УДК 681.3

ОБ ИСПОЛЬЗОВАНИИ ИДЕОЛОГИИ ИММУННОГО ПОДХОДА ПРИ РЕАЛИЗАЦИИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

© 2018 Ю. П. Преображенский

Воронежский институт высоких технологий (г. Воронеж, Россия)

В данной статье рассматриваются особенности защиты информации в компьютерных системах. Указана аналогия между иммунной системой живых организмов и средств компьютерной защиты.

Ключевые слова: информационная безопасность, компьютерная система, защита информации.

Современное человечество уже не представляет своё существование без персональных компьютеров или мобильных устройств. Да и грань между двумя этими определениями уже весьма размыта и определяется лишь степенью мобильности. В них хранится информация о частной жизни, деловой активности, личных данных владельца.

Компьютеризированные, интеллектуальные системы также тесно интегрированы в любую сферу бизнеса. И, наравне с данными обычных обывателей, в них хранится информация обо всей деятельности компании. Эти данные являются лакомым кусочком для конкурентов. Чем крупнее бизнес, тем сильнее конкуренты пытаются получить доступ к этим данным. И эти данные нужно защищать.

Внутри корпоративной сети постоянной курсируют данные между рабочими местами пользователей и серверами, системами управления производством и центрами принятия решений, базами данных и СУБД и прочее. Каждое устройство в корпоративной сети генерирует свой рабочий трафик. Также предприятие, при помощи глобальной сети Интернет ведет обмен данными с филиалами и мобильными сотрудниками. Устройства и программы изнутри корпоративной сети запрашивают информацию у компаний, их производящих, информацию об обновлениях. Компания ведет информационный обмен с компаниями-партнерами. Также компания может вести свой бизнес через Интернет и с помощью Интернета.

Информационная система предприятия постоянно подвергается атакам конкурентов, злоумышленников, компьютерных вирусов. Для вывода из строя различных компонентов предприятия могут применяться все возможные способы влияния на интеллектуальные устройства компании.

Сотрудники информационной безопасности предприятия вынуждены просчитывать все пути компрометации информации, чтобы иметь средства защиты от них. А с учетом последних публикаций работников некоторых государственных служб по информационной безопасности, нарушитель конфиденциальности может воспользоваться самыми изощренными путями проникновения в корпоративную информационную систему.

Предусмотреть все возможные пути защиты практически невозможно. Но можно научиться создавать системы безопасности у природы. В частности, иммунная система позвоночных способна справляться практически с любой опасностью, поступающей извне, динамически адаптируясь под постоянно меняющуюся внешнюю среду. И, проводя аналогии между корпоративной системой и живым организмом, можно построить систему безопасности на основе искусственной иммунной системы.

Иммунная система позвоночных представляет собой целый комплекс

защитных механизмов. Причем эти механизмы срабатывают в несколько этапов.

На рисеунке 1 представлен пример иммунной защиты организма.

Как видно из описанного выше, природа в полной мере позаботилась о защите организма самыми различными способами. Проводя аналогию между органами и различными составляющими организации, все эти способы можно переложить на предприятие.

Преображенский Юрий Петрович – Воронежский институт высоких технологий, к. т. н., доцент, профессор ВИВТ, oimk@vivt.ru.

Предприятие сталкивается с различными типами угроз. Например, физические, такие как рейдерский захват, проникновение на территорию с целью хищения имущества или информации, разрушение предприятия из-за природного катаклизма, войны или других трудно прогнозируемых факторов. Так и информационные, такие, как проникновение в компьютерную сеть с целью хищения коммерчески важной информации, разрушения информационной инфраструктуры, заражение компьютерными вирусами, вывод из строя определённых, важных для бизнеса узлов. Разные уровни «иммунитета предприятия» способны защитить от этих угроз или, в случае проникновения «возбудителя» в «организм» предприятия, минимизировать возможные потери и убытки.

Рисунок 1. Иммунная защита организма.

Первичный уровень защиты предприятия, поверхностные барьеры, состоит из зданий предприятия, заборов, ограждающих территории организации. Для контроля прохода сотрудников и других важных для функционирования предприятия элементов (как товаров, так и людей-партнеров), необходимы пропускные режимы. Как и в случае организма, поверхностные барьеры действуют одинаково для всех возможных методов физического проникновения.

Для защиты от информационного воздействия на границе корпоративной сети устанавливаются фаерволы с соответствующими списками доступа. Как и физическая защита, они одинаково блокируют всё внешнее воздействие, за исключением разрешенного. При отсутствии фаерволов, маршрутизаторы могут выполнять часть их функций по фильтрации информационного трафика.

Против физической угрозы организация создает документы, регламентирующие поведение персонала в случае возникновения различных ситуаций. Также поведение персонала может регламентироваться законодательными актами государства, в котором функционирует предприятие, либо личным опытом сотрудников предприятия.

Например, при проникновении на территорию предприятия посторонних лиц, срабатывает сигнализация, заставляя службу безопасности искать нарушителя. Чаще всего сигнализация указывает на участок, в котором произошло нарушение. Сотрудники предприятия отрабатывают, как лимфоциты в организме, идентифицируя нарушителя и применяя к нему адекватные меры воздействия. Также возможна адаптация «организма» предприятия для предотвращения возможности повторного «заражения», например, путем установления решеток на окнах в случае проникновения злоумышленников через окно.

Система информационной защиты организации, подобно иммунной системе, состоит из нескольких уровней. Эти уровни можно условно разделить, подобно уровням иммунной системы организма.

На первичном уровне, «физическом барьере», выступают различные сетевые экраны. Правильно сконфигурированный сетевой экран пускает только полезный трафик внутрь корпоративной сети, отсеивая вредоносный. Эти правила срабатывают для всех данных по принципу «что не разрешено, то запрещено», т. е. работают неспецифично. Сетевые экраны защищают всю сеть в целом, не акцентируя внимания, какие устройства или программы в этой корпоративной сети находятся. Устройства корпоративной сети, будь то персональные компьютеры сотрудников или активное оборудование, могущее взаимодействовать с другими устройствами в пределах сети предприятия или за этими приделами, также не заботятся о том, какие сетевые экраны ограничивают взаимодействие с требуемыми ресурсами. Существование «физического барьера» для них прозрачно и незаметно.

Если деструктивный трафик проникает за пределы «физического барьера», он попадает на устройство, могущее принять этот трафик. Поскольку перемещение потоков трафика информации внутри корпоративной сети подчиняются определённым законам, деструктивный трафик может воздействовать лишь на конкретное устройство, а не на все устройства организации в целом. В частности, сетевой экран часто пропускает трафик к корпоративному веб-серверу. Этот веб-сервер защищен сетевым экраном от всех видов трафика, кроме того, который может обработать. Злоумышленники могут этим воспользоваться и замаскировать деструктивный поток информации под полезный, обрабатываемый этим веб-сервером.

На устройствах внутри корпоративной сети срабатывает второй, «врожденный» уровень защиты. На втором уровне защиты отрабатываются взаимодействия различных сервисов и программ. Операционная система разграничивает доступ этих программ к жесткому диску, файловой системе, компонентам операционной системы. Программа запускается от имени пользователя, который её устанавливает. Для установки программ, могущих влиять на операционную систему в целом, операционная система требует особых привилегий, привилегий администратора, повышая тем самым ответственность пользователя и не позволяя запускаться потенциальным вредоносным программам случайно. Этот метод защиты также не специфичен и отрабатывает для всех попыток влияния на операционную систему.

Программное обеспечение обрабатывает предназначаемый для него информационный трафик. Информация, не соответствующая правилам, характерным для конкретного программного обеспечения, отбрасывается, как несоответствующая. Некоторые виды программ также требуют авторизации, не позволяя обрабатывать не аутентифицированные запросы.

По мере обнаружения уязвимостей в существующем программном обеспечении производители программ выпускают обновления, патчи и заплатки, устраняющие найденные уязвимости.

Для обнаружения и защиты от компьютерных вирусов разработано несколько специальных программ, которые позволяют обнаруживать и уничтожать компьютерные вирусы и, при возможности, устранять последствия заражения. Такие программы называют антивирусными. Эти программы условно можно отнести к третьему, адаптивному, уровню защиты информации. Антивирусные программы используют различные методы обнаружения вирусов. Примеры антивирусных программ отражены на рис. 2.

К основным методам обнаружения компьютерных вирусов можно отнести следующие:

- Метод, когда идет сравнение с эталоном
- Проведение эвристического анализа
- Проведение антивирусного мониторинга
- Использование метода обнаружения изменений
- Применение подхода, связанного с встраиванием антивирусов в BIOS компьютера и др.

Одним из простых методов, связанных с обнаружением – это метод, в котором сравнивают с эталоном, он состоит в том, что при поиске известных вирусов применяют так называемые маски. Маской в вирусе будет определенная постоянная последовательность кода, которая является специфичной по этому конкретному вирусу. Антивирусная программа последовательным образом осуществляет просмотр проверяемых файлов в поиске масок по известным вирусам. Антивирусные сканеры могу найти лишь только известные вирусы, по которым дано определение маски. Использование простых сканеров не дает защиту компьютерам от проникновения новых вирусов.

С тем, чтобы компьютерные вирусы могли размножаться, они должны делать

определенные конкретные действия: проведение копирования в память, делать записи в сектора и т. д. Эвристический анализатор, рассматривается как часть антивирусной программы, имеет список таких действий и ведется проверка программ и загрузочных секторов дисков и дискет в попытках обнаружить в них код, который характерен для вирусов. Эвристический анализатор может обнаружить, что проверяемая программа устанавливает резидентный модуль в памяти или записывает данные в исполняемый файл программы. Эвристический анализатор позволяет обнаруживать неизвестные ранее вирусы.

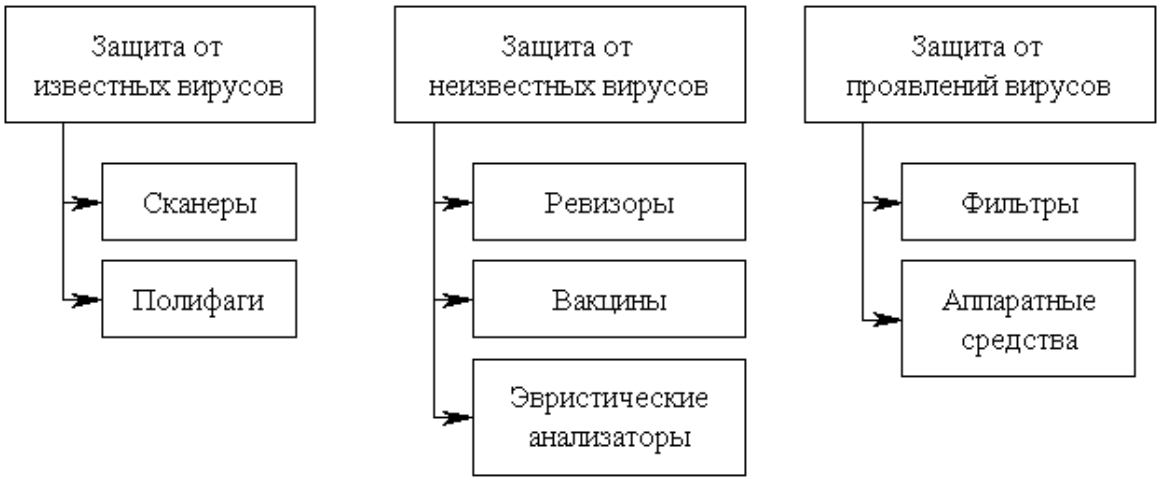

Рисунок 2. Типы антивирусных программ.

С тем, чтобы компьютерные вирусы могли размножаться, они должны делать определенные конкретные действия: проведение копирования в память, делать записи в сектора и т.д. Эвристический анализатор, рассматривается как часть антивирусной программы, имеет список таких действий и ведется проверка программ и загрузочных секторов дисков и дискет, в попытках обнаружить в них код, который характерен для вирусов. Эвристический анализатор может обнаружить, что проверяемая программа устанавливает резидентный модуль в памяти или записывает данные в исполняемый файл программы. Эвристический анализатор позволяет обнаруживать неизвестные ранее вирусы.

Метод антивирусного мониторинга состоит в том, что в памяти компьютера непрерывно есть антивирусная программа, которая осуществляет мониторинг по всем действиям, которые выполняются другими программами. Мониторинг дает возможности для проверки всех запускаемых программ, создаваемым, открываемым и сохраняемым документам, файлам программ и документам, полученным через Интернет или скопированным с внешнего носителя. Антивирусный мониторинг сообщает пользователю, либо администратору, если какая-то программа попытается выполнить потенциально опасное действие.

Когда реализуется метод обнаружения изменений антивирусные программы, которые называются ревизорами диска, проводят запоминание предварительным образом характеристики по всем областям диска, которые могут подвергнуться нападению, а потом периодически делают проверку их. При проведении сопоставления по значениям характеристик областей диска антивирусная программа может провести обнаружение изменений, сделанных как известными, так и неизвестными вирусами.

В системные платы компьютеров идет встраивание простейших средств защиты от вирусов. Такие средства дают возможности для контроля всех обращений к главной загрузочной области жестких дисков, а также к загрузочным секторам дисков и дискет. Но такая защита не является надежной. Известны вирусы, которые пробуют отключать антивирусный контроль BIOS, проводя изменение некоторых ячеек в энергонезависимой памяти компьютера.

Использование комплексных антивирусных программ, применяющих современные методы обнаружения вирусов, при регулярном обновлении антивирусных баз, позволяет защитить компьютерную сеть предприятия от вредоносных программ. Ан-

тивирусные программы постоянно совершенствуют свои средства обнаружения вирусов, по своему функционалу становясь аналогом адаптивной иммунной системы позвоночных.

ЛИТЕРАТУРА

1. Воронов А. А. Обеспечение системы управления рисками при возникновении угроз информационной безопасности / А. А. Воронов, И. Я. Львович, Ю. П. Преображенский, В. А. Воронов // Информация и безопасность. – 2006. – Т. 9. – № 2. – С. 8-11.

2. Гуськова Л. Б. О построении автоматизированного рабочего места менеджера / Л. Б. Гуськова // Успехи современного естествознания. – 2012. – № 6. – С. 106.

3.Зяблов Е. Л. Разработка лингвистических средств интеллектуальной поддержки на основе имитационно-семантического моделирования / Е. Л.Зяблов, Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2009. – № 5. – С. 24-26.

4. Львович И. Я. Факторы угрозы экономической безопасности государства / И. Я. Львович, А. А.Воронов, Ю. П. Преображенский // Информация и безопасность. – 2006. – Т. 9. – № 1. – С. 36-39.

5. Максимов И. Б. Классификация автоматизированных рабочих мест / И. Б. Максимов // Вестник Воронежского института высоких технологий. – 2014. – № 12. – С. 127-129.

6. Максимов И. Б. Принципы формирования автоматизированных рабочих мест / И. Б. Максимов // Вестник Воронежского института высоких технологий. – 2014. – № 12. – С. 130-135.

7. Пеньков П. В. Экспертные методы улучшения систем управления / П. В. Пеньков // Вестник Воронежского института высоких технологий. – 2012. – № 9. – С. 108-110.

8. Преображенский Ю. П. Оценка эффективности применения системы интеллектуальной поддержки принятия решений / Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2009. – № 5. – С. 116-119.

9. Самойлова У. А. О некоторых характеристиках управления предприятием / У. А. Самойлова // Вестник Воронежского института высоких технологий. – 2014. – № 12. – С. 176-179.

10. Фомина Ю. А. Принципы индексации информации в поисковых системах / Ю. А. Фомина, Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2010. – № 7. – С. 98-100.

THE USE OF IDEOLOGY IMMUNE APPROACH IN THE IMPLEMENTATION OF SYSTEMS OF INFORMATION PROTECTION IN COMPUTER SYSTEMS

© 2018 Yu. P. Preobrazhensky

Voronezh Institute of High Technologies (Voronezh, Russia)

In this paper the peculiarities of information security in computer systems are considered. The analogy between immune system of living organisms and means of computer protection is specified.

Keywords: information security, computer system, information security.