УДК 004.056
DOI 10.34822/1999-7604-2021-4-16-21

ИНФОРМАЦИОННАЯ СИСТЕМА КОСВЕННОГО МОНИТОРИНГА НЕСАНКЦИОНИРОВАННОЙ АКТИВНОСТИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

К. И. Бушмелева, А. В. Гавриленко, А. В. Никифоров ✉
Сургутский государственный университет, Сургут, Россия
✉*E-mail: nikiforov_av@surgu.ru*

Представлен метод непрерывного мониторинга несанкционированной активности на основе косвенных параметров вычислительной системы как средство обеспечения ее безопасности, рассмотрена архитектура информационной системы косвенного мониторинга, изучены особенности реализации ее подсистем по принципу инверсии управления, определена возможность интеграции с уже существующими системами защиты за счет гибкости и масштабируемости, а также проанализированы дальнейшие перспективы ее развития.

Ключевые слова: косвенный мониторинг, несанкционированная активность, вычислительные системы, системы защиты информации, инверсия управления.

INFORMATION SYSTEM FOR INDIRECT MONITORING OF UNAUTHORIZED ACTIVITY IN THE COMPUTER SYSTEMS

K. I. Bushmeleva, A. V. Gavrilenko, A. V. Nikiforov ✉
Surgut State University, Surgut, Russia
✉*E-mail: nikiforov_av@surgu.ru*

The method of continuous monitoring of unauthorized activity based on indirect parameters of the computing system as a means of ensuring its security is presented. The architecture of the information system of indirect monitoring is considered. The features of the implementation of its subsystems on the principle of inversion of control are studied. The possibility of integration with existing protection systems due to flexibility and scalability is determined, and further prospects for its development are analyzed.

Keywords: indirect monitoring, unauthorized activity, computing systems, information security systems, inversion of control.

Введение

Информационная безопасность играет важную роль в современном обществе, и на ее обеспечение государственные институции и частные компании не жалеют ни времени, ни средств, поскольку утечка информации из области, связанной с военно-промышленным комплексом, является угрозой национальной безопасности, а для коммерческих структур это не только потеря дохода, но и репутационные риски. Поэтому средства защиты обычно объединяют в систему, обеспечивающую информационную безопасность на аппаратном и программном уровне.

Классическими методами борьбы с несанкционированной активностью на программном уровне являются антивирусные средства, алгоритмы шифрования и пр., осуществляющие прямой мониторинг операционных систем на уязвимость и наличие вредоносного и «мусорного» программного обеспечения (навязанного пользователю без его согласия при установке другого программного обеспечения), но с учетом появления все новых способов взлома и обхода средств защиты информации безопасность и стабильность работы этих систем не гарантирована [1–6].

Методами борьбы с несанкционированной активностью на аппаратном уровне являются шифраторы, дешифраторы и пр., при этом методов прямого мониторинга несанкциони-

рованной активности аппаратного обеспечения не существует. Например, аппаратные уязвимости Meltdown и Spectre в процессорах ведущих компаний позволяют выполнять вредоносный код в обход всех программных средств защиты, поскольку никто, кроме производителя, не имеет принципиальной схемы устройств и никто не знает, каким функционалом обладает устройство и зашитое в него программное обеспечение [7–12].

Перечисленные проблемы требуют разработки и создания новых методов и средств повышения степени защищенности информации, а информационная система косвенного мониторинга вычислительной системы сможет дополнить уже существующие системы безопасности по определению несанкционированной активности.

Мониторинг несанкционированной активности на основе косвенных параметров вычислительной системы

В основе информационной системы косвенного мониторинга несанкционированной активности лежит принцип непрерывного мониторинга косвенных параметров работы вычислительной системы.

Во время работы информационная система косвенного мониторинга получает информацию от программных (объем памяти, используемый процессом, время работы процесса, наличие сетевого трафика у процесса и пр.) и аппаратных (температура, загруженность, энергопотребление и пр.) компонентов вычислительной системы для проведения анализа косвенных показателей и оценки ее текущего состояния. Полученная оценка влияет на принимаемое решение о наличии несанкционированной активности в программных или аппаратных компонентах вычислительной системы и типе действий для противодействия такой активности для исключения вторжения в ее компоненты [13].

Такого рода косвенный мониторинг вычислительной системы можно сравнить с определением заболевания у человека по изменению различных показателей, например температуры тела, потоотделения, цвета кожи и т. д. Вычислительная система так же, как человек, имеет значения нормы для различных параметров, поэтому их мониторинг позволит определить наличие несанкционированной активности.

Алгоритм мониторинга косвенных параметров заключается в однократном опросе программных и аппаратных компонентов вычислительной системы в определенный период времени и сохранении его результатов в базе данных для использования в аналитическом модуле системы. И если для сбора информации от программных компонентов вычислительной системы могут использоваться только программные средства, то для сбора информации от аппаратных компонентов существует два способа: программный и аппаратный.

Программный сбор показателей осуществляется, если аппаратная часть вычислительной системы предоставляет информацию о параметрах оборудования (температуре, энергопотреблении и т. д.). Сначала производится загрузка драйверов для аппаратной части вычислительной системы, а затем с их помощью происходит обращение к аппаратной части для получения информации о параметрах оборудования [13].

Если аппаратная часть вычислительной системы не предоставляет информацию о параметрах оборудования, осуществляется аппаратный сбор показателей по алгоритму программного, но с одним исключением. Сначала устанавливается дополнительное аппаратное обеспечение, которое позволяет производить мониторинг требуемых параметров оборудования, а затем происходит переход на первый этап алгоритма работы программного сбора [13].

Поэтому при проектировании архитектуры информационной системы учитывается не только алгоритм мониторинга косвенных параметров, но и особенности методов сбора показателей.

Архитектура информационной системы косвенного мониторинга несанкционированной активности в вычислительной системе

Следует учесть, что большое значение имеет создание качественной архитектуры информационной системы для возможности ее модификации в дальнейшем с целью решения проблемы устаревания. Одной из причин устаревания может стать сильная зависимость реализаций компонентов системы друг от друга в исходном коде. Решить данную проблему при написании исходного кода информационной системы можно, применив инверсию управления, а именно используя внедрение зависимостей.

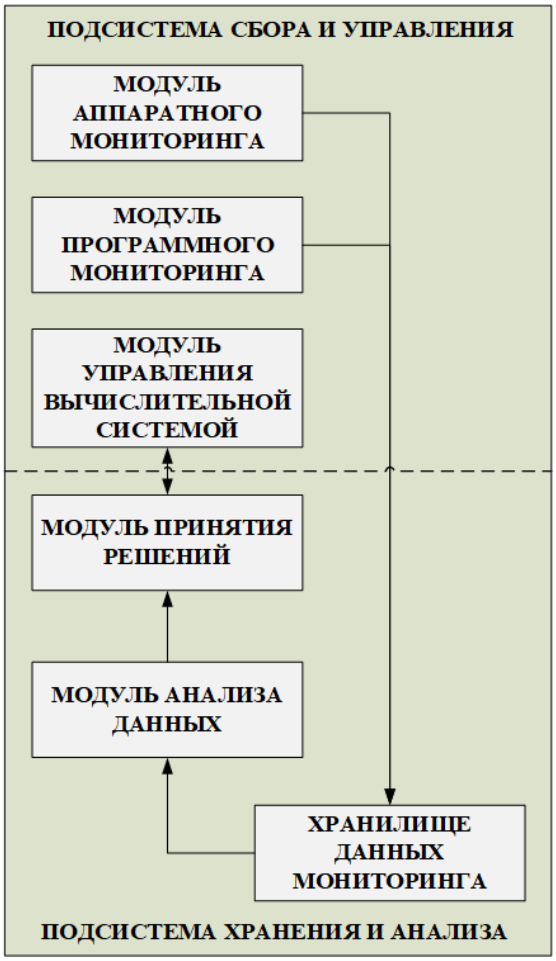

Рис. 1. Архитектура информационной системы косвенного мониторинга несанкционированной активности
Примечание: рисунок авторов.

На рис. 1 представлена архитектура информационной системы косвенного мониторинга несанкционированной активности со всеми компонентами (модулями) и связями между ними [14]. Информационная система состоит из двух подсистем: 1) сбор и управление; 2) хранение и анализ. Каждая из подсистем содержит модули различного назначения. Подсистема сбора и управления содержит следующие модули:

1. Мониторинг аппаратного обеспечения.
2. Мониторинг программного обеспечения.
3. Управление вычислительной системой.

Модули подсистемы хранения и анализа:

1. Хранение данных мониторинга (база данных, содержащая косвенные параметры работы вычислительной системы).

2. Анализ данных мониторинга (комплекс моделей или алгоритмов проверки наличия несанкционированной активности).

3. Принятие решений.

Учитывая архитектуру информационной системы, выделим три причины для использования в системе инверсии управления и внедрения зависимостей:

1. Поддержка двух способов мониторинга аппаратных компонентов вычислительной системы (программного и аппаратного).

2. Особенности устройства операционных систем (Windows, Linux и MacOS) при мониторинге программных и аппаратных компонентов (наличие платформозависимого кода).

3. Возможность одновременного создания как клиентского, так и клиент-серверного приложения.

Первые две причины очевидны и следуют из алгоритмов сбора косвенной информации о работе вычислительной системы, однако третья заслуживает отдельного рассмотрения. Если соблюсти правильную компоновку модулей по библиотекам и разработать для каждого модуля стандартизированный интерфейс взаимодействия, можно получить информационную систему, которая построена из набора модулей, связанных друг с другом средствами абстракции. Следовательно, за счет абстрагирования от деталей можно выстроить информационную систему, способную к динамическому перестроению, в которой каждый модуль не зависит от деталей реализации других модулей благодаря инверсии управления, абстракции, стандартизированным интерфейсам, поддержке современными языками программирования динамической загрузки модулей и работе с ними. Это позволяет отделить подсистему «Сбор и управление» от подсистемы «Хранение и анализ», что дает возможность получить два вида приложений (клиентское и клиент-серверное) для информационной системы косвенного мониторинга несанкционированной активности в вычислительной системе, имея однократно написанный код. Наличие двух видов приложений добавляет гибкости информационной системе мониторинга при использовании и открывает перед ней возможность интеграции с уже существующими у клиентов системами защиты информации (рис. 2).

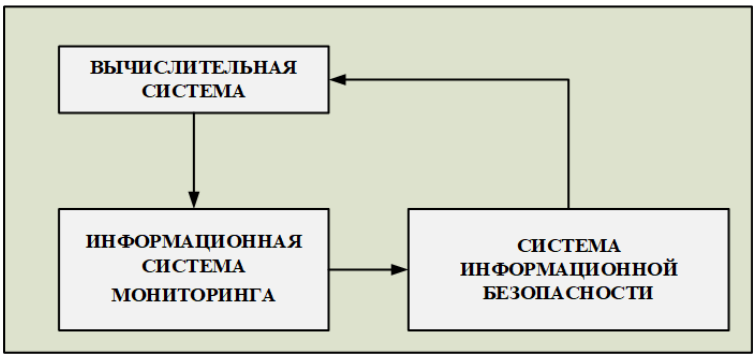

Рис. 2. Схема работы информационной системы мониторинга в рамках существующей системы безопасности
Примечание: рисунок авторов.

В данной статье не будет представлена детальная реализация описанного выше подхода по созданию динамически перестраиваемой информационной системы косвенного мониторинга несанкционированной активности в связи с общедоступностью механизмов и инструментов языка программирования, выбранного для реализации данной информационной системы.

Заключение

В перспективе рассматривается создание информационной системы на основе описанного метода мониторинга и архитектуры для получения косвенных параметров работы вычислительной системы с целью их накопления в базе данных для анализа и выявления за-

кономерностей при различных сценариях работы и их применения при создании моделей или алгоритмов модуля «Анализ данных», способных определить несанкционированную активность в вычислительной системе и оказать на нее управляющее воздействие при помощи модуля «Управление вычислительной системой» в реальном времени. Данный модуль на основе оценки, полученной из модуля «Анализ данных», будет принимать действия, направленные на предотвращение несанкционированной активности в вычислительной системе. Данные действия могут быть либо полностью автоматическими (настроенными по заранее описанному человеком сценарию), либо могут осуществляться с непосредственным участием человека.

Информационная система косвенного мониторинга несанкционированной активности в вычислительной системе имеет огромный потенциал за счет универсальности метода, который возможно применить для большинства вычислительных систем либо адаптировать под параметры конкретной вычислительной системы, а сочетание такой системы с классическими средствами информационной безопасности позволит повысить эффективность защиты от несанкционированной активности и в значительной степени снизить количество случаев хищения конфиденциальной информации.

Литература

1. Гужанков Е. Г., Воробьев Д. С, Уваровский В. В. Алгоритм атаки через микроархитектурную уязвимость процессоров MELTDOWN // Новое слово в науке: стратегии развития : сб. материалов V Междунар. науч.-прак. конф., 18 июня 2018 г. Чебоксары : Центр научного сотрудничества «Интерактив плюс», 2018. С. 153–156.

2. Гужанков Е. Г., Воробьев Д. С, Уваровский В. В. Уязвимости MELTDOWN и SPECTRE микропроцессоров производителей AMD, ARM и INTEL // Науч. исслед. и современ. образование : сб. материалов V Междунар. науч.-прак. конф., 18 июня 2018 г. Чебоксары : Центр научного сотрудничества «Интерактив плюс», 26 марта 2018 г. Чебоксары : Центр научного сотрудничества «Интерактив плюс», 2018. С. 213–215.

3. Карганов В. В., Левченко Г. Н. К вопросу о существующих методах защиты информации в информационных системах // Материалы конф. ГНИИ «Нацразвитие». 2017. С. 108–117.

4. Садилов А. В., Гонтовой С. В. О проблемах информационной безопасности, связанных с устранением уязвимостей MELTDOWN и SPECTRE // Автоматизир. системы управления и информ. технологии : материалы всерос. науч.-тех. конф., 17 мая 2018 г. Пермь : Перм. национал. исслед. политех. ун-т, 2018. С. 315–321.

5. Списивцев С. А. О проблемах информационной безопасности в современной России // Проблемы соврем. педагог. образования. 2019. № 63. С. 314–316.

6. Шелупанов А. А., Евсютин О. О. Актуальные направления развития методов и средств защиты информации // Докл. Томск. гос. ун-та систем управления и радиоэлектроники. 2017. № 3. С. 11–24.

7. Федунец Н. И., Приходько М. А. Проблема несанкционированной утечки информации в инфокоммуникационных мультиагентных системах // Прикаспийск. журн.: управление и высокие технологии. 2011. № 2. С. 13–16.

8. Москвин Д. А., Печенкин А. И. Обнаружение и предотвращение несанкционированной отправки данных из локальной сети // Безопасность информ. технологий. 2010. Т. 17, № 1. С. 95–97.

9. Дудоров Е. Н. Возможные варианты построения интеллектуальной системы обнаружения несанкционированной работы программного обеспечения // Математ. структуры и моделирование. 2005. № 15. С. 116–124.

10. Жукова П. Н., Насонова В. А., Ходякова Н. В. О некоторых средствах защиты информационных систем от несанкционированного доступа // Проблемы правоохран. деятельности. 2015. № 2. С. 83–88.

11. Бойченко О. В., Васильева Д. О. Проблемы несанкционированных операций с использованием платежных карт // Экономика строительства и природопользования. 2019. № 1. С. 40–48.

12. Гавриленко Т. В., Никифоров А. В. Методы косвенного мониторинга несанкционированной активности в вычислительных системах // Вопр. технич. и физ.-матем. наук в свете современ. исслед. М., 2020. Т. 3–4 (20). С. 38–45.

13. Бушмелева К. И., Гавриленко Т. В., Никифоров А. В. Использование инверсии управления и внедрения зависимостей в архитектуре системы косвенного мониторинга несанкционированной активности // Инновационные, информационные и коммуникационные технологии : сб. тр. XVII Междунар. науч.-практич. конф. М., 2020. С. 21–24.

14. Уваров А. Н. Инверсия управления и внедрение зависимостей // Символ науки. 2019. № 10-1. С. 28–32.