ОБНАРУЖЕНИЕ ИНСАЙДЕРСКАХ АТАК В КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ С ИСПОЛЬЗОВАНИЕМ НЕЧЕТКОГО ЛОГИЧЕСКОГО ВЫВОДА

М.В. Додонов, Н.Л. Додонова

Самарский государственный аэрокосмический университет им. академика С.П. Королева (национально исследовательский университет)

В данной работе рассматривается разработанная авторами автоматизированная система обнаружения инсайдерских атак в корпоративных информационных системах. В качестве алгоритма обнаружения инсайдерской атаки используется нечеткий логический вывод на основе данных о текущей активности сотрудников компании

В современных корпоративных информационных системах (КИС) хранится огромный объем данных. Часть таких данных относится к категории конфиденциальных и играет важную роль для ведения успешной коммерческой деятельности компании. Кража такой информации может привести к огромным убыткам или банкротству компании в целом. Для КИС, с точки зрения обеспечения безопасности данных, выделяют два основных вида угроз: внешние и внутренние. Если в настоящее время существует достаточное количество решений защиты КИС от внешних угроз, то методы и способы защиты от внутренних угроз пока не достаточно развиты.

Наиболее распространенными способами хищения конфиденциальных данных становятся планомерные незаконные действия собственных сотрудников компании, называемых инсайдерами. Под инсайдером мы понимаем сотрудника, который по своему служебному положению имеет доступ к конфиденциальной информации компании и использует ее в собственных интересах, возможно, идущих в разрез с интересами компании.

В зависимости от возможностей доступа сотрудников к конфиденциальной информации можно выделить несколько категорий потенциальных инсайдеров: сотрудники, входящие в руководство компании; привилегированные пользователи, системные администраторы, обслуживающий персонал КИС; сотрудники, имеющие доступ к автоматизированным рабочим местам (АРМ) КИС и т.д. В настоящей работе рассматривается один из подходов к защите конфиденциальной информации в КИС от инсайдеров.

В настоящее время в компаниях используются различные формальные, технические и не формальные методы защиты информации. В данной работе мы ограничимся формальными методами, а точнее рассмотрим возможности программных средств обнаружения инсайдерских атак. Обычно в компаниях производят выборочный мониторинг пользователей, используя средства удаленного рабочего стола, URL-фильтрации и систем подсчета трафика, но также важно не забывать, что и ответственный может быть в сговоре и осуществлять кражу данных. Поэтому эффективная защита от инсайдера должна находиться выше привилегированных пользователей и системных администраторов.

Наряду с доверием к сотрудникам не стоит пренебрегать мониторингом подозрительной и опасной активности, которая может иногда возникать на рабочих местах пользователей. К примеру, сильно увеличился внутренний сетевой трафик, возросло количество запросов к корпоративной базе данных, сильно увеличился расход тонера или бумаги. Эти и многие другие события должны фиксироваться и разбираться, так как за ними также может скрываться атака или подготовка к атаке на чувствительные данные.

Существует множество сценариев решения проблемы утечки информации (файлов, фактов, баз данных, печатных копий и т.п.). Продукты начального уровня позволяют отслеживать каналы утечки, собирать статистику обращений сотрудников к объектам конфиденциальной информации, закрывать порты и устройства записи и вывода информации. Более продвинутые решения строятся на применении целого комплекса мер, включающих, наряду с перечисленными, анализ сетевого трафика, мониторинг операций пользователей с конфиденциальной информацией и т.д.

В настоящее время активно используются, например, такие программные комплексы как DeviceInspector, FileControl ,SecrecyKeeper и т.д. Особенностью таких комплексов является возможность блокировки и разграничения доступа к устройствам КИС, а также, возможность ведение журналов активности пользователей с использованием программ-агентов. Основным недостатком этих систем является то, что они не дают ответа на вопрос где искать инсайдера и требуют для своего сопровождения и эксплуатации высококвалифицированных специалистов, которых может себе позволить далеко не каждая крупная компания.

В процессе работы программ слежения накапливаются огромные объемы данных об активности пользователей КИС. Эти данные, совместно с дополнительной информацией о сотрудниках, могут быть использованы для оперативного мониторинга инсайдерских атак. В настоящее время операторам по безопасности приходится самостоятельно отслеживать накапливаемые данные используемых сотрудниками документов и уровней секретности.

В данной работе предлагается для обнаружения инсайдерских атак использовать разработанную автоматизированную систему, которая выполняет следующие функции:

- сбор сведений от программ-агентов и сохранение их в централизованную базу данных;
- ведение базы данных активности пользователей и дополнительной информации об них;
- автоматический расчет возможной инсайдерской атаки с использованием правил нечеткого логического вывода;
- возможность добавления и редактирования лингвистических переменных и правил в базе знаний;
- возможности просмотра списка потенциальных инсайдеров среди сотрудников компании.

В качестве метода оценки инсайдерской угрозы предлагается использовать нечеткий логический вывод, который в настоящий момент активно используется для решения различных задач [1]. Предположим, что имеется возможность сбора информации о сотруднике, характеризующей его активность, связанную с доступом к конфиденциальной информации. По значениям подобных характеристик можно делать выводы о степени безопасности деятельности сотрудника. Такие выводы могут основываться на различных математических моделях.

Входными данными для системы является информация из журналов работы программ-агентов, осуществляющих контроль над использованием периферийных устройств и другой активности пользователей. Выходными данными будет таблица сотрудников с указанием уровня принадлежности их действий к инсайдерским. Общую схему работы системы можно рассмотреть на рисунке 1.

Вся информация о деятельности сотрудников компании через модуль накопления данных поступает в единое хранилище данных. В едином хранилище данных накапливается информация о деятельности сотрудника за определенные интервалы времени (год, квартал, месяц, день, час и т.д.). Т.е. модуль накопления данных информацию от программ-агентов распределяет по используемым в системе характеристикам деятельности сотрудников (продолжительность рабочего времени, количество отправленных данных и т.д.). Поскольку единицы измерения характеристик

будут, также, несоизмеримы, то использование нечеткого логического вывода дает возможность получить требуемый результат.

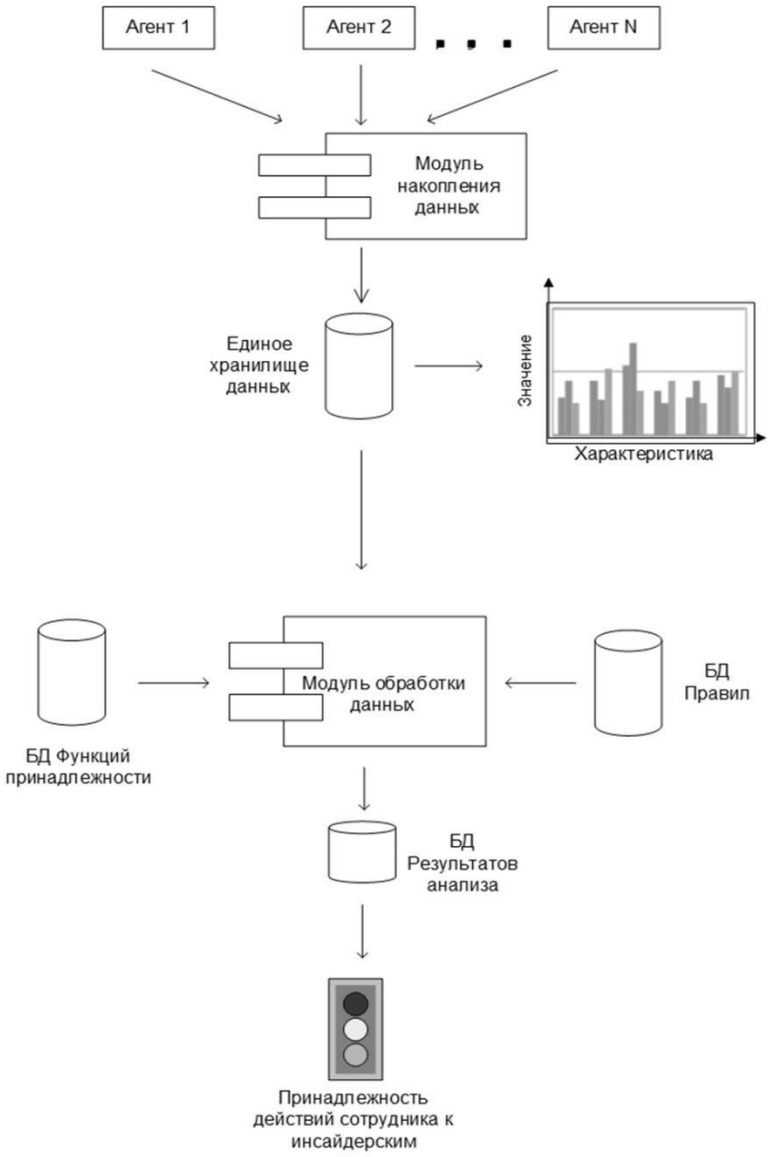

Рисунок 1 – Общая схема системы

Для хранения информации о текущей активности сотрудников компании была разработана соответствующая база данных (рисунок 2). Сущность «Значение из агентов» хранит соответствующие данные, полученные за определенный период времени от программ-агентов. Модуль накопления данных обрабатывает полученную информацию и сохраняет в удобном для дальнейшей обработки виде.

Модуль обработки данных с использованием нечеткого логического вывода с помощью заданных экспертами функций принадлежности и базы правил делает вывод по деятельности каждого сотрудника компании и записывает результаты в базу данных результатов анализа.

Рассмотрим алгоритм работы модуля обработки данных более подробно. Пусть X некоторый сотрудник организации, которого можно охарактеризовать набором характеристик $(V_1, V_2, \ldots V_n)$. Указанные характеристики учитывают должность сотрудника, время работы в организации, его полномочия, доступ и активность работы с конфиденциальной информацией и т.д.

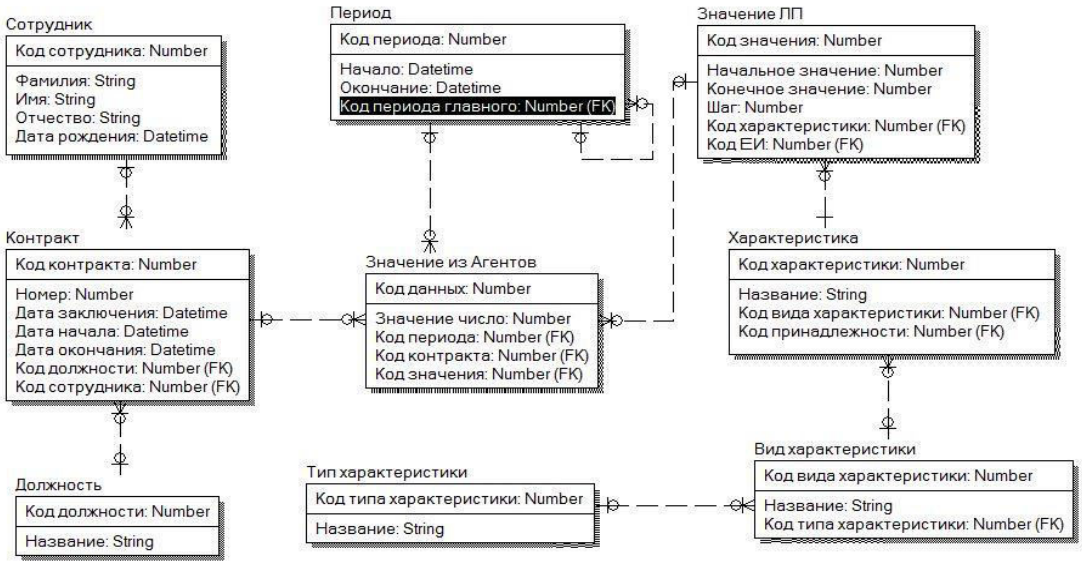

Рисунок 2 – Единое хранилище данных

Оценка деятельности сотрудника, с точки зрения причинения ущерба информационной безопасности компании, может быть описана в терминах естественного языка: «безопасная», «скорее всего безопасная», «возможно опасная» и т.п. Таким образом, деятельность сотрудника компании задается значениями лингвистических переменных, хранящихся в сущности «Значения ЛП».

Будем использовать процедуру нечеткого вывода для оценки деятельности сотрудника. На вход подаем информацию о сотруднике в виде набора его характеристик (значений лингвистических переменных), на выходе получаем информацию о степени его принадлежности к статусу инсайдера. Более подробно использования процедуры нечеткого вывода для поиска инсайдеров рассматривается в работе [2].

Результаты анализа деятельности сотрудников компании можно посмотреть на соответствующей форме системы. Для ввода новых и редактирования существующих характеристик деятельности сотрудников (сущности «Характеристика», «Вид характеристики» и «Тип характеристики» см. рисунок 2), функций принадлежности, правил базы знаний разработаны соответствующие формы. Для функций принадлежности и правил базы знаний были разработаны соответствующие базы данных. Такой подход, позволит учитывать особенности деятельности различных компаний, а сами по себе наборы характеристик, функции принадлежности и правила базы знаний могут быть предметом обмена и исследования в среде экспертов.

Данная система позволит в реальном режиме времени оценивать состояние безопасности данных в КИС и деятельность сотрудников по работе с конфиденциальными данными. В случае появления признаков инсайдерской атаки система сможет автоматически блокировать действия потенциального инсайдера и информировать руководство компании об опасности. При этом система для своего сопровождения не требует высококвалифицированных специалистов, поскольку, созданные и настроенные экспертом для конкретной компании база данных функций принадлежности и правила базы знаний, могут использоваться независимо от эксперта.

Литература

1. Додонова Н.Л., Кукольникова Е.А. Процедура нечеткого вывода состава региональных управляемых промышленных кластеров //Вестник поволжского государственного университета сервиса. Вып. № 1(33). –Тольяти: ПВГУС, 2014. –С.52-57.

2. Додонов М.В. , Додонова Н.Л. , Быханов В.А. Защита баз данных от инсайдеров на примере транспортно-экспедиторской компании //Вестник транспорта Поволжья. Вып. № 2(44). –Самара: СамГУПС, 2014. -С.84-89.