УДК 621.3

О.В. ЛАНКИН, В.В. СУХАНОВ

O.V. LANKIN, V.V. SUKHANOV

**АНАЛИЗ ПРОБЛЕМЫ МОНИТОРИНГА АНОМАЛЬНОГО ПОВЕДЕНИЯ СУБЪЕКТОВ ДОСТУПА В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ КРИТИЧЕСКОГО ПРИМЕНЕНИЯ**

**ANALYSIS OF THE PROBLEM OF MONITORING ABNORMAL BEHAVIOR OF ACCESS SUBJECTS IN DISTRIBUTED INFORMATION SYSTEMS OF CRITICAL APPLICATION**

*В данной статье авторы освещают задачу обнаружения аномального поведения субъектов доступа в распределенных информационных системах критического применения на основе применения нейросетевых методов анализа данной проблемы. Нейросеть проводит анализ информации и предоставляет возможность оценить, что данные согласуются с характеристиками, которые она научена распознавать. Степень соответствия нейросетевого представления может достигать 100%, достоверность мониторинга полностью зависит от качества системы в анализе примеров поставленной задачи.*

*Ключевые слова: автоматизированная система; защита информации; мониторинг; нейросеть; несанкционированный доступ; распределенная информационная система критического применения; субъект доступа.*

*In this article, the authors highlight the problem of detecting abnormal behavior of access subjects in distributed information systems of critical application based on the use of neural network methods for analyzing this problem. The neural network analyzes the information and provides an opportunity to assess that the data is consistent with the characteristics that it is trained to recognize. The degree of compliance of the neural network representation can reach 100%. The reliability of monitoring depends entirely on the quality of the system in the analysis of examples of the task.*

*Keywords: automated system; information protection; monitoring; neural network; unauthorized access; distributed information system of critical application; access subject.*

Организация информационного процесса в распределенных информационных системах критического применения (РИСКП) порождает целый ряд сложных проблем, и наиболее острой из них является проблема защиты информации от несанкционированного доступа (НСД).

Сложность решения задач по защите информации от НСД определяется следующими условиями:

* постоянно увеличивающимися объемами информации, накапливаемой, хранимой и обрабатываемой с помощью средств автоматизации;
* увеличением количества технических средств и связности в РИСКП;
* сосредоточением в распределенных базах данных РИСКП информации различного назначения, принадлежности и грифа секретности;
* расширением круга пользователей, имеющих непосредственный доступ к ресурсам РИСКП и обрабатываемой в них информации;
* повсеместным внедрением зарубежных программных средств и сетевых технологий, неудовлетворяющих требованиям по защите информации;
* нарушением принципов разработки и внедрения защищенных от НСД информационно-расчетных систем и т.д.

Существующие на сегодняшний день средства защиты информации, в целях поддержки и сохранности конфиденциальности, целостности и доступности информации, выполняют следующие основные функции обеспечения информационной безопасности в РИСКП [2]: идентификации, аутентификации, разграничения доступа, контроль целостности и др.

Комплексы средств защиты информации (КСЗИ), лежащие в основе защиты информации в РИСКП, предназначены для защиты критической информации от случайных воздействий и аварийных ситуаций на рабочих станциях.

КСЗИ от НСД предназначен для обеспечения возможности построения системы защиты информации от НСД автоматизированной системы (АС), обрабатывающей информацию с максимальной степенью секретности – «совершенно секретно», и соответствующей требованиям руководящих документов Гостехкомиссии РФ, отнесенным к классу защищенности АС-1Б [1].

Статистика нарушений, в РИСКП показывает, что злоумышленником, в 60% от общего числа случаев, является штатный пользователь, как правило, обладающий высоким уровнем квалификации, в распоряжении которого имеются современные методы и средства реализации НСД. В связи с этим одной из ключевых задач становится задача контроля и поддержания на соответствующем уровне защищенности информационных ресурсов РИСКП от НСД, осуществляемая посредством мониторинга аномального поведения субъектов доступа (СД) к ресурсам РИСКП, анализа и оценки собранной информации, исследования ситуаций, классифицируемых как нарушение политики безопасности, документирования причин НСД, своевременного оповещения и принятия мер направленных на предотвращение повтора выявленных ситуаций.

Неотъемлемой составляющей защиты информации в РИСКП является мониторинг аномального поведения СД к ресурсам РИСКП. Под мониторингом аномального поведения СД понимается определение в каждый конкретный момент времени соответствия действий СД, использующих в текущий момент времени защищаемый ресурс РИСКП, принятой политике безопасности. Следует отметить, что если политика безопасности – это совокупность исключительно организационных мер, а КСЗИ – совокупность программно-технических мер, то механизмы мониторинга аномального поведения СД представляют собой совокупность организационных и программно-технических мер, направленных на оценку реальной защищенности РИСКП, а, следовательно, на эффективность используемой политики безопасности и КСЗИ.

Существующие на сегодняшний день системы мониторинга аномального поведения СД в РИСКП обладают одним существенным недостатком. Подобные системы, как правило, позволяют обнаружить уже свершившейся факт НСД, а не предотвратить его угрозу в РИСКП, т.е. по существу они позволяют, в лучшем случае, блокировать, а не упредить злоупотребление (угрозу).

Сложившаяся ситуация может быть преодолена повышением эффективности систем контроля СД на основе совершенствования традиционных и разработки новых методов мониторинга действий пользователей РИСКП. Возникает задача перехода от систем мониторинга, работающих по принципу «обнаружение и ликвидация», к системам, построенным по принципу «анализ – прогнозирование – предупреждение». Перспективные системы мониторинга, реализующие последний принцип, объединяются общим понятием – системы активного мониторинга.

Под активным мониторингом понимается технология, направленная на выявление подозрительной (аномальной) активности СД с целью оперативного принятия ответных мер, по повышению защищенности РИСКП. Под аномальным поведением СД понимается их преднамеренные действия, направленные на исследование и преодоление системы защиты информации, осуществляемые неявным образом с использованием штатных средств вычислительной техники (ВТ) в пределах установленных прав и полномочий.

Для выявления аномального поведения СД в мировой практике использовано несколько универсальных методов [3]:

* статистические методы;
* экспертные системы;
* нейросетевые.

Статистические методы, как правило, применяются при обнаружении аномального поведения постоянных пользователей. Для успешного использования статистических методов важным является вопрос выбора параметров для систем обнаружения аномального поведения СД и атак. Их небольшое количество или неправильное отобранные параметры могут привести к тому, что модель описания аномального поведения СД будет некорректной.

Экспертные системы – это системы, которые при мониторинге аномального поведения СД, принимают решение о принадлежности того или иного факта к определенной группе злоупотреблений на основе имеющихся данных. В большинстве случаев правила экспертной системы опираются на шаблоны (сигнатуры), которые и ищутся в РИСКП [4].

Нейросетевые методы - это методы решающие задачи аномального поведения СД, которые трудно решить при помощи классических математических методов. Например, задача распознавания образов, к которой в том числе относится, и обнаружение аномального поведения СД и для которой достаточно сложно разработать готовый алгоритм. Нейросетевой метод не критичен к наличию готового алгоритма; достаточно, чтобы сеть могла «самообучаться» в процессе работы, вырабатывать определенные алгоритмы обработки информации, в условиях динамически изменяющейся обстановки и периодически корректировать эти алгоритмы в процессе своей работы. Самообучение - это главная характеристика нейросетевого метода обнаружения аномального поведения СД в РИСКП. Она позволяет изучить поведение СД и самостоятельно адаптироваться к постоянному изменению его поведения. Любое неправильно предсказанное событие сигнализирует об отклонении действий СД от установленного для него профиля.

Сравнительный анализ методов использующихся в системах обнаружения аномального поведения СД представлен в таблице 1.

Таблица 1 – Сравнительный анализ методов использующихся в системах обнаружения аномального поведения СД

|  |  |  |
| --- | --- | --- |
| Используемый метод | Достоинства | Недостатки |
| Статистические | Возможность локализации новых и сложных атак.  Возможность адаптации к изменению поведения СД. | «Приручение» системы, путем навязывание деятельности, соответствующей аномальному поведению, в качестве нормальной.  Вероятность получения ложных сообщений об аномальном поведении СД выше, чем при других методах.  Невозможность обнаружения аномального поведения СД, для которых невозможно описать шаблон типичного поведения и при нарушении порядка следования действий.  Методы невосприимчивы к порядку следования событий. |
| Экспертные | Простота реализации и высокая скорость функционирования.  Отсутствие ложных сигналов. | Неспособность к обнаружению новых атак, поиск аномального поведения СД строго по шаблону.  Система зависит от квалификации специалистов, заполняющих базу знаний. |
| Нейросети | Обнаружение новых атак.  Функционирование в условиях неопределенности и при наличии нечеткости (неполноты, искажение данных).  Прогнозирование поведения СД и появления новых злоупотреблений. | Нейронная сеть принимает решение, но не объясняет, почему было принято именно такое решение.  Большой объем обучающего материала. |

Исходя из проделанного анализа применение нейронных сетей для решения обозначенной проблемы позволит:

* проводить анализ данных, даже если они являются неполными или искаженными;
* обрабатывать данные от большого количества источников в нелинейном режиме (выявление скоординированных атак нескольких злоумышленников);
* реагировать в реальном времени на проводимые атаки до того, как в защищаемой системе появятся непоправимые повреждения.

**СПИСОК ЛИТЕРАТУРЫ**

1. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. М.: Военное издательство, 1992.
2. Бочков М.В., Ланкин О.В. Макаров О.Ю. Рогозин Е.А. Методологические основы интелектуальной защиты информации от несанкционированного доступа в автоматизированных системах управления критического применения. Воронеж: ГОУВПО «Воронежский государственный университет», 2011. 366с.
3. Гузик С. Зачем проводить аудит информационных систем // Jet Infosystems. 2000. №10.
4. Гриняев С.Н. Интеллектуальное противодействие информационному оружию. М.: Синтег, 1999.

**Ланкин Олег Викторович**

Воронежский институт правительственной связи (филиал) Академии Федеральной службы охраны Российской Федерации, г. Воронеж

д.т.н., доцент, сотрудник

Тел.: +79102406760

E-mail: [oleg\_lankin@mail.ru](mailto:oleg_lankin@mail.ru)

**Суханов Валерий Викторович**

Воронежский институт правительственной связи (филиал) Академии Федеральной службы охраны Российской Федерации, г. Воронеж

Сотрудник

Тел.: +79202285411

E-mail: vasukhanov@yandex.ru