ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 28 МАТЕМАТИКИ Выпуск 2
2021

С. Ж. Симаворян, **А. Р. Симонян**, **Е. И. Улитина**, **Г. А. Попов** (Сочи, СГУ, Астрахань, АГТУ). **Методы аварийного противодействия вторжениям в информационных системах.**

УДК 004.02

Резюме: В процессе противодействия как известных, так и ранее неизвестных вторжений (угроз) в информационных системах используются специальные процедуры нейтрализации (локализации и ликвидации), относящиеся к классу аварийных. Основная особенность аварийных ситуаций — жесткие временные ограничения на время реакции и противодействия атакам. По этой причине основным ограничением для всех реализуемых процедур является время их реализации. Все процедуры, время реализации которых больше допустимого, отбрасываются вне зависимости от того, какими бы эффективными и замечательными они не были. Наиболее опасные ситуации — когда вторжения не оставляют никаких следов, системы поиска вторжений никак не реагируют на реальное вторжение. Поэтому, в этой связи, требуется провести системный анализ методов аварийного противодействия вторжениям и включить новые методы, помогающие поиску вторжений, на которые система информационной безопасности своевременно не среагировала.

Ключевые слова: скрытая атака, информационная безопасность, система обнаружения вторжений, системный подход.

В настоящее время, создан довольно большой арсенал эффективных методов и средств по поиску/противодействию известных угроз (атак) на информационные системы, и механизмы по обнаружению новых. Но для того, чтобы обойти систему защиты, злоумышленники разрабатывают средства (программы), которые проникают в информационную систему и носят скрытый характер. Возникает ситуация, когда вторжение напрямую с его параметрами и локацией в системе не обнаруживает себя, его местонахождение почти неизвестно, и может быть, на его наличие указывают лишь отдельные его следы. Поэтому проведение процедур общесистемного профилактического характера с применением соответствующих методов крайне необходимо делать на регулярной основе. Перечислим некоторые из этих мероприятий (методов), обеспечивающих противоборство предполагаемой или реальной атаке/вторжению. То есть часть мероприятий данного перечня может проводиться и в случае предположения о возможном совершении злонамеренного вторжения (см. [1]–[5]).

1. Полный контроль доступа. Проникшее вторжение может иметь связи с другими программами или компонентами в системе обработки данных, эти связи могут быть внутренними и внешними. Поэтому резкое ужесточение контроля доступа на уровне всех активных процессов может существенно ограничить возможности вторжения. При этом, однако, необходимо учитывать требования по затратам времени на действия по контролю.

2. Блокировка отдельных узлов, разделов на ПК, подсистем, технических компонентов, всех некритичных связей и т. д. Данное действие может обеспечить режим изолирования вторжения, тем самым ограничить его возможности по распространению своего вредоносного воздействия. Данная процедура требует предварительной

программно-аппаратной подготовки систем информационной безопасности и обработки данных по избежание возникновения нежелательных ситуаций.

3. Максимально полное, насколько возможное прекращение процессов обработки данных и отключение всех подсистем и программно-аппаратных средств, связанных с этой обработкой. Данная процедура сузит возможности вторжения по всем возможным его действиям и путям распространения.

4. Отключение всех некритичных внешних связей для максимально ограничения возможностей вторжения по передаче данных и получению управляющих указаний извне.

5. Информирование всех органов и должностных лиц в соответствии с установленным регламентом о сложившейся ситуации. Соответствующие инструктивные материалы, фиксирующие правила и процедуры действий при аварийных ситуациях должны быть прописаны заранее в соответствующих нормативных документах согласно установленной частной политики.

6. Создание системы предварительно подготовленной совокупности ловушек для вторжения с целью зафиксировать его наличие, если до этого оно не было выявлено, принят меры по его идентификации и реализации процедур противодействия.

7. Как крайняя мера: уничтожение всех информационных ресурсов, которые могут представлять интерес для вторжения, исходя из принципа: ни в коем случае к злоумышленнику данные не должны попасть. Иногда лучше уничтожить ценную информацию, чтобы она не попала в руки к злоумышленнику. Принятие на «вооружение» данного принципа предполагает проведение целой серии подготовительных мероприятий, связанной с созданием копий и разработки технологии их создания, хранения, обновления, архивирования и активизации. Также целесообразно разработать и алгоритмизировать процедуру их восстановления (возможно, даже ручного) в случае неудовлетворительного состояния с копированием и/или копиями. В настоящее время имеются требуемые технологии по организации процедуры создания и хранения копий с описанием процедур нахождения требуемых параметров, в частности, частоты копирования, количества копий, мест их хранения (см. [6]).

Непосредственно процесс обнаружения вторжений после совершения всех требуемых мероприятий по локализации вторжения, и ликвидации его последствий, в том числе и из списка перечисленных выше мер, опирается на рассмотренные выше процедуры обнаружения вторжений; прежде всего, опирающиеся на поиск аналогов, прецедентов, мнения компетентных в этой сфере экспертов.

Рассмотрим теперь более опасную ситуацию, когда вторжение не оставляет никаких следов, системы поиска вторжений никак не реагируют на реальное вторжение. В этом случае процесс поиска вторжений может опираться на реализуемый в непрерывном режиме времени процесс слепой профилактики. Опишем некоторые методы, которые могут быть включены в этот процесс поиска вторжений.

Первый метод — это метод тотального (полного) просмотра всех имеющихся в информационной системе файлов — назовем его методом облавы по аналогии с аналогичными действиями службы защиты. То есть неожиданным для внешнего окружения образом блокируется определенная группа файлом в оперативной или жесткой памяти. Блокируется означает, что эти файлы полностью лишаются возможности контактов с операционной средой. Для файлов, находящихся в оперативной памяти, эта ситуация может оказаться нежелательной и даже критичной, поскольку некоторые из этих файлов могут в текущий момент активно функционировать и быть востребованными. Поэтому возникает новое требование к операционной системе: обеспечить возможность ее функционирования в подобных условиях, возможно, с помощью замены блокированных файлов на альтернативные. Еще одно требование по данному методу: необходимо быть уверенным, что процессоры полностью подконтрольны операционной системе и не перехвачены сторонней программой. Поэтому программы, реализующие данный метод (назовем ее программой выявления атаки), должны обеспечить условия под-

контрольности процессора, с возможной перезагрузкой компьютера после реализации процедуры блокирования.

Второй метод — это метод систематического случайного мониторинга отдельных программ, программных систем и программно-технических устройств на предмет выявления в них возможных отклонений от предписанных значений. Непосредственно механизм выбора очередного файла или другого объекта для мониторинга и выявления вторжения должен опираться на предшествующий опыт его реализации. И этот механизм должен содержать случайные элементы во избежание крайнего случая, когда сам механизм станет полностью известен злоумышленнику. Наличие случайности в реализации метода не даст злоумышленнику полных гарантий, что механизм поиска не коснется его файлов. Данный метод может быть реализован на основе обучаемых специальным образом нейронных сетей.

Третий метод — метод выявления неизвестных вторжений, опирающийся на аналитическое исследование отклонений в результатах работы системы в целом, на анализ общесистемных характеристик. Данный метод больше пригоден при выявление уже реализованных скрытых вторжений, поскольку его эффективная реализация требует значимых затрат времени. Выявление факта совершения вторжения постфактум также очень актуально, поскольку позволяет принять определенные меры по уменьшению потерь, связанных с данным вторжением.

Приведенные методы поиска неизвестных вторжений опираются на реализуемый в непрерывном режиме времени процесс слепой профилактики. Такой подход позволяет более эффективно реализовывать методы аварийного противодействия вторжениям в информационных системах.

Благодарности. Работа выполнена при финансовой поддержке гранта РФФИ № 19-01-00383.

СПИСОК ЛИТЕРАТУРЫ

1. *Кленин Д. В.*, *Максимова Е. А.* Модель вторжений в информационную систему/ NBI technologies: научно-теоретический журнал / учредитель и издатель: Федеральное государственное автономное образовательное учреждение высшего образования «Волгоградский государственный университет». Волгоград: ВолГУ, 2018, т. 12, № 3, 52 с.
2. *Бойченко о.*, *Гавриков С.* Системы обнаружения вторжений в комплексе информационной безопасности банков. — Информация и космос № 1 информатика, вычислительная техника и управление, 1990, № 5, с. 25–31.
3. *Попов Г. А.*, *Симаворян С. Ж.*, *Симонян А. Р.*, *Улитина Е. И.* Моделирование процесса мониторинга систем информационной безопасности на основе систем массового обслуживания. — Информатика и ее применения, 2020, т. 14, № 1, с. 71–79.
4. *Ежгуров В. Н.*, *Юмашева Е. С.*, *Бач М. А.* Проблемы внедрения системы обнаружения вторжения и устранения Нацразвитие гуманитарный национальный исследовательский институт (Санкт-Петербург). Материалы конференций ГНИИ "Нацразвитие": сборник избранных статей / Гуманитарный национальный исследовательский институт "Нацразвитие". Санкт-Петербург: Гуманитарный национальный исследовательский институт "Нацразвитие 2016–2018, январь, протокол № 28, 2018, 262 с.
5. *Назаров А. В.*, *Енгалычев А. Н.*, *Мельников В. П.* Эксплуатация объектов сетевой инфраструктуры. Учебник. Москва: ИНФРА-М, 2019, 360 с.

UDC 004.02

Simavoryan S. Zh., Simonyan A. R., Ulitina E. I., Popov G. A. (Sochi, Sochi State University, Astrakhan, Astrakhan State Technical University)**. Methods of emergency counteraction to intrusions in information systems.** *Abstract*: In the process of counteracting both known and previously unknown intrusions (threats), information systems use special neutralization (localization and elimination) procedures related to the class of emergency. The main feature of emergency situations is strict time limits on reaction time and counteraction to attacks. For this reason, the main limitation for all implemented procedures is the time of their implementation. All procedures whose implementation time is longer than permissible are discarded, regardless of how effective and remarkable they are. The most dangerous situations are when invasions leave no trace, intrusion search systems do not respond to a real invasion. Therefore, it is necessary to carry out a systematic analysis of emergency anti-intrusion methods and include new methods to help search for intrusions that the information security system did not respond to in a timely manner.

Keywords: hidden attack, information security, intrusion detection system, system approach.