УДК 004

Актуальность разработки модели по обнаружению компьютерных атак на объекты критических информационных инфраструктур

К.А. Пестракова

Брянский государственный университет, бульвар 50-летия Октября, 7, Брянск, 241035, Россия

E-mail: kris.siniczckaia@yandex.ru

Аннотация. Рассмотрена актуальность проблемы компьютерных атак. Проведена подробная характеристика информационных систем общего пользования, которые в наибольшей степени подвержены воздействию компьютерных атакам. Приведена оценка объектов критической информационной инфраструктуры. Описаны цели компьютерных атак. Особое внимание уделено требованиям к российскому законодательству, которое направленно на защиту критической информационной инфраструктуры. Разработаны структурная схема формирования образа компьютерной атаки и последовательность формирования ее образа. Произведен анализ характеристик основных методов обнаружения и анализа компьютерных атак. Рассмотрены и описаны метод анализа сигнатур и метод обнаружения аномальных отклонений. Представлена информация, в которой описаны необходимые действия по идентификации компьютерных атак. Предложены направления по поиску правил и алгоритмов выявления эффективных способов обнаружения компьютерных атак. Поставлена задача изучения развития алгоритмических моделей, которые обеспечивают распознавание образа атаки на основании набора ее отличительных признаков. Выдвинуты утверждения о целесообразности представления модели обнаружения компьютерных атак. Обозначена задача формирования моделей атаки на объекты критической информационной инфраструктуры. Выдвинуто предложение по созданию схемы формирования модели компьютерных атак на объекты критической информационной инфраструктуры на основе функционального подхода.

Ключевые слова: критическая информационная инфраструктура, защита информации, компьютерная атака

The relevance of developing a model for detecting computer attacks on objects of critical information infrastructures

К.А. Pestrakova

Bryansk State Technical University, 50th anniversary of October Boulevard, 7, Bryansk, 241035, Russia

E-mail: kris.siniczckaia@yandex.ru

Abstract. The article deals with the relevance of the problem of computer attacks. It describes information systems of general use that are the most susceptible to computer attacks. The objects of critical information infrastructure are considered as the targets of computer attacks. Special focus was given to Russian legislative requirements directed to the protection of critical information infrastructure. The generalized structural scheme of the computer attack and the sequence of its form are examined. The article includes the search for effective algorithms for detection and analysis of the attacks. The method of analysis of signatures and the method of detecting abnormal deviations are considered and described. The information needed to the identification of computer attacks is analyzed. The directions for searching and identifying the effective ways to detect computer attacks are suggested. There is the task to consider the development of algorithmic models providing the recognition of the image of an attack based on a set of its distinctive features. There are statements about the advisability of presenting the computer attack detection model in the form of a composition of two main components. The article includes the formation of models of attack on objects of a critical information infrastructure. A proposal has been made to create a model of critical information infrastructure tools based on a functional approach.

Keywords: critical information infrastructure, information security, computer attack

1. Введение

В настоящий период времени в России актуальными направлениями деятельности являются вопросы, связанные с обеспечением как национальной безопасности в целом, так и информационной безопасности в частности. С каждым днем обостряется геополитическая обстановка и нарастает противостояние со многими иностранными государствами, которые с негативом относятся к России. В связи с этим информационные системы и ресурсы выступают как уязвимое место в государственной и общественной жизни, так и являются самими действенными рычагами воздействия в экономической, информационной, политической борьбе между конкурирующими государствами. Поэтому в сложившейся ситуации для защиты национальных информационных ресурсов стоит уделить внимание обеспечению информационной безопасности России.

Для реализации данного направления, 26 июля 2017 года был принят Федеральный закон № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» и был сформирован и утвержден список необходимых требований по обеспечению безопасности информации со стороны государственных служб-регуляторов в области защиты информации [1]. Данный закон регулирует обеспечение безопасности критической информационной инфраструктуры России (далее КИИ) в целях ее устойчивого функционирования при проведении в отношении данной инфраструктуры компьютерных атак.

2. Постановка задачи

Негативное компьютерное воздействие на объекты КИИ в большей степени может сказаться на системах государственного управления, системах связи и коммуникаций, энергетических и транспортных секторах, банковской сфере и др. В ближайшее время проблему компьютерных атак на объекты КИИ также может усугубить внедрение информационных технологий во все сферы жизнедеятельности [2]. Под термином «компьютерная атака» Так что же принято понимать – целенаправленное воздействие на информационные системы и информационно-телекоммуникационные сети программно-техническими средствами, которое осуществляется для нарушения безопасности информации в этих сетях и системах.

Как правило, до недавнего времени информационные системы обеспечивали защиту от массовых, типовых информационных атак, например, от мошенничества, компьютерных вирусов, сетевых атак, внутренних утечек информации и т.д. В

ISBN 978-5-6045165-2-2

результате этого системы защиты информации приобрели типовой, шаблонный вид, который ко всему этому содержит алгоритм определенных средств защиты, к нему относятся все возможные антивирусные средства, межсетевые экраны и другое. Все это влияет на защиту и позволяет отбить все возможные традиционные атаки.

Внедрение современных комплексных решений, таких как применение SIEM и DLP – систем сыграло огромную роль для повышения эффективности информационных систем. Но наряду с этим не всегда можно решить проблему компьютерных атак, используя при этом комплексные и дорогостоящие решения информационной безопасности. В последнее время стали появляться компьютерные атаки, направленные на определенную цель, задача которых взломать конкретные государственные организации, коммерческие предприятия и их вычислительные сети. Количество данных компьютерных атак будет только возрастать, поэтому необходимо исследовать данные атаки и рассматривать их информационную составляющую с позиции защищенности [3].

3. Методы и материалы исследования

Как известно, для достижения цели информационной атаки на объекты КИИ, необходимо присутствие в атаке следующих структурных компонентов (рисунок 1):

- источник атаки (субъект) – программа, которая ведет атаку и осуществляет воздействия;
- уязвимости информационной системы;
- алгоритм исследования уязвимостей информационных систем;
- объект атаки, например, автоматизированные системы, телекоммуникационные системы, информационно-управляющие системы, и т.д.

ISBN 978-5-6045165-2-2

Рисунок 1. Структурная схема формирования образа компьютерной атаки.

Состояние объекта атаки изменяется посредством реализации воздействия компьютерной атаки, при этом формируется образ атаки в результате данных негативных воздействий.

Получается, что основой формирования эффективных мер противодействия будет являться анализ данного состояния. Как правило, в качестве основных средств по борьбе с компьютерными атаками для систем защиты информации используют алгоритмы анализа и обнаружения компьютерных атак. Обычно алгоритмы анализа и обнаружения компьютерных атак подразделяют на методы анализа сигнатур и методы обнаружения аномальных отклонений (таблица 1).

Таблица 1. Характеристика метода анализа сигнатур и метода обнаружения аномальных отклонений.

	Методы анализа сигнатур	Методы обнаружения аномальных отклонений
Предназначение	обнаружение известных атак	выявление неизвестных ранее компьютерных атак
Описание	контроль программ и данных в критически важной информационной системе и эталонная сверка последовательности символов и событий в сети с базой данных сигнатур атак	выявление отклонений от нормального поведения системы

Для идентификации компьютерных атак, направленных на объекты КИИ необходима, информация, которая представлена данными по результатам аудита и на

ISBN 978-5-6045165-2-2

основании эффективного анализа этих данных необходимо внедрение автоматизированных алгоритмов. При использовании систем обнаружения компьютерных атак в целом эффективность систем защиты информации повышается. На основании данного утверждения, сделаем вывод, что для эффективного применения способов обнаружения атак необходимо использовать алгоритмические модели, которые смогут обеспечить идентификацию образа атаки в соответствии наборам отличительных признаков [2].

Многообразие вариаций неблагоприятных информационных воздействий, которые могут выступать в качестве объектов исследований, нуждается в значительном упрощении для вероятности их модельного представления, при этом учитывая сохранность адекватного представления модели действительному образу атаки.

Адекватное представление модели выражается в двух аспектах:

- Адекватное представление прототипа – корректное описание соответствующей компьютерной атаки.
- Адекватное представление главной цели – использование адекватных мер по борьбе с компьютерными атаками для системы защиты.

В исследованиях, посвященных системам анализа и обнаружения компьютерных атак на объекты КИИ, рассматриваемые методы и методики не имеют достаточного описания с математической стороны. Обычно они представлены в виде функций и средств обнаружения компьютерных атак, которые используются как в инструментальных средствах, так и средствах обнаружения и предупреждения атак. Одним из главных этапов в разработке и внедрении автоматизированных систем в защищенном исполнении различного назначения, в том числе для критических информационных инфраструктур является модельное представление процессов обработки информации и процессов защиты информации, связанных с ними.

4. Полученные результаты

Таким образом, анализ роста по количественным показателям компьютерных атак на информационные системы и потребность в защите объектов КИИ нуждаются в поиске обнаружения атак наиболее эффективным способом и применение имеющего множества средств защиты информации. Разработка модели по обнаружению компьютерных атак на объекты КИИ позволит представить информационную систему с точки зрения функционального подхода, который выполняет задачу поиска полного арсенала состояний безопасности информационной системы [4]. Поиск полного арсенала

ISBN 978-5-6045165-2-2

подобных состояний, допустит определить признаки компьютерной атаки. Дальнейшее рассмотрение характера компьютерной атаки будет проходить на основании системного анализа пространства в системе по предложенным правилам и нахождение тех параметров, характеризующих действия схожей компьютерной атаки.

5. Вывод

В итоге исследования, стоит отметить серьезность и опасность внешних угроз информационной безопасности. На современном этапе развития наиболее важной задачей является создание и поддержка условий для сохранности КИИ РФ в состоянии устойчивости и работоспособности. Значит, при построении и защите от компьютерных атак информационную систему необходимо тщательное осуществление правового регулирования в указанной сфере и разрабатывать модель по обнаружению компьютерных атак.

Список литературы

1. Гамаюнов, Д.Ю. Обнаружение компьютерных атак на основе анализа поведения сетевых объектов: диссертация … канд. физ.-мат. наук: 05.13.11/ Д.Ю. Гамаюнов. – М: Изд-во МГУ им. Ломоносова, 2007. – 89 с.
2. Российская Федерация. Законы. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон № 187-ФЗ: [принят Государственной Думой 12 июля 2017 г.: одобрен Советом Федерации 19 июля 2017 г.]. – Москва, Кремль, 2017. – 20 с.
3. Шабуров, А.С. Модель выявления каналов утечки информации в автоматизированных системах на основе симплекс-метода/ А.С. Шабуров, Е.Е. Журилова // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2017. – № 24. – С. 7-19.
4. Шабуров, А.С. Обнаружение компьютерных атак на основе функционального подхода / А.С. Шабуров, А.А. Миронова// Вестник Пермского университета. Математика. Механика. Информатика. – 2015. – Вып. 4(31). – С. 110-115.

ISBN 978-5-6045165-2-2