DOI: https://doi.org/10.15688/NBIT.jvolsu.2023.1.3

УДК 004.056
ББК 32.973

РАЗРАБОТКА МАТЕМАТИЧЕСКОЙ МОДЕЛИ ОБНАРУЖЕНИЯ ПРОГРАММНЫХ ЗАКЛАДНЫХ УСТРОЙСТВ

Егор Андреевич Жуйков

Ассистент, кафедра информационной безопасности,
Волгоградский государственный университет
zhuikov.egor@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В статье анализируются программные закладные устройства, подходы к выявлению программных закладных устройств, выделены критерии оценки подходов обнаружения программных закладных устройств. Разработана математическая модель обнаружения программных закладных устройств.

Ключевые слова: информационная безопасность, закладное устройство, программное закладное устройство, недекларированные возможности, программное воздействие, техническая защита информации.

В настоящее время защита конфиденциальной информации является основной задачей компаний, так как ее утечка влечет за собой непоправимый ущерб для репутации компании, а также финансовые потери. Для обеспечения защиты конфиденциальной информации от несанкционированного доступа к ней, компании используют специальный комплекс мер, в который входят технические, программные, программно-аппаратные и административные меры защиты информации.

Одним из способов получения конфиденциальной информации являются программные закладные устройства, которые могут попасть в систему различными способами. Чтобы выявить такие устройства на рабочих местах необходимо использовать специальные методы.

Основываясь на статистике компании Positive Technologies за 2020 г., хищение конфиденциальной информации с использованием средств стороннего ПО возросло до 54 %. В них входит использование шпионского ПО (24 % у организаций, 50 % у частных лиц), ВПО для удаленного подключения (18 % у организаций, 16 % у частных лиц), загрузки (12 % у организаций, 14 % у частных лиц), троян (11 % у организаций, 22 % у частных лиц), рекламное ПО (1 % у организаций, 13 % у частных лиц). Опираясь на статистику, можно сделать вывод, что в большинстве случаев утечка конфиденциальной информации происходит с помощью программных закладок. Для того чтобы защитить конфиденциальную информацию необходимо регулярную проводить проверку систем на наличие программных закладных устройств [1].

Сложность обнаружения программных закладных устройств заключается в том, что нет единого метода обнаружения, и приходится использовать различные средства и способы для поиска и обнаружения программных закладных устройств.

Программное закладное устройство – преднамеренно внесенный в программное обеспечение функциональный объект, который при определенных условиях инициирует реализацию недекларированных возможностей программного обеспечения [2].

Исходя из определения, можно сделать вывод, что основное предназначение программного закладного устройства состоит в том, чтобы обеспечить несанкционированный доступ к информации.

Существуют два способа реализации программных закладных устройств (рис. 1):

1. Вредоносная программа;

2. Программный код.

Особенностью данных программных закладных устройств является то, что они могут быть частью системы и задействовать меры по маскировке своего нахождения. При внедрении программного закладного устройства в систему создается скрытый канал для обмена информацией. Такой канал может находиться незамеченным в течение длительного времени.

Программные закладные устройства можно поделить на три группы по воздействию, которое они могут осуществлять (рис. 2):

1. Копирование информации пользователя компьютерной системы, находящейся в оперативной или внешней памяти этой системы.

2. Изменение алгоритмов функционирования системных, прикладных, служебных программ.

3. Навязывание определенных режимов работы.

Также программные закладные устройства можно классифицировать по методу внедрения их в компьютерную систему (рис. 3) [4; 5]:

1. Программно-аппаратные закладки, данные программные закладные устройства встраиваются в BIOS.

2. Загрузочные закладки, такие программные закладные устройства находятся в загрузочных секторах жесткого диска и начинают работу с программами начальной загрузки.

3. Драйверные закладки, программные закладные устройства данного типа связаны с драйверами устройств.

4. Прикладные закладки.

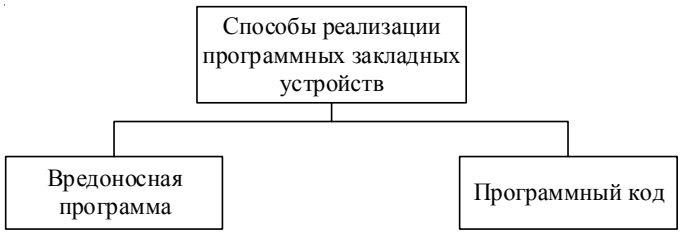

Рис. 1. Способы реализации программных закладных устройств

Рис. 2. Группы воздействия программах закладных устройств

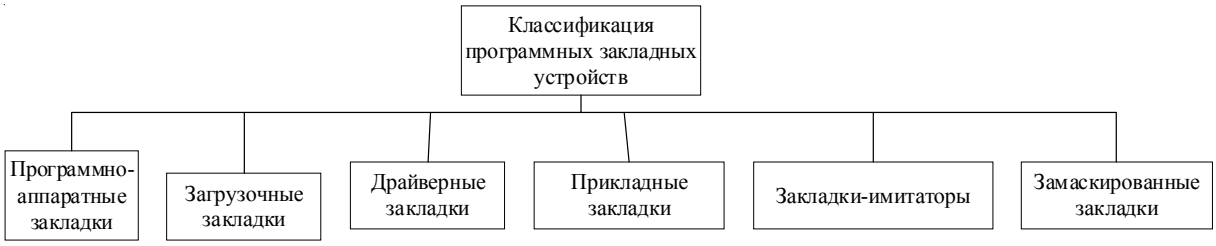

Рис. 3. Классификация программных закладных устройств

5. Закладки-имитаторы.

6. Замаскированные закладки.

Для защиты информации от программных закладных устройств, предприятия могут использовать два метода защиты – это использование организационных мер защиты и создание изолированной программной среды (рис. 4).

Исходя из всего вышесказанного, можно сделать вывод, что программные закладные устройства могут искажать и уничтожать информацию, нарушать работу системы, собирать и отправлять информацию злоумышленнику.

Также можно сделать вывод, что какого-либо универсального подхода эффективной защиты от программных закладных устройств не существует.

Чтобы определить наиболее подходящий подход к обнаружению программных закладных устройств, необходимо рассмотреть все существующие подходы обнаружения.

Выявление программах закладных устройств производится путем обнаружения признаков их присутствия в системе. Поэтому условно можно обозначить два подхода, со следующими названиями (рис. 5):

1. Качественный и визуальный подход [3; 6].

Данный подход основывается на признаках, которые могут быть обнаружены пользователем в системе. Такими признаками могут быть как отклонения в работе системы, так и изменения в пользовательских и системных файлах. Также к признакам, что в системе может находиться программное закладное устройство, можно отнести наличие в системе файлов «призраков».

2. Обнаружение средствами тестирования и диагностики [3; 6].

Суть данного подхода заключается в автоматическом поиске и нахождении вредоносного кода, наблюдении за активными

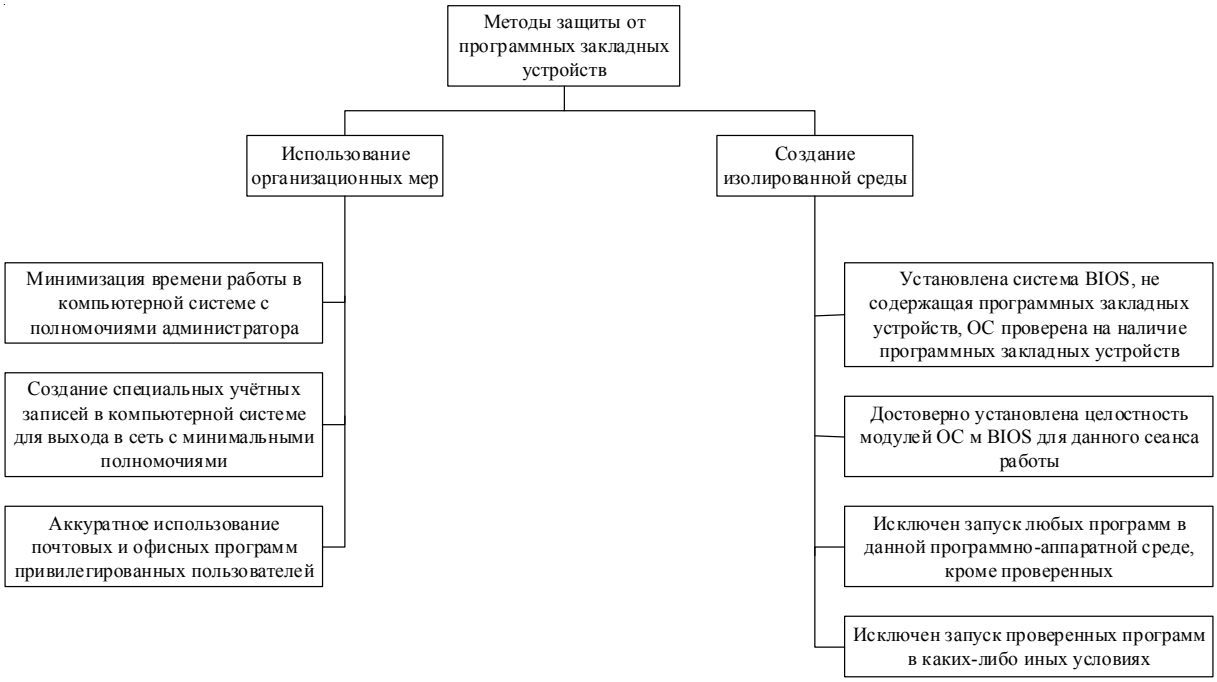

Рис. 4. Методы защиты от программных закладных устройств

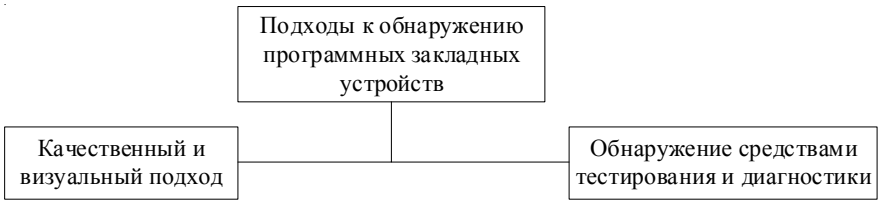

Рис. 5. Подходы к обнаружению программных закладных устройств

процессами, наблюдении за IP-портами, просмотре разделов реестра и выявлении установленных программ, проверке журнала событий.

Для выбора наилучшего подхода к обнаружению программных закладных устройств необходимо определить критерии для оценки данных подходов:

Критерий 1. Объем. Данный критерий определяет объем обрабатываемой информации.

Критерий 2. Автоматическое нахождение. Данный критерий определяет возможность автоматизации нахождения программной закладки.

Критерий 3. Использование стороннего ПО. Данный критерий определяет возможность использовать стороннее ПО для нахождения программной закладки.

Критерий 4. Время. Данный критерий определяет время нахождения программной закладки.

Критерий 5. Надежность. Данный критерий определяет возможность возникновения ошибок при обнаружении программной закладки.

Проведем сравнительный анализ подходов к обнаружению программных закладок по выделенным критериям. В таблице представлены обозначения «1» – критерий выполняется, «0» – критерий не выполняется.

Исходя из сравнительного анализа подходов к обнаружению программных закладных устройств по выделенным критериям, выявлено, что наиболее соответствующий подход – «Обнаружение средствами тестирования и диагностики». Однако необходимо дополнить, что оба этих подхода важны и связанны между собой.

Исходя из результатов сравнительного анализа, мы будем разрабатывать метод обнаружения программных закладных устройств, который будет включать в себя два этих подхода.

Функциональную модель обнаружения программных закладных устройств можно представить в виде диаграммы, приведенной на рисунке 6.

В общем виде обнаружение программных закладных устройств состоит из следующих этапов, представленных на рисунке 7.

В общем виде обнаружение программных закладных устройств состоит из следующих этапов:

1. Вычисление средних показателей нагрузки на систему на основании ее загруженности.

2. Формирование списка исключений на основании сведений об установленных программах.

3. Сканирование системы на наличие программных закладных устройств на основании средней нагрузки на систему и списка исключений.

Процесс обнаружения программных закладных устройств осуществляется на протяжении всего рабочего времени системы с момента ее запуска до выключения.

Для корректного обнаружения предварительно выполняется этап анализа системы. При этом формируется:

множество $PO_{isk} = \{po_{isk1},...,po_{iskn}\}$ – множество программного обеспечения, установленного в системе, где n – количество установленного программного обеспечения, n>1;

CP_{isk} – максимально допустимое значение загруженности процессора, формируемое на этапе анализа системы;

Сравнительный анализ подходов к обнаружению программных закладных устройств

Критерий	Подход	
	Качественный и визуальный подход	Обнаружение средствами тестирования и диагностики
Объем	0	1
Автоматическое нахождение	0	1
Использование стороннего ПО	1	1
Время	1	0
Надежность	0	1
Итог	0,4	0,8

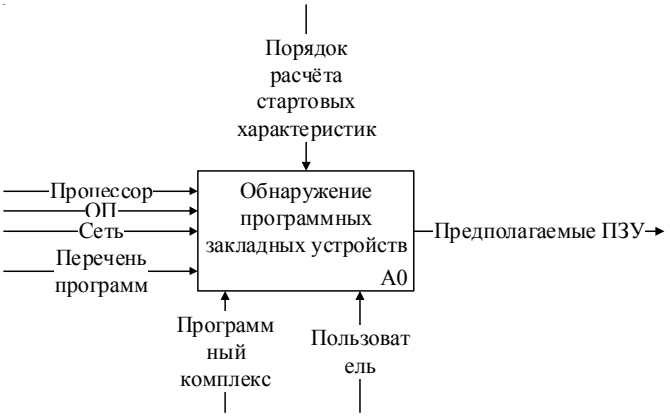

Рис. 6. Функциональная модель обнаружения программных закладных устройств

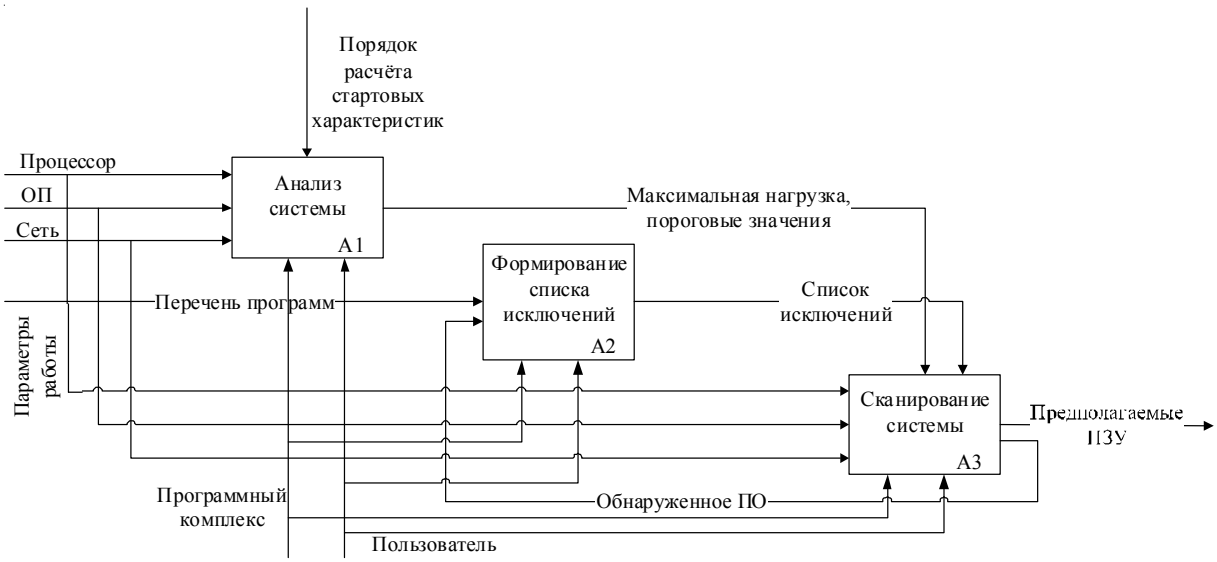

Рис. 7. Функциональная модель обнаружения программных закладных устройств

OZ_{isk} – максимально допустимое значение загруженности оперативной памяти, формируемое на этапе анализа системы;

NT_{isk} – максимально допустимая скорость отправки данных через сетевой интерфейс, формируемая на этапе анализа системы.

По завершению этапа анализа системы максимально допустимые значения становятся равными 1.

Непосредственно при обнаружении программных закладных устройств формируется:

Множество $PO_{rea} = \{po_{rea1},...,po_{reaq}\}$ – множество программного обеспечения, где q – количество установленного программного обеспечения в момент сканирования системы, $q > 1$;

CP_{rea} – значение нагрузки на центральный процессор, получаемое на текущий момент времени;

OZ_{rea} – значение нагрузки на оперативную память, получаемое на текущий момент времени;

NT_{rea} – значение скорости отправки данных по сети, получаемое на текущий момент времени.

Считается, что потенциальное программное закладное устройство внедрено в систему, если выполняется одно из следующих условий:

1. Множество программного обеспечения, уставленного в системе в момент сканирования, превышает эталонное множество программного обеспечения, установленного в системе.

2. Значение нагрузки на центральный процессор на текущий момент времени превышает эталонное значение нагрузки на центральный процессор.

3. Значение нагрузки на оперативную память на текущий момент времени превышает эталонное значение нагрузки на оперативную память.

4. Значение скорости отправки данных через сетевой интерфейс на текущий момент времени превышает эталонное значение скорости отправки данных через сетевой интерфейс.

Для принятия решения о том, имело ли место внедрение программного закладного устройства, вычисляются результаты сравнений:

$$PO^* = \begin{cases} 0, \text{если } PO_{isk} = PO_{rea}, \text{следовательно,} \\ \text{изменений в составе ПО не обнаружено;} \\ 1, \text{если } PO_{isk} < PO_{rea}, \text{следовательно,} \\ \text{изменения в составе ПО обнаружены;} \end{cases}$$

случай, когда не рассматривается, так как администратором проводится плановый периодический контроль установленного ПО после обновления или установки ПО.

$$CP^* = \begin{cases} 0, \text{если } CP_{isk} \geq CP_{rea}, \text{следовательно, превышение} \\ \text{нагрузки на центральный процессор не обнаружено;} \\ 1, \text{если } CP_{isk} < CP_{rea}, \text{следовательно, обнаружено} \\ \text{превышение нагрузки на центральный процессор;} \end{cases}$$

$$OZ^* = \begin{cases} 0, \text{если } OZ_{isk} \geq OZ_{rea}, \text{следовательно, превышение} \\ \text{нагрузки на оперативную память не обнаружено;} \\ 1, \text{если } OZ_{isk} < OZ_{rea}, \text{следовательно, обнаружено} \\ \text{превышение нагрузки на оперативную память;} \end{cases}$$

$$NT^* = \begin{cases} 0, \text{если } NT_{isk} \geq NT_{rea}, \text{следовательно, превышение} \\ \text{скорости отправки данных не обнаружено;} \\ 1, \text{если } NT_{isk} < NT_{rea}, \text{следовательно, обнаружено} \\ \text{превышение скорости отправки данных;} \end{cases}$$

После получения всех результатов рассчитывается:

$$F = PO^* \vee CP^* \vee OZ^* \vee NT^*$$

Значение F интерпретируется следующим образом:

$$F = \begin{cases} 0 - \text{потенциальное ПЗУ не обнаружено;} \\ 1 - \text{потенциальное ПЗУ обнаружено;} \end{cases}$$

Так как обнаружение программных закладных устройств происходит на протяжении всего рабочего времени системы, то при F = 0 осуществляется повторный мониторинг в соответствии с вышеописанным процессом обнаружения программных закладных устройств, до момента, при котором F = 1, или выключения системы.

СПИСОК ЛИТЕРАТУРЫ

1. Актуальные киберугрозы: итоги 2020 года // Positive Technologies. – Электрон. текстовые дан. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/

2. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения // Электронный фонд правовой и нормативно-технической информации – docs.cntd.ru. – Электрон. текстовые дан. – Режим доступа: https://docs.cntd.ru/document/1200057516

3. Методы защиты от программных закладок // Хелпикс. – Электрон. текстовые дан. – Режим доступа: https://helpiks.org/9-27388.html

4. Программная закладка // Википедия – свободная энциклопедия. – Электрон. текстовые дан. – Режим доступа: https://ru.wikipedia.org/wiki/Программная_закладка

5. Программные закладки // Файловый архив для студентов. StudFiles. – Электрон. текстовые дан. – Режим доступа: https://studfile.net/preview/4339469/page:15/

6. Способы обнаружения присутствия программных закладок // Профтемы студенту и преподавателю. – Электрон. текстовые дан. – Режим доступа: http://taketop.ru/articles/infor-bezop/zashitakompin/sposobu-obnar

REFERENCES

1. Aktualnye kiberugrozy: itogi 2020 goda [Current Cyber Threats: 2020 Results]. *Positive Technologies*. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/.

2. GOST R 51275-2006 Zashhita informacii. Objekt informatizacii. Faktory, vozdejstvujushhie na informaciju. Obshhie polozhenija [GOST R 51275-2006 Information Protection. Object of Informatization. Factors Affecting Information. General Provisions]. *Elektronnyj fond pravovoj i normativno-tehnicheskoj informacii* [Electronic Legal and Regulatory Technical Information Fund]. URL: https://docs.cntd.ru/document/1200057516

3. Metody zashhity ot programmnyh zakladok [Methods of Protection Against Implants]. *Helpiks* [Helpix – Internet Assistant]. URL: https://helpiks.org/9-27388.html

4. Programmnaja zakladka [Implant Tool]. *Vikipedija – svobodnaja jenciklopedija* [Wikipedia – Free Encyclopedia]. URL: https://ru.wikipedia.org/wiki/Программная_закладка

5. Programmnye zakladki [Software Backdoors]. *Fajlovyj arhiv dlja studentov. StudFiles*

[File Archive for Students. StudFiles]. URL: https://studfile.net/preview/4339469/page:15/

6. Sposoby obnaruzhenija prisutstvija programmnyh zakladok [Methods of Detecting the Presence of Software Backdoors]. *Proftemy studentu i prepodavatelju* [Profthems to the Student and Teacher]. URL: http://taketop.ru/articles/infor-bezop/zashitakompin/sposobu-obnar

DEVELOPMENT OF A MATHEMATICAL MODEL FOR DETECTING SOFTWARE BACKDOORS

Egor A. Zhuikov

Assistant, Department of Information Security,
Volgograd State University
zhuikov.egor@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. This article analyzes software backdoors that can be used to illegally access information or collect confidential data. To detect such backdoors, various approaches were considered that make it possible to identify the presence of backdoors in the system. During the study, criteria were highlighted that allow assessing the effectiveness of various approaches to detecting software backdoors. These include detection accuracy, data processing speed, resistance to circumvention of protective measures and other factors. Currently, the protection of confidential information is the main task of companies, since its leakage entails irreparable damage to the company's reputation, as well as financial losses. To ensure the protection of confidential information from unauthorized access to it, companies use a special set of measures, which includes technical, software, hardware and administrative measures to protect information. One of the ways to obtain confidential information is software backdoors that can enter the system in various ways. To identify backdoors at workplaces, special methods must be used. In general, this article represents an important contribution to the field of detection of software backdoors and can be used in the development of new methods of information protection.

Key words: information security, backdoor, software backdoor, undeclared capabilities, software impact, technical protection of information.