УДК 681.323

А.А.ЗАМУЛА, канд. техн. наук, С.А.СИРОТА, Н.И.КОСИКОВСКАЯ

КОЛИЧЕСТВЕННАЯ ОЦЕНКА УЯЗВИМОСТЕЙ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

В организациях часто не учитывается тот факт, что администраторы и пользователи регулярно изменяют конфигурацию информационных систем (ИС). В результате этих изменений могут появляться новые уязвимости, связанные с операционными системами (ОС) и приложениями. Кроме того, очень быстро изменяются информационные и сетевые технологиb, регулярно появляется новое ПО. Непрерывное развитие сетевых технологий при отсутствии постоянного анализа их безопасности и нехватке ресурсов для обеспечения защиты приводит к тому, что со временем защищенность ИС падает, так как появляются новые неучтенные угрозы и уязвимости системы.

В большинстве случаев для решения возникших проблем с защитой информации в организациях используются технические подходы. Администраторы безопасности имеют тенденции реагировать только на те риски информационной безопасности, которые им понятны. Фактически рисков может быть существенно больше. Только строгий постоянный контроль защищенности ИС и комплексный поход, обеспечивающий единую политику безопасности, позволяют существенно снизить риски безопасности.

Атакой на ИС является любое действие, выполняемое нарушителем для реализации угрозы путем использования уязвимостей ИС. Под уязвимостью ИС понимается любая характеристика или элемент ИС, использование которых нарушителем может привести к реализации угрозы.

Эффективное применение информационных технологий – общепризнанный стратегический фактор роста конкурентоспособности компании. Многие предприятия переходят к использованию широких возможностей Интернета и электронного бизнеса, неотъемлемым элементом которого являются электронные транзакции.

Цель статьи – оценка уязвимостей информационно-телекоммуникационных систем и классификация систем обнаружения атак на информационные системы.

Системы анализа защищенности

Для любой компании (финансовой, страховой, торговой и т.п.) существует типовая информационная система, состоящая из компонент, решающих специфичные задачи, но в общем случае ИС включает в себя четыре уровня функционирования:

1. Уровень прикладного программного обеспечения, отвечающий за взаимодействие с пользователем. Примерами элементов ИС, работающих на этом уровне, являются редактор WinWord, редактор электронных таблиц Excel, почтовая программа Outlook, системы MS Query и т.д.

2. Уровень системы управления базами данных (СУБД), отвечающий за хранение и обработку данных информационной системы. Примерами элементов ИС, работающих на этом уровне, являются СУБД Oracle, MS SQL Server, Sybase и даже MS Access.

3. Уровень операционной системы (ОС), отвечающий за обслуживание СУБД и прикладного программного обеспечения. Примерами элементов ИС, работающих на этом уровне, являются ОС MicrosoftWindowsNT, SunSolaris, NovellNetware и другие.

4. Уровень сети, отвечающий за взаимодействие узлов информационной системы. Примерами элементов ИС, работающих на этом уровне, являются стеки протоколов TCP/IP, IPS/SPX и SMB/NetBIOS.

Злоумышленники обладают широким спектром возможностей по нарушению политики безопасности. Воздействия злоумышленника могут быть осуществлены на указанных уровнях функционирования ИС.

С целью повышения уровня защищенности ИС от различных атак необходимо наряду с “традиционными” средствами защиты (например, межсетевые экраны) использовать

“адаптивные” средства: система анализа защищенности, системы обнаружения атак и другие.

Системы анализа защищенности проводят всесторонние исследования систем для обнаружения уязвимостей, которые могут привести к нарушениям политики безопасности. Результаты, полученные от средств анализа защищенности, представляют "мгновенный снимок" состояния защиты системы в данный момент времени. Несмотря на то, что эти системы не могут обнаруживать атаку в процессе ее развития, они могут определить возможность реализации атак.

При решении практических задач защиты информации первостепенное значение имеет количественная оценка ее уязвимости. Поскольку воздействие на систему различных факторов в значительной мере является случайным, то в качестве количественной меры уязвимости системы наиболее целесообразно принять вероятность нарушения защищенности, а также потенциально возможный размер ущерба, наносимого таким воздействием. При этом основными параметрами, влияющими на вероятность нарушения защищенности информации, являются: количество и типы структурных компонентов системы или объекта, количество и типы случайных угроз, количество и типы преднамеренных угроз, число и категории лиц, которые потенциально могут быть нарушителями установленных правил обработки информации, и, наконец, виды защищаемой информации.

Оценки уязвимостей ИС

Известно, что несанкционированное получение информации возможно не только путем непосредственного доступа к базам данных, но и многими другими путями, не требующими такого доступа. При этом основную опасность представляют преднамеренные действия злоумышленников. Воздействие случайных факторов само по себе не ведет к несанкционированному получению информации, оно лишь способствует появлению каналов несанкционированного получения информации (КНПИ), которыми может воспользоваться злоумышленник.

Для несанкционированного получения информации необходимо одновременное наступление следующих событий:

-- нарушитель должен получить доступ в соответствующую зону;

-- во время нахождения нарушителя в зоне в ней должен проявиться соответствующий КНПИ;

-- КНПИ должен быть доступен нарушителю соответствующей категории;

-- в момент доступа нарушителя к КНПИв данном канале должна находиться защищаемая информация.

Безусловно, важным является получение количественной оценки уязвимости информации. В качестве такой оценки может быть использована вероятность несанкционированного получения информации (P_{ijkl})нарушителем *k*-й категории по *j*-му КНПИ в *l*--*й* зоне информационных ресурсов *i*-го структурного компонента системы:

$$P_{ijkl} = P_{ijl}^{(d)} P_{ijl}^{(k)} P_{ijkl}^{(h)} P_{ijl}^{(u)}, \qquad (1)$$

где $P_{ikl}^{(d)}$ – вероятность доступа нарушителя *k*-й категории в *l*-ю зону информационных ресурсов *i*-го компонента компьютерной системы;

$P_{ijl}^{(u)} \mathbf{P_{ijl}^{(k)}}$ – вероятность наличия *j*-го КНПИ в *l*-й зоне информационных ресурсов *i*-го компонента компьютерной системы;

$P_{ijkl}^{(h)}$ – вероятность доступа нарушителя *k*-й категории к *j*-му КНПИ в *l*-й зоне информационных ресурсов *i*-го компонента при условии доступа нарушителя к базе данных;

$P_{ijl}^{(u)}$ – вероятность наличия защищаемой информации в *j*-м КНПИ в *l*-й зоне информационных ресурсов *i*-го компонента в момент доступа туда нарушителя.

Вероятность несанкционированного получения информации в одном компоненте компьютерной системы одним злоумышленником одной категории по одному КНПИ. Назовем базовым показателем уязвимости информации [2]. С учетом (1) выражение для базового показателя будет иметь вид

$$P_{ijk}^{б} = 1 - \prod_{l=1}^{5}\left(1 - P_{ijkl}\right) = 1 - \prod_{l=1}^{5}\left[1 - P_{ijl}^{(d)} P_{ijl}^{(k)} P_{ijkl}^{(h)} P_{ijl}^{(u)}\right). \quad (2)$$

Рассчитанные таким образом базовые показатели уязвимости сами по себе имеют ограниченное практическое значение. Для решения задач, связанных с разработкой и эксплуатацией систем защиты информации, необходимы значения показателей уязвимости, обобщенные по какому-либо одному индексу (*i, j, k)* или по их комбинации. Рассмотрим возможные подходы к определению таких частично обобщенных показателей.

Пусть {К} – интересующее нас подмножество из полного множества потенциально возможных нарушителей. Тогда вероятность нарушения защищенности информации указанным подмножеством нарушителей по *n*-му фактору в *i*-м компоненте системы ($P_{ij\{K*\}}$) может быть определена следующим образом:

$$P_{ij\{K*\}} = 1 - \prod_{K*}\left[1 - P_{ijk}^{б}\right], \quad (3)$$

где $\prod_{K*}$означает перемножение выражений в скобках для всех нарушителей, входящих в подмножество {*K**}.

Аналогично, если {*J**} есть подмножество представляющих интерес КНПИ, то уязвимость информации в *i-м* компоненте по данному подмножеству факторов относительно *k*-го нарушителя может быть определена следующим образом:

$$P_{i\{J*\}k} = 1 - \prod_{J*}\left[1 - P_{ijk}^{б}\right]. \quad (4)$$

Если же {*I**} есть подмножество интересующих нас структурных компонентов системы, то уязвимость информации в них по *j*-му КНПИ относительно *k-го* нарушителя:

$$P_{\{I\}jk} = 1 - \prod_{I*}\left[1 - P_{ijk}^{б}\right]. \quad (5)$$

Каждое из приведенных выше выражений позволяет производить обобщение по одному из множества параметров. Нетрудно получить и общее выражение, если нас интересуют подмножества {*I*}, {*J*} и {*K*} одновременно. В этом случае:

$$P_{\{I\}\{J\}\{K\}} = 1 - \prod_{I*}\left[1 - P_{ijk}^{б}\right]\prod_{K*}\left[1 - P_{ijk}^{б}\right]\prod_{K*}\left[1 - P_{ijk}^{б}\right]. \quad (6)$$

Очевидно, общий показатель уязвимости P при таком подходе:

$$P = 1 - \prod_{I*}\left[1 - P_{ijk}^{б}\right]\prod_{K*}\left[1 - P_{ijk}^{б}\right]\prod_{K*}\left[1 - P_{ijk}^{б}\right]. \quad (7)$$

На практике наибольший интерес представляют экстремальные показатели уязвимости, характеризующие наиболее неблагополучные условия защищенности информации: самый уязвимый структурный компонент системы (*I**), самый опасный КНПИ (*J**), самая опасная категория нарушителей (*K**).

Аналогичным образом может быть проведена оценка уязвимости информации и в других случаях, в частности в случаях нарушения целостности.

Для расчета показателей уязвимости информации с учетом интервала времени, на котором оценивается уязвимость, следует учитывать, что чем больше интервал времени, тем больше возможностей у нарушителей для злоумышленных действий и тем больше вероятность изменения состояния системы и условий обработки информации.

Можно определить такие временные интервалы (не сводимые к точке), на которых процессы, связанные с нарушением защищенности информации, являлись бы однородными. Назовем такой интервал малым. Такой малый интервал, в свою очередь, может быть разделен на очень малые интервалы, уязвимость информации на каждом из которых определяется независимо от других. При этом, в силу однородности происходящих процессов, уязвимость информации на каждом из выделенных очень малых интервалов будет определяться по одной и той же зависимости.

Тогда, если P_t^m – показатель уязвимости на фиксированном интервале, а $P^{\text{м}}$-показатель уязвимости на малом интервале, то:

$$P^{\text{м}} = 1 - \prod_{t=1}^{n} [1 - P_t^m], \tag{8}$$

где t – интервал деления выбранного объекта СУБД интервалов наотдельные сегменты; n – общее число очень малых интервалов.

Рассмотренный подход можно распространить и на другие интервалы, а именно: большой интервал представить некоторой последовательностью малых, очень большой – последовательностью больших, бесконечно большой – последовательностью очень больших интервалов [2].

Системы обнаружение атак

Системы обнаружения атак реализуются посредством анализа журналов регистрации операционной системы и прикладного ПО, сетевого трафика в реальном времени. Компоненты обнаружения атак, размещенные на узлах или сегментах сети, оценивают различные действия, в том числе, использующие известные уязвимости [3].

Рассмотрим этапы осуществления атаки. Первый, подготовительный этап, заключается в поиске злоумышленником предпосылок для осуществления той или иной атаки. На этом этапе злоумышленник ищет уязвимости в системе.

На втором, основном этапе реализации атаки, – осуществляется использование найденных уязвимостей. На третьем, заключительном этапе, злоумышленник завершает атаку и старается скрыть следы вторжения [1].

Существующие механизмы защиты, реализованные в межсетевых экранах (firewall), серверах аутентификации, системах разграничения доступа и т.д., работают только на втором этапе. Т.е. по существу они являются средствами блокирующими, а не упреждающими атаки. Комплексная система обеспечения информационной безопасности должна работать на всех трех этапах осуществления атаки. И обеспечение адекватной защиты на третьем, завершающем, этапе не менее важно, чем на первых двух. Ведь только в этом случае можно реально оценить ущерб от "успешной" атаки, а также разработать меры по устранению дальнейших попыток реализовать аналогичную атаку.

Обнаруживать, блокировать и предотвращать атаки можно несколькими путями. Первый, самый распространенный, способ – обнаружение уже реализуемых атак. Этот способ применяется в "классических" системах обнаружения атак (например, RealSecure компании Internet Security Systems), межсетевых экранах и т.п. Однако "недостаток" средств данного класса в том, что атаки могут быть реализованы повторно. Они также повторно обнаруживаются и блокируются. Второй путь – предотвратить атаки еще до их реализации. Осуществляется это поиском уязвимостей, которые могут быть использованы для реализации атаки. И, наконец, третий путь – обнаружение уже совершенных атак и предотвращение их повтор-

ного осуществления. Таким образом, системы обнаружения атак могут быть классифицированы по этапам осуществления атаки (рис. 1):

- системы, функционирующие на первом этапе атак и позволяющие обнаружить уязвимости информационной системы, используемые нарушителем для реализации атаки. Иначе средства этой категории называются системами анализа защищенности (security assessment systems) или сканерами безопасности (security scanners);

- системы, функционирующие на втором этапе атаки и позволяющие обнаружить атаки в процессе их реализации, т.е. в режиме реального (или близкого к реальному) времени. Именно эти средства и принято считать системами обнаружения атак в классическом понимании. Помимо этого в последнее время выделяется новый класс средств обнаружения атак – обманные системы;

- системы, функционирующие на третьем этапе атаки и позволяющие обнаружить уже совершенные атаки. Эти системы делятся на два класса – системы контроля целостности, обнаруживающие изменения контролируемых ресурсов, и системы анализа журналов регистрации.

Рис.1

Помимо этого, существует еще одна распространенная классификация систем обнаружения нарушения политики безопасности – по принципу реализации: host-based, т.е. обнаруживающие атаки, направленные на конкретный узел сети, и network-based, направленные на всю сеть или сегмент сети. Обычно на этом дальнейшая классификация останавливается. Однако системы класса host-based можно разделить еще на три подуровня:

- Application IDS, обнаруживающие атаки на конкретные приложения;
- OS IDS, обнаруживающие атаки на операционные системы;
- DBMS IDS, обнаруживающие атаки на системы управления базами данных.

Выделение обнаружения атак на системы управления базами данных (СУБД) в отдельную категорию связано с тем, что современные СУБД уже вышли из разряда обычных приложений и по многим своим характеристикам, в т.ч. и по сложности, приближаются к операционным системам. Таким образом, классификация систем обнаружения атак по уровню реализации выглядит следующим образом (рис. 2). Можно заметить, что это деление соответствует уровням информационной системы предприятия .

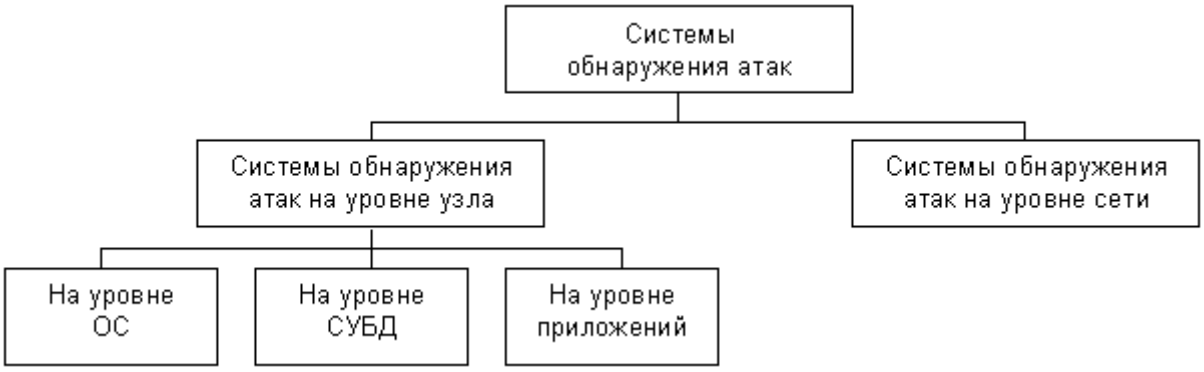

Рис. 2

Выводы

1. Таким образом, применение “традиционных” средств безопасности не позволяет реализовать эффективную защиту от способов воздействия на информационные ресурсы компании. Только комплексное применение "традиционных" и "адаптивных" механизмов позволит гарантировать высокий уровень защищенности информационной системы предприятия от внешних и внутренних злоумышленников.

2. Для того чтобы привести систему обеспечения информационной безопасности организации в соответствие современным требованиям, необходимо дополнить имеющееся решения компонентами, реализующими анализ защищенности ИС и обнаружение атак на ИС.

Список литературы: *1. Малюк, А.А.* Информационная безопасность. – М. : Горячая линия Телеком, 2004. – 280с. 2. *Шаньгин, В.Ф.* Информационная безопасность компьютерных систем и сетей. – М. : ИД «ФОРУМ», 2008. – 415с. 3. *Лукаций, А.В.*Обнаружение атак. – СПб. : БХВ-Петербург, 2004. – 624с. 4. *Лукаций, А.В.* Безопасность беспроводных сетей // Технологии и средства святи. – 2005. – №1 5. *Зима, В.М.* Компьютерные сети и защита передаваемой информации. – СПб. : Изд. СПбГУ, 2003. – 569с. 6. *Костров, Д.* Системы обнаружения атак // BYTE Россия. – 2002. – №8

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 13.09.2012