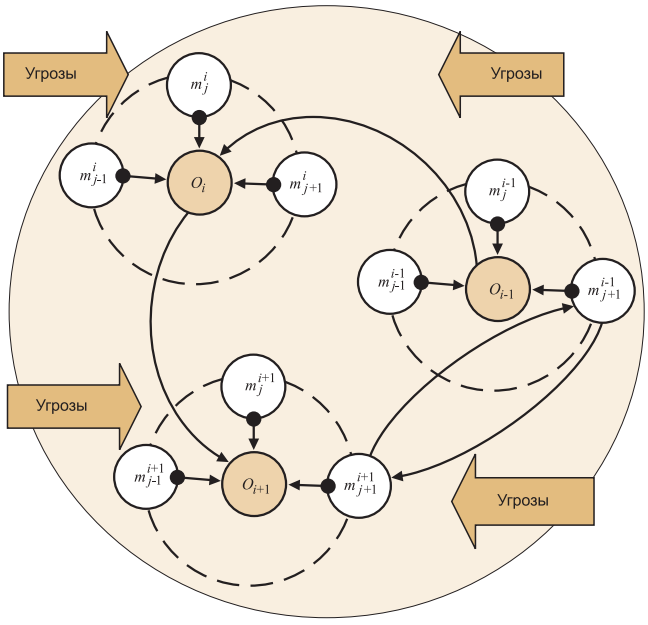
Введение

Технологической основой современных АСУП является распределенная информационная система (ИС). Распределенная обработка в АСУП обладает несомненными достоинствами, такими как открытость, малое время отклика, высокая доступность, возможность совместного использования ресурсов, инкрементального наращивания мощности как системы в целом, так и ее компонентов.

Тем не менее, эти качества порождают и уязвимости, среди которых важнейшая – слабая защита от вредоносных программ. В АСУП выстраиваются различные системы защиты, включающие аппаратные и программные средства, но всегда существует вероятность поражения ресурсов ИС, которая влечет за собой как минимум снижение качества функционирования всей системы. Обозначенная проблема приобретает особую актуальность при интеграции АСУП и АСУТП в единую систему [1]. Такая интеграция потенциально обеспечивает доступ внешнего злоумышленника к производству.

Быстрый рост числа вирусных эпидемий, громкие атаки хакеров, сетевое мошенничество, угроза spyware привели к необходимости продумывания мер, способных обеспечить адекватную защиту ИС от вредоносных программ. Разработанные и внедренные в настоящее время модели защиты, построенные на основе классических и проактивных технологий, не удовлетворяют заявленным требованиям. По оценкам антивирусных экспертов даже самые современные эвристические анализаторы не способны остановить более 30% вредоносных кодов, имея при этом большое число ложных срабатываний [2]. Существующие системы защиты не могут гарантировать даже 70% детектирования вирусов, но и создание универсального противоядия от всех возможных в будущем угроз в принципе невозможно [3].

Рассмотрим модель организации защитных механизмов в ИС, позволяющую одновременно использовать различные технологии обнаружения и отражения атак злоумышленников на ресурсы, и алгоритм обнаружения атаки, основанный на понятии критической области угроз. Реализация модели позволяет уменьшить время обнаружения атаки и добиться лучшего соотношения между вероятностью обнаружения и частотой генерации "ложной тревоги" системы защиты в целом.



Модель организации защитных механизмов в распределенной ИС

Описание модели

Под атакой на ресурсы ИС будем понимать попытку реализации угрозы или ряда угроз злоумышленником.

Рассмотрим модель организации защитных механизмов в распределенной ИС, которую для наглядности представим в виде ориентированного графа (рисунке). Вершины графа – объекты защиты (защищаемые ресурсы и процессы ИС, множество О) и модули защиты (совокупность средств обнаружения (СО) и средств отражения или уничтожения ($СО_{тр}$), множество М). Дуги (связи) графа – возможные пути атаки угроз.

Кольцом защиты объекта O_i будем называть совокупность модулей защиты (m^i_{j-1}, m^i_j, m^i_{j+1}), число и состав которых зависит от характеристик объекта защиты. Для эффективной работы кольца защиты с течением времени должны претерпевать модернизацию в связи с изменением самих объектов ИС.

Для обеспечения защиты от различных видов угроз в каждом кольце защиты одновременно может функционировать несколько модулей, включающих различ-

ные СО. При этом каждое СО характеризуется вероятностью обнаружения угроз определенного типа. Примерами СО могут являться антивирусные пакеты программ (Dr.Web, Антивирус Касперского и т.п.), межсетевые экраны, системы сканирования сетевого трафика, управления вычислительными сетями, множество других программных средств и даже оператор ЭВМ, контролирующий работоспособность системы.

В процессе проектирования колец защиты решается задача комбинирования различных СО. При этом должны выполняться следующие условия:

1. возможность совместной работы объединяемых средств обнаружения;
2. обеспечение скорости работы кольца защиты не ниже требуемой;
3. обеспечение заданной вероятности обнаружения нарушений за счет использования нескольких СО, построенных на различных принципах, имеющих общую зону обнаружения и совпадающие характеристики объекта обнаружения;
4. снижение средней частоты ложных тревог, вызываемых различными помехами.

Кроме этого, необходима выработка метода объединения сигналов от нескольких СО, образующих кольца защиты, для принятия решения о наличии атаки в системе.

Алгоритм обнаружения атаки

В [4] предложены алгоритмы решения данной задачи, основанные на логической обработке бинарных сигналов тревоги от отдельных СО, достоинством которых является простота. Однако отсутствие учета индивидуальных особенностей и характеристик каждого отдельно взятого СО не позволяет добиться наилучшего соотношения между вероятностью обнаружения и частотой генерации "ложной тревоги" кольца защиты в целом.

Другим подходом к объединению результатов работы различных СО является способ обнаружения атаки, построенный на анализе статистических данных.

В общем случае атака состоит в реализации нескольких угроз, каждая из которых может быть обнаружена или нет СО, входящими в состав кольца защиты. Пусть кольцо защиты включает n СО, каждое из которых вырабатывает сигнал X_k $(k = 1,2,...,n)$ о наличие j угрозы. Случайные величины (СВ) X_k, принимают значения: 1 – угроза обнаружена; 0 – угроза не обнаружена. Независимые СО обладают разными значениями вероятности обнаружения и вероятности "ложной тревоги", данное обстоятельство будем учитывать при формировании общего сигнала кольца защиты.

Ситуацию можно трактовать так: имеется СВ X_0, которая принимает значение 1, если атака есть и 0 в противном случае. Предметом нашего внимания является распределение многомерной СВ $(X_0, X1, ..., X_n)$.

Таблица

x_0	x_1	x_2	x_3	$p(x_0, x)$
1	0	0	0	0,03
1	0	0	1	0,02
1	0	1	0	0,1
1	0	1	1	0,2
1	1	0	0	0,05
1	1	0	1	0,15
1	1	1	0	0,02
1	1	1	1	0,03
0	0	0	0	0,08
0	0	0	1	0,04
0	0	1	0	0,02
0	0	1	1	0,1
0	1	0	0	0,09
0	1	0	1	0,02
0	1	1	0	0
0	1	1	1	0,05

Введем следующие обозначения: x_0 – показатель, принимающий значения 0 или 1 (реализация X_0); $x = (x_1, x_2, ..., x_n)$ – система показателей, где x_k так же принимает одно из двух значений; S – множество всех наборов x, состоящее из $N = 2^n$ элементов; S^* – критическая область угроз (КОУ), такая что, если $x \in S^*$, то атака существует, иначе – атака отсутствует, при этом $S^* \subset S$.

Статистическая функция $P = p(x_0, x1, ..., x_n)$, где значения p – это относительные частоты появления кода $(x_0, x_1, ..., x_n)$ позволяет определить КОУ. Таким образом, $0 \le p \le 1$ и сумма $p(x_1, x_2, ..., x_n)$ по всем кодам равна 1. Выборочный закон распределения СВ X_0, в частности, имеет вид: значению $X_0 = 0$ соответствует вероятность q_0, значению $X_0 = 1$ – вероятность p_0, где

$$p_0 = \sum_{x \in S} p(1; x); \quad q_0 = 1 - p_0 .$$

Одним из основных является вопрос, как на основании показаний средств обнаружения X_k определить, есть атака или нет. В рамках традиционного подхода он может быть решен следующим образом [5]. Пусть, например, основная гипотеза H_0 заключается в том, что атаки нет $(X_0 = 0)$, тогда H_1 – альтернативная гипотеза означает, что атака есть $(X_0 = 1)$. Тогда, если $x \in S^*$, то гипотеза H_0 отвергается.

Ошибка первого рода α состоит в том, что H_0 отвергается, хотя она верна, при этом вычисляется по формуле:

$$\alpha = \frac{1}{q_0} \sum_{x \in S^*} p(0; x) .$$

Ошибка второго рода β состоит в том, что H_0 принимается, в то время как верна H_1, и вычисляется по следующей формуле:

$$\beta = 1 - \frac{1}{p_0} \sum_{x \in S^*} p(1; x) .$$

Заметим, что αq_0 может быть интерпретирована как вероятность "ложной тревоги", p_0 – как вероятность "необнаруженной атаки".

Задача построения КОУ состоит в том, чтобы при фиксированном уровне значимости за счет выбора S^* минимизировать β. Она может быть решена в рамках следующего алгоритма.

Шаг 1. Пронумеруем элементы множества S так, чтобы величины $p(1; x_a)/p(0;x_a)$ не возрастали, где $a = 1, 2, ..., N$.

Шаг 2. Построим последовательность расширяющихся подмножеств $S_a^* \subset S$, а именно: $S_0^* = \varnothing$, $S_1^* = \{x_1\}$, $S_2^* = \{x_1, x_2\}$ и т.д. Если найдутся наборы элементов x с частотой $p(0; x) = 0$, то такие наборы x включаются в подмножество S_0^*.

Шаг 3. Рассчитаем две числовые последовательности:

$$0 = \alpha_0 \le \alpha_1 \le ... \le \alpha_{N'} = 1,$$

Если любовная атака не удалась, надо переходить к мозговому штурму...
Военный закон Мерфи

$$\beta_0 \ge \beta_1 \ge \ldots \ge \beta_{N'} = 0,$$

где $N' \le N$, $\alpha_a = \frac{1}{q_0} \sum_{x \in S^*_a} p(0;x)$, $\beta_a = 1 - \frac{1}{p_0} \sum_{x \in S^*_a} p(1;x)$

Шаг 4. Вычислим суммы соответствующих элементов: $\alpha_0 + \beta_0$, $\alpha_1 + \beta_1$ и т.д. Определим номер a, которому соответствует наименьшее из полученных значений. Подмножество S^*_a будет являться КОУ. Вычислим значения вероятностей q_0 и p_0 кольца защиты.

Практические результаты

Предложенный защитный механизм, использующий КОУ, дает возможность снизить время обнаружения атаки. Рассмотрим формирование защитных механизмов в условии вирусной атаки (вирусы: Virus.Win32.Blackcat.2537, Virus. MSWord.Buendia, Virus.WinREG. Antireg.a). В кольцо защиты включены антивирусные программы: Касперского Personal 5.0.372, McAfee 9.0., Norton Antivirus 2005.

В обычной схеме кольцо защиты обнаруживало атаку за 150 единиц компьютерного времени [6], имея при этом большое число ложных срабатываний. По результатам работы предложенной системы были получены данные, представленные в таблице.

В КОУ данного кольца защиты входят следующие наборы x: (1, 1, 0); (1, 0, 1); (0, 1, 0) и (0, 1, 1). Время обнаружения атаки сократилось минимум вдвое, при этом вероятность "ложной тревоги" $\alpha q_0 = 0{,}14$, а вероятность "необнаруженной атаки" $\beta p0 = 0{,}13$.

Заключение

Предложенный и исследованный алгоритм обнаружения атак, основанный на понятии критической области угроз, позволяет объединить показания нескольких средств обнаружения и оптимизировать ошибки первого и второго рода.

Разработанная модель организации защитных механизмов в распределенной ИС позволяет учитывать индивидуальные особенности и характеристики каждого отдельно взятого СО, добиться лучшего соотношения между вероятностью обнаружения и частотой генерации "ложной тревоги" кольца защиты в целом. Одним из практических результатов является сокращение времени обнаружения атаки.

Список литературы

1. *Мамиконов А.Г., Кульба В.В., Шелков А.Б.* Достоверность, защита и резервирование информации в АСУ. М.: Энергоатомиздат. 1986.
2. *Доля А.* Проактивные технологии для борьбы с вирусами // Экспресс Электроника, 2006 г.
3. *Cohen, F.* Computer Viruses: theory and experiments // DOD/NBS 7th Conf. on Computer Security (1984).
4. *Груздева Л.М., Монахов М.Ю.* Алгоритмы обнаружения угрозы информационной безопасности // Автоматизированная подготовка машиностроительного производства, технология и надежность машин, приборов и оборудования: материалы междун. научно-технич. конф. Т.2. Вологда: ВоГТУ, 2005.
5. Mathematical methods of statistics by Harald Cramer / Пер. с англ. под ред. Колмогорова А.Н., 1975.
6. *Груздева Л.М.* Экспериментальное исследование антивирусных программ в распределенных информационных системах // Образовательная среда сегодня и завтра: Материалы III Всероссийской научно-технической конференции / Редсовет; Отв. Ред. В.И.Солдаткин. М.: Рособразование. 2006.

Груздева Людмила Михайловна *– аспирант,* ***Монахов Михаил Юрьевич*** *– д-р техн. наук, проф., зав. каф. "Информатика и защита информации" Владимирского государственного университета*

Контактный телефон (4922) 279-746. E-Mail: glm@izivlgu.vladimir.ru

Оценка эффективности производственной системы для выполнения авиационно-химических работ

И.С. Костина (ОГУ)

Сформулированы и обоснованы задачи аналитического описания и моделирования авиационно-химических работ (АХР) в сельском хозяйстве, определения влияния различных параметров модели АХР на эффективность производственной системы в целом. Для решения поставленных задач разработано специализированное программное средство.

В настоящее время без применения химических средств обработки сельскохозяйственных угодий практически невозможно получить продуктивную урожайность сельскохозяйственных культур. Для этого успешно используется целый ряд необходимых средств защиты растений, прошедший длительный период исследований и экспериментов в разных климатических условиях, на разных составах почвы и на многообразии культур, испытаний токсикологических и экологических аспектов их применения. Избирательность и интегрированность этих средств направлены на получение оптимальной эффективности против вредителей, болезней и сорняков при высокой степени безопасности для окружающей среды, человека и животных [1].

В этом аспекте важным технологическим звеном сельскохозяйственного производства являются авиационно-химические работы (АХР) – один из видов применения авиации в отраслях экономики с использованием воздушных судов, оборудованных аппаратурой для распыливания, опрыскивания, рассева сыпучих и жидких материалов, средств химизации, а