УДК 681.3

В.Н. Кострова, О.В. Милошенко

ПРОГРАММНЫЕ РЕШЕНИЯ ДЛЯ АНАЛИЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Воронежский государственный технический университет
Воронежский институт высоких технологий

В работе проведен анализ современных программных решений, предназначенных для оценки характеристик информационной безопасности. Отмечены особенности защиты рабочих станций. Указаны характеристики программ для оценки информационных рисков.

Ключевые слова: защита информации, программа, безопасность, компьютер.

Введение. Для современного этапа развития нашей страны можно отметить возрастающую роль информационной сферы, она представляет собой общий объем источников информации, компонентов инфраструктур, тех, кто проводит обработку, формирование, передачу и фильтрацию информации.

Исходя из этого, вопросы информационной безопасности должны решаться на высоком уровне. Как показывает анализ, российская киберпреступность имеет весьма большие масштабы и тенденции роста.

С каждым годом происходит увеличение не только количества киберпреступлений, но и тот урон, который получается вследствие них. Основываясь на вышесказанном, для современных условий существование хорошо разработанной системы информационной безопасности является одним из главных условий повышения условий конкурентоспособности любой фирмы.

Программные системы, предназначенные для обнаружения и предотвращения компьютерных атак. Среди одних из перспективных направлений, касающихся данного направления можно выделить моделирование систем информационной безопасности которое опирается на понятие онтологий, которые являются спецификациями указанной предметной области [1-5].

На основе онтологий есть возможности проведений концептуализации предметной области, то есть проводить теоретическую организацию накопленных знаний, проводить определение понятий, отношений и механизмов управления, которые требуются для того, чтобы описать процесы решения задач в анализируемой предметной области.

Применение таких систем уже наблюдается как один из требуемых рубежей, связанных с обороной информационных систем. Проводятся исследования в сфере обнаружения атак на различные компьютерные системы и сети, такие работы уже проходят в течение нескольких десятилетий.

Если говорить о сегодняшнем дне, то существующие системы, предназначенные для проведения обнаружений вторжений и атак, как правило, являются программными или аппаратно-программными решениями, которые осуществляют автоматизацию процесса контроля событий, которые протекают внутри компьютерной системы или сети, а также проводят самостоятельный анализ таких событий для поиска признаков возникающих проблем безопасности.

На настоящее время можно провести разделение всех систем на сетевые и локальные. При этом сетевые системы, как правило, устанавливают на определенных для таких целей компьютеров и проводится анализ трафика, который циркулирует внутри ЛВС. Происходит размещение локальных систем на отдельных компьютерах, которые нуждаются в защите, и проводится анализ различных событий (это может относиться к действиям пользователя или программным вызовам) [6-9].

Можно провести разделение всех систем обнаружения вторжений, с точки зрения ориентирования на поиск [8]:

- возникающих аномалий по взаимодействию контролируемых объектов;
- характерных сигнатур по всем узнаваемым атакам.

На основе сигнатурных методов может быть проведено описание атаки на основе набора правил или на основе формальной модели. Это может быть использованы символьные строки, семантические выражения на специальном языке и т.д.

Характерная черта указанного подхода состоит в применении специализированной базы данных по шаблонам (сигнатурам) атак с целью проведения поиска тех действий, которые подпадают под определение "атака".

Если говорить об эффективности работы сигнатурной системы, то она может зависеть от трех основных факторов: оперативность пополнения сигнатурной базы, полнота ее, если говорится об определениях сигнатур атак, кроме этого должны быть интеллектуальные алгоритмы, которые сводят действия атакующих к определенным основным шагам, исходя из которых осуществляются процессы сравнений с сигнатурами.

Для систем поиска аномалий происходит идентификация необычных поведений ("аномалия") с точки зрения работы контролируемого объекта. При этом в качестве объекта наблюдения можно рассматривать или сеть целиком, может быть компьютер, это может относиться к сетевой службе (например, это может быть файловый сервер FTP), пользователи и др. Происходит сигнализация системы исходя из условия, что действия, которые происходят при проведении нападения, могут отличаться от обычной работы пользователей и компьютеров.

Весьма распространенный способ в обнаружении злоумышленного поведения - это экспертные системы. Среди представителей таких систем можно отметить бесплатно распространяемую и достаточно популярную систему Snort [10]. Указанную систему разрабатывает компания Sourcefire и ее можно быть использовать для того, чтобы обнаруживать разчные виды атак, среди них может быть проведение переполнения буфера, проведение сканирования портов и др.

Если говорить о защите рабочих станций, то можно отметить систему Cisco Security Agent (CSA) [11]. Указанная система проводит объединение различных защитных механизмов и функций для одного решения – происходят действия по предотвращению атак, появляется персональный межсетевой экран, осуществляется защита от внедряющегося вредоносного кода, проводится контроль целостности, осуществляется блокирование утечки информации через USB-порты, а также с использованием других внешних устройств, ограничиваются возможности Интернет-пейджеров (например, ICQ), проводится обнаружение перехватчиков с клавиатуры и т.п.

Весьма большой интерес с точки зрения защиты рабочих станций можно отметить в отношении Proventia Desktop Endpoint Security (Proventia Desktop). Этот продукт создан сотрудниками американской компании Internet Security Systems [12].

Решение предназначено для проведения защиты рабочих станций. Работу такой системы можно характеризовать таким образом, что, что очень сильно уязвимы те узлы в корпоративной сети, которые относятся к рабочим станциям. С их помощью проводится обработка большого объема конфиденциальной информации и осуществляется хранение данных по интеллектуальной собственности компании. Программа Proventia Desktop разработана как одна из частей в единой платформе Proventia Enterprise Security Platform (ESP).

Эта платформа дает решения, связанные с обеспечением информационной безопасности, которые выявляют заметные критические уязвимости и ведущие к предотвращению атак, при использовании централизованных средств управления и средств, позволяющих проводить создание отчетов.

Среди российских разработок может быть отмечена система раннего предупреждения и прогнозирования атак NetTrap [13]. Она разработана фирмой Информзащита. Указанна сетевая система NetTrap дает возможности осведомленности компании-заказчика о различных нацеленных против нее действиях от сетевой разведки. Существуют возможности по проведению сбора данных, позволяющих проводить дальнейшее расследование инцидентов. С целью анализа действительных способов и мотивов злоумышленника система NetTrap применяет

совместное применение традиционных средств, связанных с противодействием вторжениям (проведение обнаружения по заданному шаблону и проведение обнаружения из аномалий в поведении) со различными средствами, дающими возможности осуществления скрытого мониторинга действий злоумышленника, изучения его средств, тактики и уровня квалификации.

Достаточно известной российской разработкой, касающейся сферы компьютерной безопасности может быть назван антивирус Касперского. Kaspersky Internet Security 2015 [14] представляет собой продукт класса Internet Security и он необходим для проведения защит домашних компьютеров. Указанный продукт дает возможности не только базовых инструментов обеспечения безопасности, но и при этом хорошо разработанный набор дополнительных инструментов. Среди них отметим безопасную среду запуска приложений и браузеров, монитор, показывающий активность программ, сетевой экран, родительский контроль и др.

Отметим, что рассмотренные программные средства представляют собой средства, которые при обнаружении ненормального функционирования корпоративной информационной системы, будут проводить исправление такой системы. Они не дают просчета целесообразности действий, связанных с исправлением, вероятностей того, что проведение отказа от процессов исправления даст нежелательные последствия и др. То есть, в них нет функционалов управления информационными рисками по указанной корпоративной системе.

Программы анализа и оценки рисков неблагоприятных событий.

Программы указанного вида необходимы для осуществления процессов аудита для информационной безопасности фирмы. Аудит позволяет проводить анализ текущей безопасности функционирования корпоративной информационной системы, проводить оценку и прогноз рисков, управления ими с точки зрения влияния на бизнес-процессы предприятия, корректным и обоснованным образом рассматривать к вопросы, связанные с поддержанием безопасности ее активов. Проведение анализа существующих программных систем, которые предназначены для проведения оценки указанных рисков, проведено в работах [15-16].

Но программные средства по анализу и оценке информационных рисков не нацелены на проведение риск-менеджмента для условий атаки, которая началась. Они необходимы для того, чтобы проводить указание на существующие недостатки, касающиеся обеспечения информационной безопасности предприятия. Когда атака, началась, то они не могут указать для каких из существующих «дыр» требуется осуществлять первоочередное закрытие.

Методологию OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) разрабатывали с учетом активного участия тех, кто владеет информацией в процессах поиска тех информационных массивов, которые защищены минимальным образом. Основные положения методологии базируются на использовании последовательностей специальным образом сформированных внутренних семинаров, и проведение оценок рисков идет в рамках трех этапов, до которых необходимо провести согласовние графика семинаров, сделать планирование по действиям участников и сопоставить для них роли.

На первом этап идет разработка по профилям угроз, которые соответствуют сетям данной фирмы, с учетом законодательной базы. Второй этап соответствует анализу уязвимостей по системам компании с точки зрения угроз, по профилям которых было формирование для первого этапа. И, потом, на третьем этапе происходят процессы оценивания рисков информационной безопасности, которое заключается в том, что устанавливается вероятность или степень возникновения ущерба когда осуществляются угрозы при существующих уязвимостях. Как итог, идет принятие решений при обработке рисков [17-20].

Приложение Oracle Crystal Ball используется совместно с Microsoft Excel при моделировании бизнес-процессов, расчете показателей рисков, прогнозировании характеристик неопределённых данных и процессах, связанных с оптимизацией результатов. Методику можно применять при использовании исторических данных по продажам, вследствие этого можно сделать прогноз. Применение подходов, связанных с моделированием на основе метода Монте Карло позволяет определить дополнительные возможности, связанные с оптимизацией [21].

Программное обеспечение CRAMM может быть настроено для разных областей с привлечением встроенных профилей: коммерческие, гражданские государственные учреждения, финансовые сектора и др. При анализе риска идет идентификация и определение уровней по рискам, базируясь на оценках, которые присваивались для элементов в модели угроз. Как выходной результат получаем профиль контрмер, на базе которого осуществляется контроль рисков [22].

Систему CORAS разрабатывали для программы Information Society Technologies. Она базируется на том, что идет адаптация, уточнение и комбинирование таких способов анализа рисков: использование цепей Маркова, FMECA, Event-Tree-Analysis и HazOp. Для системы применяют технологию UML, а исходит она из австралийского стандарта AS/NZS 4360: 1999 Risk Management и ISO/IEC 17799–1: 2000 Code of Practice for Information Security Management [23].

Вывод. В работе обозначены основные подходы и программные решения, позволяющие проводить анализ характеристик защищенности

информационных систем. Показано, что для эффективной работы систем необходимо проводить расчет показателей рисков, прогнозирование характеристик по неопределённым данным и процессам, которые связаны с оптимизацией результатов.

ЛИТЕРАТУРА

1. Пальчунов, Д.Е. Решение задач поиска информации на основе онтологий // Бизнес-информатика, т.1, 2008, с. 3-13.
2. Пальчунов, Д.Е. Поиск и извлечение знаний: порождение новых знаний на основе анализа текстов естественного языка // Философия науки. 2009. №4(43). С. 70-90.
3. Фомина Ю.А., Преображенский Ю.П. Принципы индексации информации в поисковых системах / Вестник Воронежского института высоких технологий. 2010. № 7. С. 98-100.
4. Иванов М.С., Преображенский Ю.П. Разработка алгоритма отсечения деревьев / Вестник Воронежского института высоких технологий. 2008. № 3. С. 031-032.
5. Зазулин А.В., Преображенский Ю.П. Особенности построения семантических моделей предметной области / Вестник Воронежского института высоких технологий. 2008. № 3. С. 026-028.
6. Ермолова В.В., Преображенский Ю.П. Архитектура системы обмена сообщений в немаршрутизируемой сети / Вестник Воронежского института высоких технологий. 2010. № 7. С. 79-81.
7. Милошенко О.В. Методы оценки характеристик распространения радиоволн в системах подвижной радиосвязи / Вестник Воронежского института высоких технологий. 2012. № 9. С. 60-62.
8. Мишин Я.А. О системах автоматизированного проектирования в беспроводных сетях / Вестник Воронежского института высоких технологий. 2013. № 10. С. 153-156.
9. Головинов С.О., Хромых А.А. Проблемы управления системами мобильной связи / Вестник Воронежского института высоких технологий. 2012. № 9. С. 13-14.
10. Интернет-портал компании Информзащита, разработчика ПО "NetTrap": http://www.infosec.ru/ [Электронный ресурс] Доступ: 18.03.2015.
11. Palchunov, D.E., Yakhyaeva, G.E. Interval fuzzy algebraic systems // Proceedings of the Asian Logic Conference 2005. World Scientific Publishers. 2006, pp. 23-37.
12. Wille, R. Formal Concept Analysis as Mathematical Theory of Concepts and Concept Hierarchies // Fachbereich Mathematik Technische Hochschule Darmstadt, 2005, - 347 p.
13. ДСМ-метод автоматического порождения гипотез: Логические и

эпистемологические основания // Сост. Аншаков, О.М., Фабрикантова, Е.Ф.; Под общ. Ред. Аншакова, О.М. - М.: Книжный дом "ЛИБРОКОМ", 2009. - 432 с.

14. Интернет-портал компании "Лаборатория Касперского", разработчика ПО "Kaspersky Internet Security 2015": http://www.kaspersky.ru/ [Электронный ресурс] Доступ: 08.03.2015.
15. Пальчунов, Д.Е., Яхъяева, Г.Э. Нечеткие алгебраические системы // Вестник НГУ. Серия: Математика, механика, информатика. 2010. Т.10, вып. 3. С. 75-92.
16. Rubens, Paul. Medusa: Open Source Software "Login Brute-Forcer" for Password Auditing: http://www.serverwatch.com/tutorials/article.php/3886791/Medusa-Open-Source-Software-Login-BruteForcer-for-Password-Auditing.htm/ [Электронный ресурс] Доступ: 08.03.2015.
17. Дешина А.Е., Чопоров О.Н., Разинкин К.А. Информационные риски в мультисерверных системах: выбор параметров системы защиты / Информация и безопасность. 2013. Т. 16. № 3. С. 365-370.
18. Душкин А.В., Чопоров О.Н. Декомпозиционная модель угроз безопасности информационно-телекоммуникационным системам / Информация и безопасность. 2007. Т. 10. № 1. С. 141-146.
19. Завьялов Д.В. О применении информационных технологий / Современные наукоемкие технологии. 2013. № 8-1. С. 71-72.
20. Дешина А.Е., Ушкин И.А., Чопоров О.Н. Интегральная оценка общего риска при синтезе ИТКС на основе параметров риска ее компонентов / Информация и безопасность. 2013. Т. 16. № 4. С. 510-513.
21. Медведовский И. Д. Современные методы и средства анализа и контроля рисков информационных систем компаний [Электронный ресурс]. - Режим доступа: http://www.bugtraq.ru/library/security/itrisk.html Доступ: 08.03.2015.
22. Пастоев. А. Методологии управления ИТ-рисками [Электронный ресурс]. - Режим доступа: http://www.iso27000.ru/chitalnyi-zai/upravlenie-riskami-informacionnoi-bezopasnosti/metodologii-upravleniya-it-riskami, Доступ: 08.03.2015.
23. Oracle. Information decides [Электронный ресурс]. - Режим доступа: http://www.oracle.com/us/products/middleware/bus-int/crystalball/cb-brochure-404904.pdf, Доступ: 08.03.2015.

V. N. Kostrova, O. V. Miloshenko

THE SOFTWARE SOLUTIONS FOR THE ANALYSIS OF INFORMATION SECURITY

Voronezh state technical university
Voronezh Institute of High Technologies

In the paper the analysis of the modern software solutions intended for an assessment of characteristics of information security is carried out. The features of protection of workstations are noted. The characteristics of programs for an assessment of information risks are specified.

Keywords: information security, program, safety, computer.