ТЕХНИЧЕСКИЕ НАУКИ

Емелин Павел Анатольевич
аспирант
ФГБОУ ВПО «Самарский государственный
технический университет»
г. Самара, Самарская область

РАЗРАБОТКА СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМ

Аннотация: *данная работа включает исследования, направленные на разработку математического и программного обеспечения СППР: рассмотрены теоретические основы информационной безопасности предприятия и приведена классификация существующих средств защиты информации от несанкционированного доступа; на основе модели представления знаний спроектирована формальная программа логического вывода.*

Ключевые слова: *локальная сеть, экспертная система, безопасность локальной вычислительной сети, система принятия решений, математическая модель.*

Использование систем поддержки принятия решений (СППР) для анализа безопасности информационно-коммуникационных систем (ИКС), является малоизученной проблемой. Решение этой проблемы позволило бы провести структуризацию и оптимизацию построенной модели предметной области, упростить процесс проектирования определенного класса средств защиты информации.

Основные требования к информационному обеспечению СППР следующие [8]:

1) наличие необходимой информации для обеспечения как автоматизированных, так и ручных процессов проектирования;

2) возможность хранения и поиска информации, представляющей результат ручных и автоматизированных процессов проектирования;

3) достаточный объем хранилищ информации;

4) структура системы должна допускать возможность наращивания емкости памяти вместе с ростом объема информации, подлежащей хранению;

5) достаточное быстродействие системы информационного обеспечения;

6) возможность быстрого внесения изменений и корректировки информации, доведения этих изменений до потребителя, а также получение твердой копии документа;

Прогресс подарил человечеству великое множество достижений, но тот же прогресс породил и массу проблем. Вечная проблема – защита информации. На различных этапах своего развития человечество решало эту проблему с присущей для данной эпохи характерностью. Изобретение компьютера и дальнейшее бурное развитие информационных технологий во второй половине 20 века сделали проблему защиты информации настолько актуальной и острой, насколько актуальна сегодня информатизация для всего общества [1].

Главная тенденция, характеризующая развитие современных информационных технологий – рост числа компьютерных преступлений и связанных с ними хищений конфиденциальной и иной информации, а также материальных потерь. Сегодня, наверное, никто не сможет с уверенностью назвать точную цифру суммарных потерь от компьютерных преступлений, связанных с несанкционированным доступом к информации. Это объясняется, прежде всего, нежеланием пострадавших компаний обнародовать информацию о своих потерях, а также тем, что не всегда потери от хищения информации можно точно оценить в денежном эквиваленте. Однако можно предположить, что потери от несанкционированного доступа к информации в компьютерных системах исчисляются сотнями миллионов долларов [2].

Именно по этим причинам в настоящее время появляется множество программных продуктов, позволяющих решить проблему утечки информации, – средства защиты информации от несанкционированного доступа.

Система защиты информации от несанкционированного доступа – комплекс организационных мер и программно-технических (в том числе криптографических) средств зашиты от несанкционированного доступа к информации в автоматизированных системах. Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления [2, с. 16].

Под средством защиты информации понимается техническое, программное средство или материал, предназначенные или используемые для защиты информации.

Под информационной безопасностью [3, с. 17] мы будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

Для поддержания режима информационной безопасности особенно важны программно-технические меры [5, с. 14], поскольку основная угроза компьютерным системам исходит от самих этих систем (сбои оборудования, ошибки программного обеспечения, промахи пользователей и администраторов и т.п.).

Существует пять основных механизмов безопасности [16, с. 4]:

а) идентификация и аутентификация;

б) управление доступом;

в) протоколирование и аудит;

г) криптография;

д) межсетевое экранирование.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности. Субъект доступа – лицо

или процесс, действия которых регламентируются правилами разграничения доступа. Объект доступа – единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Средства управления доступом позволяют специфицировать и контролировать действия, которые субъекты (пользователи и процессы) могут выполнять над объектами (информацией и другими компьютерными ресурсами). В данном случае речь идет о логическом (в отличие от

физического) управлении доступом, который реализуется программными средствами. Логическое управление доступом – это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов и, до некоторой степени, их доступность (путем запрещения обслуживания неавторизованных пользователей) [14].

Под протоколированием понимается сбор и накопление информации о событиях, происходящих в информационной системе предприятия. У каждого сервиса свой набор возможных событий, но в любом случае их можно подразделить на внешние (вызванные действиями других сервисов), внутренние (вызванные действиями самого сервиса) и клиентские (вызванные действиями пользователей и администраторов). Аудит – это анализ накопленной информации, проводимый оперативно, (почти) в реальном времени, или периодически (например, раз в день).

Одним из наиболее мощных средств обеспечения конфиденциальности и контроля целостности информации является криптография. Во многих отношениях она занимает центральное место среди программно-технических регуляторов безопасности, являясь основой реализации многих из них, и, в то же время, последним (а подчас и единственным) защитным рубежом. Например, для портативных компьютеров, физически защитить которые крайне трудно, только криптография позволяет гарантировать конфиденциальность информации даже в случае кражи.

Межсетевое экранирование следует рассматривать как самостоятельный (причем принципиально важный) сервис безопасности. Сетевые реализации данного сервиса, называемые межсетевые экранами, распространены весьма широко; сложилась терминология, оформилась классификация механизмов.

Принятие решений по обеспечению информационной безопасности строится на базе действующих стандартов и норм, которые для каждого конкретного случая требуют анализа применимости.

Учитывая требования современного мира к построению надежной системы защиты необходимы новые эффективные подходы к решению названных выше проблем. Один из таких подходов называется адаптивной сетевой безопасностью [6].

Адаптивная безопасность сети описывается как процесс, содержащий:

1) технологию анализа безопасности или поиска уязвимостей;

2) технологию обнаружения атак;

3) адаптивный компонент, который расширяет две первые технологии;

4) управляющий компонент.

Анализ безопасности ИКС, [11] – это поиск уязвимых мест в сети. Сеть состоит из соединений, узлов, хостов, рабочих станций, приложений и баз данных. Все они нуждаются как в оценке эффективности их защиты, так и в поиске неизвестных уязвимостей в них. Средства, реализующие технологию анализа безопасности, исследуют сеть и ищут «слабые» места в ней, обобщают эти сведения и создают по ним исчерпывающий отчет, содержащий подробные рекомендации по устранению найденных уязвимостей. Если система, реализующая эту технологию, содержит и адаптивный компонент, то вместо «ручного» устранения найденной уязвимости оно будет осуществляться автоматически.

Обнаружение атак [7] является процессом оценки подозрительных действий, которые происходят в корпоративной сети. Обнаружение атак реализуется посредством анализа или журналов регистрации операционной системы и

прикладного программного обеспечения, или сетевого трафика в реальном времени. Компоненты обнаружения атак, размещенные на узлах или сегментах сети, оценивают различные действия, в т. ч. и использующие известные уязвимости.

Использование модели адаптивной безопасности сети позволяет контролировать практически все угрозы, и своевременно реагировать на них высокоэффективным способом, позволяющим не только устранить уязвимости, которые могут привести к реализации угрозы, но и проанализировать условия, приводящие к появлению уязвимостей. Эта модель также позволяет уменьшить злоупотребления в сети, повысить осведомленность пользователей, администраторов и руководство компании о событиях безопасности в сети.

Системы анализа безопасности выполняют серию тестов по обнаружению уязвимостей, аналогичных тем, которые применяют злоумышленники при осуществлении атак на корпоративные сети.

Сканирование начинается с получения предварительной информации о сканируемой системе, например, разрешенных протоколах и открытых портах, версии операционной системы и т.п., и заканчивая попытками имитации проникновения, используя широко известные атаки, например, «подбор пароля». Системы анализа безопасности на уровне сети могут быть использованы как для оценки уровня безопасности организации, так и для контроля эффективности настройки сетевого программного и аппаратного обеспечения [9; 10].

Наибольшее распространение получили средства анализа безопасности сетевых сервисов и протоколов [12; 13]. Связано это, в первую очередь, с универсальностью используемых протоколов. Изученность и повсеместное использование таких стеков протоколов, как TCP/IP и т.п. позволяет с высокой степенью эффективности проверять защищенность корпоративной сети, работающей в данном сетевом окружении, независимо от того, какое программное обеспечение функционирует на более высоких уровнях. Вторыми по распространенности являются средства анализа безопасности операционных систем. Связано это также с универсальностью и распространенностью некоторых операционных систем. Однако, из-за того, что каждый производитель вносит в операционную систему

(ОС) свои изменения, средства анализа безопасности ОС анализируют в первую очередь параметры, характерные для всего семейства одной ОС. И лишь для некоторых систем анализируются специфичные для нее параметры [15].

Существующие системы анализа безопасности имеют значительные недостатки:

1. Отсутствие единого формализма для описания функционирования механизма логического вывода.

Существующие системы анализа безопасности не обладают каким-либо формализмом, позволяющим описать работу механизма логического вывода, что не дает возможности оценить эффективность его работы.

2. Обновление баз уязвимостей только через определенный промежуток времени, что позволяет злоумышленнику воспользоваться уязвимостью до того момента, пока базы уязвимостей сканера безопасности будут обновлены.

Администратор безопасности не имеет возможности самостоятельно добавлять в базу уязвимостей информацию о новых уязвимостях. Возможности проектирования базы уязвимостей самим администратором безопасности не имеет ни один из существующих сканеров безопасности.

3. Отсутствие хорошего аппарата для оперативного пополнения баз уязвимостей самим администратором сети.

Существующие сканеры безопасности не имеют редактора базы уязвимостей, что не дает возможности администратору безопасности оперативно пополнять базу уязвимостей новой информацией.

4. Большое количество обнаружений ложных уязвимостей.

Отсутствие какого-либо математического аппарата у существующих систем анализа безопасности для анализа найденных уязвимостей приводит к большому количеству обнаружений ложных уязвимостей.

5. Узкая направленность на конкретную область.

Существующие системы анализа безопасности можно разделить на 4 категории: системы анализа безопасности сети, системы анализа безопасности операционной системы, системы анализа безопасности прикладного ПО, системы

анализа безопасности СУБД. На данный момент не существует системы анализа безопасности, объединяющей в себе все системы, перечисленные выше.

6. Плохая информативность выдаваемых отчетов по найденным уязвимостям.

В основе разрабатываемой системы поддержки принятия решений для анализа безопасности информационно-коммуникационных систем необходимо заложить экспертную систему, позволяющую анализировать данные, поступающие в результате сканирования компьютеров и дающую возможность пополнять существующую базу уязвимостей информацией о новых уязвимостях.

Список литературы

1. Азаркин А.В. Средства обеспечения защищенности информационных систем (часть 1) / А.В. Азаркин, Г.В. Фоменков // Защита информации. Конфидент. – №1. – 2008. – С. 34–41.

2. Алексенцев А.И. Защита информации. Сводный словарь основных терминов и понятий / А.И. Алексенцев // Безопасность информационных технологий. – М.: Изд. МИФИ, 2008. – № 4. – С. 101–108.

3. Алин Б.Ю. Защита компьютерной информации / Б.Ю. Алин – СПб.: БХВ-Санкт-Петербург, 2000. – 384 с.

4. Вейнеров О.М. Разработка САПР. Проектирование баз данных САПР / О.М. Вейнеров, Э.Н. Самохвалов – М.: Высшая школа, 2000. – 144 с.

5. Глушань В.М. Комбинаторные аппаратные модели и алгоритмы в САПР / В.М. Глушань, В.М. Курейчик, Л.И. Щербаков – М.: Радио и связь, 2000. – 216 с.

6. Гуляев Н.Б. Разработка САПР. Проектирование программного обеспечения САПР // Н.Б. Гуляев, Б.С. Федоров – М.: Высшая школа, 2000. – 159 с.

7. Корячко В.П. Теоретические основы САПР: Учебник для вузов / В.П. Корячко, В.М. Курейчик, И.П. Норенков. – М.: Энергоатомиздат, 2007. – 400 с.

8. Лозовский В.С. Семантические сети. Представление знаний в человеко-машинных и робототехнических системах / В.С. Лозовский – М.: ВИНИТИ, 1984. – С. 84–120.

9. Лукацкий А.В. Выявление уязвимостей компьютерной сети / А.В. Лукацкий – М.: Сетевой. – 2001. – №1. – С. 8–14.

10. Лукацкий А.В. Обнаружение атак / А.В. Лукацкий. – СПб.: БХВ-Петербург, 2001. – 624 с.

11. Норенков И.П. Введение в автоматизированное проектирование / И.П. Норенков – М.: Высшая школа, 1996. – 335 с.

12. Родионов А.Н. Компьютерные преступления и организация борьбы с ними / А.Н. Родионов // Системы безопасности 2009. Межотраслевой тематический каталог. – М.: Гротек, 2000. – С. 25–27.

13. Тимофеев П.А. Принципы защиты информации в компьютерных системах / П.А. Тимофеев // Защита информации. Конфидент. – 1998. – №3. – С. 72–76.

14. Шипли Грег. Обнаружение сетевых вторжений. Дубль второй / Грег Шипли // Сети и системы связи. – 2010. – №2 (52). – С. 96–109.

15. Щербаков А.Ю. Введение в теорию и практику компьютерной безопасности / А.Ю. Щербаков. – М.: Изд. Молгачева С.В., 2001. – 352 с.