Операция Create задает отображение декартова произведения множеств субъектов и объектов на объединение множества субъектов с пустым множеством. На физическом уровне операция Create означает, что субъект Sj, обладая управлением и ресурсами, может передать Sk часть ресурсов и управление (активизация). Заметим также, что в КС действует дискретное время и фактически новый субъект Sk порождается в момент времени t+1 относительно момента t, в который произошло воздействие порождающего субъекта на объект-источник.

Очевидно, что операция порождения субъектов зависит как от свойств активизирующего субъекта, так и от содержания объекта-источника.

Считаем, что если Create(Sj,Oi) $\rightarrow$NULL (конструкция NULL далее обозначает пустое множество), то порождение нового субъекта из объекта Oi при активизирующем воздействии Sj невозможно.

Свойство АЗ быть активной реализуется не только в выполнении действий над объектом с целью создания нового субъекта, но и с целью чтения или записи данных в объект. В общем случае необходимо отметить, что поскольку объекты КС по определению являются пассивными, то для выполнения аппаратной закладкой всех описанных выше действий, необходимо существование потоков информации от субъекта к объекту (в противном случае невозможно говорить об изменении объектов). Так как данный поток инициируется и реализуется субъектом – АЗ, это означает, что операция порождения потока локализована в субъекте – АЗ и отображается состоянием его функционально ассоциированных с ней объектов.

Поток информации между объектом Om и объектом Oj всегда должен быть связан с некоторой операцией над объектом Oj, реализуемой субъектом Sj и зависящей от Om. Поток информации от объекта Om к объекту Oj обозначим как Stream(Si, Om) $\rightarrow$Oj. При этом будем выделять источник (Om) и получатель (приемник) потока (Oj). Из данного определения также следует, что поток всегда инициируется (порождается) субъектом.

Очевидно, что с помощью приведенного определения операции Stream над объектами Om и Oj формализуется операции доступа субъекта S к объекту Oj для записи в него данных из Om или наоборот. Отметим, что в частном случае операция Stream может создавать новый объект или уничтожать его. Операции порождения субъектом потока, а также порождения субъектов назовем операциями доступа.

Понятие доступа является одним из основополагающих в теории защиты информации, поскольку разрешение или запрет доступа для заданных множеств субъектов и объектов в конечном итоге определяет безопасность КС.

Выводы

В работе предложена субъектно-объектная модель аппаратных ресурсов КС, охватывающая такой класс угроз, как аппаратные закладки (АЗ), а также определена операция доступа для АЗ. Полученные результаты могут быть использованы для разработки модели безопасности КС, включающей средства защиты от угроз, реализуемых АЗ.

Литература: ***1.*** *Девянин П. Н., Михальский О. О., Правиков Д. И., Щербаков А. Ю. и др. Теоретические основы компьютерной информации. – М.: Радио и связь, 2000. –189 с.* ***2.*** *Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000.452., ил.* ***3.*** *Горбачев В. А., Степаненко В. В. Сертификация периферийных устройств компьютерных систем.// Радиотехника: сб. научн. трудов. Выпуск 134.-Харьков: ХНУРЭ, 2003. С. 206 – 209.*

УДК 681.3

СИСТЕМЫ ОБНАРУЖЕНИЯ АТАК ДЛЯ ЗАЩИТЫ ИНТРАНЕТ

Вячеслав Шорошев
НИИ НАВД Украины

Аннотация: **Система обнаружения атак – перспективная технология защиты информационных ресурсов сетей Intranet, которая получает все более широкое распространение в ведущих странах мира и в Украине. Даются рекомендации для Intranet – что, от чего, от кого, как и чем защищать. Также даются практические советы по критериям оценки и выбора систем обнаружения атак и их краткий обзор.**

Summary: **System of detection of attacks - perspective technology of protection of information resources of networks Intranet, which receives more and more wide circulation in the conducting countries of the world and on Ukraine. The recommendations for Intranet - that are given, from what, from whom, as well as than**

to protect. Practical advice(councils) by criteria of an estimation and choice of systems of detection of attacks and their brief review also is given.
Ключевые слова: **Обнаружение атак, атака НСД, адаптивная безопасность, узлы Интранет, политика безопасности, мониторинг, сенсор, сканер.**

I Введение

Вопрос об актуальности и перспективности новой технологии защиты информационных ресурсов сетей Intranet от атак несанкционированного доступа (НСД) ранее уже поднимался [1 – 3]. Новая технология защиты основана на мониторинге, обнаружении и нейтрализации любых атак на информационные ресурсы корпоративных сетей Интранет. Особую опасность среди них представляют атаки НСД. Дело в том, что по таким международным стандартам компьютерной безопасности, как TCSEC (Оранжевая книга, 1983 г.), ITSEC (Европейские критерии, 1991 г.) даже вся компьютерная система оценивалась по степени защиты от атак НСД [4]. Так, классы безопасности С2, FC-2 соответствовали минимальному рейтенгу защиты от НСД, классы В2, FB-2 –относительно стойкой защите от НСД, а классы В3, FB-3 – стойкой защите от НСД.

Правомерно говорить о перспекивном «методе» защиты, когда мы используем такое явление, как «обнаружение» атак. Но можно говорить о «технологии» или «средствах» защиты, когда мы используем конкретные «системы обнаружения» атак. Термин «метод» является более общим понятием, «технология» / «средство» уже предполагает применение в данном «методе» защиты («обнаружении» атак) уже конкретной «системы» обнаружения атак. Это, так сказать, о терминологической корректности понятий «метода» и «технологии» / «средства» защиты. Однако и в первом, и во втором случае обеспечивается, прежде всего, полная реализация требований так называемой политики «адаптивной безопасности» обязательно под множество потенциально возможных и самых различных по своей природе атак извне на информационные ресурсы Интранет. Реализация политики «адаптивной безопасности» достигается путем создания и использования соответсвующей системы обнаружения нарушений выбранной политики безопасности или более информативно и кратко – специальной системы обнаружения атак (System of detection of attacks или SDA-системы). Но первоначально для приобретения или создания такой SDA-системы необходимо выполнить три обязательных условия.

Первое, что необходимо сделать еще до начала приобретения или создания SDA-системы, – это понять, где она в вашей корпоративной локальной сети, которая имеет постоянное или временное соединение с Интернет, будет установлена и какие задачи она будет решать. Без ответа на эти вопросы применение даже самой эффективной SDA-системы будет просто бесполезным. Выяснив решаемые задачи, вы тем самым сможете понять, какой технологии отдать предпочтение, например, или обнаружению атак на уровне сети Интранет, или на уровне операционной системы (ОС), или системы управления базой данных (СУБД), или приложений. Возможно, что на разных участках вашей корпоративной сети Интранет вы найдете применение всем этим технологиям защиты.

Второе, что необходимо сделать, прежде чем покупать или создавать SDA-систему, – точно и предметно понимать – что, от кого, от чего, как и чем вы хотите защитить свою сеть Интранет.

И третье, независимо от выбранной SDA-системы, нужно рассмотреть следующие аспекты, многие из которых уже должны быть описаны в карте вашей сети Интранет:

- защищаемые ресурсы;
- наиболее вероятные атаки;
- объекты (протоколы, адреса, порты, файлы и т. д.), доступные извне для защищаемого ресурса;
- субъекты (пользователи, приложения и т. п.), использующие этот ресурс;
- показатели доступности и производительности для защищаемого ресурса;
- кто и как будет управлять SDA-системой;
- масштабы потенциального роста защищаемого ресурса и, как следствие, масштабы расширения возможностей SDA-системы.

Только выполнение вышеперечисленных трех обязательных условий позволит правильно и быстро установить, настроить и эксплуатировать приобретенную или созданную SDA-систему. Теперь предметно рассмотрим основные практические рекомендации для Интранет – что, от кого, от чего, как и чем нужно защищать. Ответы на эти вопросы предопределяют ваш успех в выборе и реализации стратегии защиты ресурсов своей сети Интранет. Вы последовательно придете к самому трудному и главному решению при ответе на последний вопрос (чем защищать) – выбирать нужно, по большому счету, новую и перспективную SDA-систему, но обязательно дополняемую уже существующими традиционными методами, технологиями и средствами защиты.

II Основная часть

Что защищать в Интранет. Прежде чем приобретать/создавать дорогостоящие технологии /средства обнаружения атак, необходимо осознать, какие ресурсы вашей сети Интранет подлежат защите. Возможно, после такого анализа вы поймете, что не стоит тратить средства на покупку/создание понравившейся вам SDA-системы, а достаточно обойтись организационными мерами или встроенными защитными механизмами. В каждой организации имеются свои ресурсы, требующие защиты. Можно выделить общие категории таких ресурсов для Интранет:

- файловые серверы;
- серверы баз данных;
- телекоммуникационные серверы;
- маршрутизаторы;
- межсетевые экраны и иные средства периметровой защиты, извне-защиты;
- Web-, FTP- и почтовые серверы;
- рабочие станции, обрабатывающие критическую и важную информацию (например, транспортные машины в банках).

Даже простое перечисление критичных для организации ресурсов поможет понять, какие технологии обнаружения атак выбрать для их защиты. Например, для файловых серверов на первое место выходят средства контроля целостности, позволяющие отслеживать несанкционированные изменения файлов. Для маршрутизаторов приоритетными будут системы обнаружения атак на уровне сети и т. д. В табл. 1 перечислены категории важных ресурсов и наиболее часто применяемые для их защиты технологии обнаружения атак в SDA-системах.

Таблица 1 – Первоочередные технологии обнаружения атак в SDA-системах для различных типов узлов корпоративной сети Интранет

Ресурсы защиты	Технологии обнаружения атак
Файловые серверы	Системы контроля целостности Системы обнаружения атак на уровне ОС
Серверы баз данных	Системы обнаружения атак на уровне СУБД Системы обнаружения атак на уровне ОС Системы анализа защищенности на уровне СУБД
Телекоммуникационные серверы	Системы обнаружения атак на уровне сети Системы обнаружения атак на уровне ОС Системы анализа защищенности на уровне сети
Маршрутизаторы	Системы обнаружения атак на уровне сети
Межсетевые экраны, иные средства периметровой защиты, извне защиты й защиты	Системы обнаружения атак на уровне сети Системы обнаружения атак на уровне ОС Системы анализа защищенности на уровне сети Системы анализа защищенности на уровне ОС
Web-, FTP- и почтовые серверы Рабочие станции	Системы обнаружения атак на уровне приложений Системы обнаружения атак на уровне сети Системы обнаружения атак на уровне ОС Системы контроля целостности Системы анализа защищенности на уровне сети Системы анализа защищенности на уровне ОС Системы обнаружения атак на уровне ОС

От чего защищать Интранет. Прежде всего, как уже говорилось в начале статьи, надо защищать от атак НСД и злоупотреблений персонала. Однако имеется большое количество различных типов несанкционированных действий. Систем, защищающих от всех атак НСД, не существует. Поэтому, прежде всего, необходимо проанализировать наиболее вероятные атаки для ваших информационных ресурсов Интранет. Например, вы хотите поставить под охрану сервер приложений, работающий на платформе Windows 2000. При этом распознавание сетевых вторжений вы возлагаете на систему обнаружения атак на уровне сети, установленную в том же сегменте. Это сразу сужает круг вероятных атак на ваш Windows-сервер. То есть, сразу можно сказать, что вам надо выбрать систему обнаружения атак на уровне узла, которая анализирует журналы регистрации или деятельность пользователей. При этом система должна поддерживать именно ОС Windows 2000, а не какую-то другую. Таким образом, проведя пятиминутную

предварительную оценку, вы тем самым существенно сузили круг возможных средств до двух-трех, облегчив себе правильный выбор и сэкономив деньги на приобретение / создание SDA-системы, способной выполнять функции или поддерживать ОС, которые никогда бы не использовались в вашей организации.

От кого защищать Интранет. Задайте этот вопрос обычному человеку, и в абсолютном большинстве случаев вы получите ответ: «От хакеров». Конечно, не вдаваясь в терминологию, можно сказать, что по мнению большинства специалистов основная опасность исходит именно от внешних злоумышленников, которые проникают в компьютерные системы банков и военных организаций, перехватывают управление спутниками и т. д. Весь этот ажиотаж вызван средствами массовой информации, которые за последнее время выдали немало публикаций о хакерах и их опасности.

Стоит только вспомнить репортажи различных телекомпаний о хакерах, которые вторгались в американские банки и переводили миллионы долларов на подставные счета, или публикации о российских «профессионалах-одиночках», которые проникали в компьютерные сети Пентагона, крали важнейшую информацию с грифом «TOP EC RET" и оставляли после себя надписи: «Здесь был Вася!»

Конечно, реально такая опасность для Интранет существует и нельзя ее недооценивать. Но она слишком уж преувеличена. И все же больше половины всех компьютерных преступлений связаны с внутренними нарушениями, т. е. осуществляются персоналом Интранет. Нынешними или уволенными. Представьте, что вам удалось найти лазейку в системе информационной безопасности какой-либо организации. Через эту «дыру» вы проникаете в корпоративную сеть, а затем, в святая святых – к финансовым данным или перспективным разработкам. И что? Не являясь специалистом в области, в которой работает компания, разобраться без посторонней помощи в мегабайтах и гигабайтах информации попросту невозможно. Злоумышленник, использующий уязвимости в системе защиты, будет находиться в растерянности, не зная, что из открытой перед ним информации представляет ценность, а что – является бесполезным хламом. Можно провести интересную аналогию. Допустим, что вы, зная только русский язык, попали в трущобы Пекина, где все указатели написаны на китайском языке, а вам надо в аэропорт. Возможно, вы туда и попадете, но только после долгих блужданий и объяснений с местными жителями на пальцах. Свой сотрудник – совсем другое дело. Он знает, что к чему. Он может реально оценить стоимость той или иной информации. И зачастую он обладает привилегиями, которые не являются необходимыми для него.

"Зачем моему сотруднику обкрадывать меня?" – спросите вы. Причин может быть множество. Однако к самым распространенным можно отнести неудовлетворенность своим положением или зарплатой, затаенную обиду и т. д. Можно привести массу случаев, когда сотрудник, считая, что его на работе не ценят, совершал компьютерное преступление, приводящее к многомиллионным убыткам. В широко известном примере с проникновением в американский Ситибанк также не обошлось без помощи «своего». Однако в публикациях это обычно умалчивается или считается неважным. Другой пример – сотрудник при увольнении затаил обиду на весь свет и хочет отомстить обидчикам, т. е. компании или ее руководству. Если в своей работе он имел достаточно широкие права, то, используя их, он может очень существенно навредить и после ухода. Ведь обычно увольнение сотрудника сопровождается изъятием у него пропуска и только. Во всех системах запись о нем, как правило, остается, и он по-прежнему может использовать вычислительные ресурсы Интранет компании в своих целях. В «лучшем» варианте особого вреда он не нанесет. Например, известен случай, когда после увольнения бывший сотрудник отдела автоматизации одной компании еще в течение года пользовался доступом в Internet, зарегистрированным на данную компанию. При увольнении этого специалиста никто не удосужился сменить пароли, к которым он имел доступ в рамках своих служебных обязанностей. На самом деле, никто так и не заметил, что бывший сотрудник пользуется доступом в Internet, и он мог и дальше наносить ущерб (хоть и небольшой) своей бывшей компании. Однако эта компания развалилась и больше не смогла оплачивать приходящие к ней счета за услуги Internet. Этот случай достаточно показательный, т. к. иллюстрирует очень распространенную в украинских организациях практику увольнения.

Однако самая большая беда может исходить не от уволенных или обиженных обычных сотрудников, а от тех, кто облечен очень обширными полномочиями и имеет доступ к широкому спектру самой различной информации Интранет. По преимуществу, это специалисты отделов автоматизации, информатизации и телекоммуникации, которые обладают сведениями о паролях ко всем системам, используемым в Интранет организации. Их квалификация, знания и опыт, примененные во вред, могут привести к очень большим проблемам. Кроме того, таких нарушителей очень трудно обнаружить, поскольку они имеют достаточные знания о системе защиты Интранет организации, чтобы обойти используемые защитные механизмы. Именно поэтому при покупке/создании SDA-системы необходимо защищаться не только и не столько от внешних злоумышленников, сколько от злоумышленников в

Интранет внутренних. Так например, даже такие «классические» системы защиты, как межсетевые экраны или серверы аутентификации, ориентированы именно на внутренние атаки НСД [1].

Ответ на вопрос «от кого?» позволит вам установить соответствующие приоритеты в обнаружении внешних и внутренних атак НСД. Кстати, ответ на вопрос о решаемых задачах, который был рассмотрен в начале статьи, также поможет вам определить направление приложения своих финансовых ресурсов и сил. Например, если ваша организация/компания преимущественно занимается электронной коммерцией (например, Internet-магазин), то вы должны сконцентрироваться на внешних атаках НСД и т. д.

Как защищать Интранет. На этот вопрос ответить не так легко. С одной стороны, можно поступить довольно просто – купить рекламируемые SDA-системы, установить в своей сети Интранет и потом презентоваться перед коллегами, что вот у меня есть современнейшая система обнаружения атак НСД, которая также используется, например, в Министерстве обороны США. Если компания богата, то она может позволить себе этот путь. Однако необходимо правильно расходовать имеющиеся в распоряжении средства. Во всем мире сейчас принято развертывать комплексную систему защиты, следуя нескольким этапам. Первый, — информационное обследование – самый важный. Именно здесь определяется, от чего в первую очередь следует защищаться компании. На этом же этапе строится так называемая модель нарушителя, которая описывает вероятный образ злоумышленника, т. е. его квалификацию, имеющиеся средства для реализации тех или иных атак, обычное время действия и т. п. И здесь же вы получаете ответ на два вопроса – зачем и от кого надо защищаться? На этом же этапе выявляются и анализируются возможные методы и технологии защиты от угроз безопасности / атак НСД, оценивается вероятность и ущерб от их реализации в своей сети Интранет. По результатам анализа вырабатываются рекомендации по устранению выявленных угроз, правильному выбору и применению средств защиты. Пока вы не перешли к следующему этапу может быть рекомендовано не приобретать достаточно дорогие SDA-системы, а ограничиться уже имеющимися в распоряжении. Например, в случае наличия в Интранет фильтрующего маршрутизатора проще задействовать встроенные в него защитные функции, а не приобретать межсетевой экран.

На первом подготовительном этапе наряду с анализом существующей комплексной системы защиты информации (КСЗИ) в своей сети Интранет (незащищенные сети Интранет организаций в настоящее время уже не используются) должна осуществляться разработка организационно-распорядительных документов персоналу Интранет (инструкций, положений, наставлений и т. п.). Они дают необходимую правовую базу службам безопасности и отделам защиты информации Интранет организации для проведения всего комплекса защитных мероприятий, взаимодействия с внешними организациями, привлечения к ответственности нарушителей безопасности и т. п. Результатом этого этапа является разработанная и утвержденная руководством организации политика безопасности, адаптированная под потенциальные угрозы безопасности, в т. ч. касающаяся вопросов обнаружения атак НСД и антивирусной защиты.

Следующим шагом построения комплексной системы защиты информации Интранет является приобретение, установка и настройка рекомендованных на предыдущем этапе традиционных средств/механизмов обеспечения информационной безопасности. К таким средствам можно отнести системы технической защиты информации от несанкционированного доступа, системы криптографической защиты, системы защиты от ПЕМИН, межсетевые экраны, пакеты фильтрующих программ, фильтрующие маршрутизаторы и др. Традиционные средства являются обязательным дополнением к предлагаемым новым и перспективным SDA-системам, поскольку даже они не являются абсолютно надежными и универсальными системами защиты.

Для правильного и эффективного применения установленных средств защиты необходим квалифицированный персонал. Как уже упоминалось ранее, пока таких специалистов мало. Выходом из сложившейся ситуации могут быть курсы повышения квалификации, на которых сотрудники отделов защиты информации и служб безопасности получат все необходимые практические знания для использования имеющихся средств защиты, выявления угроз безопасности и их предотвращения. Кстати, ответ на вопрос «кто будет эксплуатировать систему обнаружения атак?» также сужает число возможных альтернатив. Если у вас нет возможности выделить отдельного оператора для слежения за сигналами тревоги, появляющимися в реальном режиме времени, то и выбирать вам нужно систему, которая позволяет проводить автономный анализ.

Однако на этом процесс обеспечения безопасности не заканчивается. С течением времени имеющиеся оборудование и программное обеспечение устаревают, выходят новые версии систем обеспечения информационной безопасности, постоянно расширяется список найденных уязвимостей и атак, меняется технология обработки информации, совершенствуются программные и аппаратные средства, приходит и уходит персонал компании. И необходимо периодически пересматривать разработанные организационно-распорядительные документы, проводить обследование ИС или ее подсистем, обучать новый персонал,

обновлять средства защиты. Следование описанной выше последовательности построения комплексной системы обеспечения защиты информации поможет достичь необходимого и достаточного уровня защищенности вашей автоматизированной системы.

Чем защищать Интранет. Ответы на первые четыре вопроса (что, от чего, от кого и как защищать) позволят сузить круг выбираемых SDA-систем до 2 – 3, что качественно облегчит их выбор и ускорит процесс тестирования. В табл. 1 перечислены технологии, которые могут использоваться для защиты важных ресурсов корпоративной сети Интранет. При этом вы можете выбрать любую из технологий. Однако далеко не всегда самый очевидный выбор является самым правильным. Например, вы хотите защитить файловый сервер. Решение как-будто очевидное – это применение систем контроля целостности. Однако представим себе, что на файловом сервере происходят ежесекундные изменения хранимых файлов. Каждое такое событие приводит к проверке его санкционированности со стороны системы контроля целостности. Разумеется, это не может не сказаться на производительности файлового сервера. Вероятна даже ситуация, когда файловый сервер будет настолько занят решением вопроса целостности своих файлов, что захватит 100% всех системных ресурсов и тем самым блокирует все запросы пользователей на доступ к файлам сервера. В этом случае целесообразнее применять систему обнаружения атак на уровне ОС или выбрать небольшое число самых важных файлов, целостность которых должна контролироваться. Аналогичные примеры можно привести и для других технологий.

Даже краткий анализ приведенных выше рекомендаций по защите сетей Интранет (что, от чего, от кого, как и чем защищать) показывает, что если мы хотим создать самую эффективную и лучшую защиту, а в принципе это может реализовать только система по надежному обнаружению всех нарушений политики безопасности ресурсов Итранет, то мы безусловно отдадим предпочтение новым и перспективным SDA-системам. Рассмотрим их возможный базовый состав и классификацию. За основу возьмем SDA-системы для обнаружения и защиты от наиболее опасных атак для Интранет – атак НСД.

Обычно классическая атака НСД осуществляется в три этапа (рис. 1) [4].

Рисунок 1 – Этапы реализации атаки НСД

Первый этап – предварительные действия перед атакой или сбор информации об объекте атаки НСД (information gathering UAA); второй этап – реализация атаки НСД (exploitation UAA); третий этап – завершение атаки НСД (ending of atak UAA). Обычно, когда говорят об атаке НСД, то подразумевают именно второй этап, забывая о первом и последнем. Сбор информации об объекте атаки и завершение атаки ("заметание следов"), в свою очередь, также могут являться атакой и, соответственно, разбиваться на три этапа.

Но основной этап – это сбор информации об объекте атаки НСД. Именно эффективность работы злоумышленника на данном этапе является залогом успешной атаки. В первую очередь выбирается цель нападения и собирается информация о ней (ОС, сервисы, конфигурация, субд, приложения и т. д.). Затем идентифицируются наиболее уязвимые узлы атакуемой Интранет, воздействие на которые приведет к нужному результату.

На первом этапе злоумышленник пытается выявить все каналы взаимодействия объекта атаки с другими узлами. Это позволит не только выбрать тип реализуемой атаки, но и источник ее реализации. Предположим, атакуемый узел взаимодействует с двумя серверами под управлением ОС UNIX и Windows NT. С одним сервером атакуемый узел имеет доверенные отношения, а с другим – нет. В зависимости от того, через какой сервер злоумышленник будет осуществлять нападение, зависит, какая атака НСД будет задействована, какая утилита будет ее реализовывать и т. д. Затем, на основании полученной информации и преследуемого результата выбирается атака, дающая наибольший эффект. Например, для нарушения функционирования узла можно использовать SYN Flood, Teardrop, UDP Bomb и т. п., а для проникновения на узел и похищения информации – сценарий phf для кражи файла паролей, удаленного подбора пароля и т. д. Затем приходит очередь второго этапа - реализация выбранной атаки НСД.

Традиционные средства защиты Интранет (популярные межсетевые экраны, различные пакеты фильтрующих программ, фильтрующие маршрутизаторы и др.) вступают в действие на втором этапе, совершенно "забывая" о первом и третьем [2, 3, 5]. Это влечет за собой то, что зачастую совершаемую атаку очень трудно остановить даже при наличии мощных и эффективных средств защиты. Пример тому –

исключительно опасные распределенные атаки НСД (из нескольких источников и по нескольким узлам Интранет). Логично было бы, чтобы традиционные средства защиты начали работать еще на первом этапе, т. е. предотвращали возможность сбора информации об атакуемом узле Интранет. Это позволило бы если и не полностью "обезглавить" атаку, то существенно усложнить работу злоумышленника.

Также традиционные средства не позволяют обнаружить уже совершенные атаки НСД и оценить ущерб после их реализации (третий этап) и, следовательно, нельзя определить меры по предотвращению таких атак впредь.

В зависимости от достигаемого результата нарушитель концентрируется на том или ином этапе. Например, для отказа в обслуживании он в первую очередь подробно анализирует атакуемую сеть и выискивает в ней лазейки и слабые места для атаки на них и выведения узлов сети из строя. Для хищения информации злоумышленник основное внимание уделяет незаметному проникновению на анализируемые узлы при помощи обнаруженных ранее уязвимостей. Но подробно описать технологию всех этапов атак НСД – это предмет отдельного разговора. Даже приведенный краткий анализ этапов атак НСД показал, что довольно популярные традиционные средства защиты сетей бессильны перед вторым и третьим этапами атаки НСД на Интранет. Только SDA-системы эту задачу решают успешно на всех трех этапах атаки НСД. Рассмотрим их класификацию, возможный базовый (типовой) состав и уже существующие продукты.

Обнаруживать, блокировать и предотвращать нарушения политики безопасности можно несколькими путями [2, 3, 5].

Первый, и самый распространенный способ – это распознавание уже реализуемых атак. То есть, если вспомнить этапы реализации атак (рис. 1), то в соответствии с предложенной классификацией данный способ функционирует на втором этапе осуществления атаки. Этот способ применяется в "классических" системах обнаружения атак (например, RealSecure Network Sensor или Cisco IDS), межсетевых экранах (таких как Check Point Firewall-1), системах защиты информации от НСД (например, SecretNet) и т. п. Однако недостаток средств данного класса в том, что атаки могут быть реализованы повторно. Они также повторно обнаруживаются и блокируются. И так далее, до бесконечности, что, само собой разумеется, неэффективно, т. к. приводит к непозволительной трате временных, человеческих и материальных ресурсов. Было бы правильнее предотвращать атаки еще до их осуществления. Это и есть второй способ. Реализуется он путем поиска уязвимостей, т. е., представляет собой обнаружение потенциальных атак, которые могут быть использованы для совершения атаки.

И, наконец, третий путь – выявление уже совершенных атак и предотвращение их повторения в дальнейшем. В силу сказанного системы обнаружения нарушений политики безопасности могут быть классифицированы по этапам развития атаки (рис. 2). Типовой состав SDA-системы для защиты Интранет может включать в себя:

системы, функционирующие на первом этапе осуществления атак и позволяющие обнаружить уязвимости Интранет, используемые нарушителем; средства этой категории называются системами анализа защищенности (security assessment systems) или сканерами безопасности (security scanners); примерами таких систем являются Internet Scanner или SATAN; некоторые специалисты считают неправильным причисление систем анализа защищенности к классу средств обнаружения атак, однако, если следовать описанным выше принципам классификации, то такое отнесение вполне логично;

системы, действующие на втором этапе осуществления атаки и позволяющие выявить 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; примерами таких систем являются RealSecure Network Sensor или Okena StormWatch; помимо этого, в последнее время выделился новый класс средств обнаружения атак – обманные системы (deception systems); в качестве примера таких систем можно привести RealSecure Server Sensor или DTK;

– системы, действующие на третьем этапе осуществления атаки и обнаруживающие уже совершенные атаки; эти системы делятся на два класса – системы контроля целостности (integrity checkers), отслеживающие изменения контролируемых ресурсов, и системы анализа журналов регистрации (log checkers); в качестве примеров таких систем могут быть названы Tripwire или RealSecure Server Sensor.

Помимо приведенной (рис. 2), существует еще одна распространенная классификация обнаружения нарушения политики безопасности (SDA-систем) – по принципу реализации или по уровням сети (рис. 3):

host-based, т. е. обнаружение уязвимостей или атак, направленных на конкретный узел сети;

- network-based – обнаружение уязвимостей или атак, направленных на всю сеть или сегмент сети.

- системы обнаружения атак на уровне прикладного ПО (application-based), выявляющие атаки на конкретные приложения (например, на Web-сервер); примерами таких систем являются RealSecure OS Sensor или WebStalker Pro;

Рисунок 2 – Классификация систем обнаружения атак НСД по етапам их реализации

Рисунок 3 –- Классификация систем обнаружения атак НСД по принципам (уровням) их реализации в Интранет

- системы обнаружения атак на уровне ОС (OS-based), распознающие атаки на уровне операционной системы; примерами таких систем служат DirectoryAlert и ServerAlert компании NetVision, обнаруживающие атаки в сетях Netware;
- системы обнаружения атак на уровне системы управления базами данных (DBMS-based), обнаруживающие атаки на конкретные системы управления базами данных (СУБД).

Выделение средств обнаружения атак на СУБД в отдельную категорию связано с тем, что современные СУБД уже вышли из разряда обычных прикладных приложений и по многим своим характеристикам, в т. ч. и по сложности, приближаются к операционным системам. При этом системы обнаружения атак (точнее, системы анализа защищенности) на уровне СУБД могут функционировать как на самом узле, так и через сеть (например, Database Scanner). В свою очередь, система обнаружения атак на уровне сети может быть локализована и на конкретном узле для регистрации атак, направленных не на все узлы сегмента, а только на тот, на котором она установлена. Пример такой системы – RealSecure Desktop Protector.

Данная классификация может вызвать споры. Многие специалисты считают неправильным отнесение сканеров безопасности к системам обнаружения атак. Аналогичная ситуация и с системами контроля целостности и анализа журналов регистрации. Эти системы помогают в обнаружении атак, "но на системы IDS совсем не похожи". Не будем оспаривать этот факт, заметим только, что с учетом этапов реализации атак приведенная классификация вполне закономерна.

Кроме того, до сих пор не выработана единая терминология в этой области. Каждый производитель, желая показать, что его система уникальная и превосходит другие решения, создает новый класс систем обнаружения атак. Так появились гибридные системы обнаружения атак (например, Prelude IDS), виртуальные системы обнаружения атак (например, IntruShield от In-truVert), многоуровневые системы (multitiered IDS), шлюзовые (gateway IDS), системы с контролем состояния (stateful IDS) и даже системы, основанные на спецификациях (specification-based IDS) или стеке (stack-based IDS) и т. д.

Дадим несколько практических советов для выбора/создания системы обнаружения атак (SDA-системы) по совокупности некоторых критериев, которые рекомендуется использовать для различных категорий пользователей Интранет по опыту ведущих западных стран [2, 3, 5].

Все требования к выбираемой системе обнаружения атак НСД (SDA-системе) можно условно разделить на три группы – обязательные, желательные и дополнительные. Поскольку не существует системы, которая удовлетворяла бы всем описываемым ниже требованиям, то свой выбор надо останавливать на той системе, которая в первую очередь удовлетворяет обязательным требованиям, независимо от соответствия большому числу дополнительных критериев оценки. Заранее определить необходимость того или иного критерия не представляется возможным, это зависит от множества условий, в том числе и от типа потребителя Интранет. Все критерии оценки условно можно разделить на несколько групп, которые являются основой для тестирования систем обнаружения атак: обнаружение атак; реагирование на атаки; управление; производительность; собственная защита; инсталляция и конфигурация; дополнительные возможности; производитель/поставщик. Группы критериев оценки разбиваются затем еще на ряд частных критериев и т. д. Полный перечень рекомендуемых критериев оценки для выбора / создания SDA-системы с указанием их приоритета (3 – очень важно, 1 – неважно) для различных категорий пользователей Интранет приведен в табл. 2. Выборочно проанализируем некоторые критерии оценки.

Таблица 2 – Приоритеты различных критериев выбора систем обнаружения атак

Критерий	Малые компании	Крупные компании	Транснацио-нальные компании	Internet-провайдер	Провай-дер услуг	Госу-дарство
Обновление атак	3	3	3	3	3	3
Способ обновления	1	3	3	2	3	3
Создание своих событий	1	2	2	3	3	2
Мониторинг дополнит. событий	3	2	1	1	1	1
Уведомление о пропуске атак	2	2	2	3	3	2
Создание вариантов реагирования	1	2	2	2	3	1
Удаленное управление	1	3	3	2	3	3
Неограниченное число управляе-мых сенсоров	1	2	3	2	3	3
Иерархическое управление	1	2	3	1	1	2
Групповые операции с сенсорами	1	2	3	2	2	2
Корреляция событий	1	2	3	1	3	3
Динамическое изменение - приоритета атаки	1	2	3	1	3	3
Анализ тенденций	1	2	3	1	3	3
Отображение событий	3	3	3	2	3	2

Продовження Таблиці 2.

Группирование защищаемых ресурсов	1	2	3	1	3	2
Единая консоль управления	1	2	3	3	3	3
Поддержка единого времени	1	1	3	1	3	3
Автоматизация рутинных задач	1	2	3	1	2	2
Поддержка шаблонов	1	2	3	1	3	3
Защита от НСД	1	2	3	3	3	3
Отказоустойчивость	1	3	3	3	3	2
Интеграция	1	2	3	3	3	2
Инсталляция	1	2	3	1	1	3
Обучение	2	3	3	1	2	2

Место (уровень) установки SDA-системы. Это первый по важности критерий. Существуют две основные точки установки систем обнаружения атак – на сегменте сети Интранет и на конкретном узле. В зависимости от того, какой ресурс должен быть защищен, может быть применена (см. табл. 1) либо система обнаружения атак уровня сети (network-based), либо система, функционирующая на уровне ОС, СУБД или приложений (host-based). Например, если необходимо обеспечить безопасность файлового сервера, то приоритетом должны пользоваться системы контроля целостности. Для серверов приложений на первое место выходят средства анализа журналов регистрации. При этом выбираемая система должна контролировать не только системные (EventLog или syslog), но и любые «другие журналы регистрации. Для защиты Web-сервера можно выбрать две системы обнаружения атак, отталкиваясь от того, где он расположен. Например, если Web-сервер размещается в демилитаризованной зоне (ДМЗ), в которой также находятся и другие узлы (SMTP-, FTP-, DNS-серверы), то вся ДМЗ контролируется системой обнаружения атак уровня сети, а конкретный Web-сервер – системой анализа журналов регистрации. В том случае, если в ДМЗ установлен только один Web-сервер, то целесообразнее применение интрегрированного решения, объединяющего контроль журналов регистрации и «Обнаружение сетевых атак» (например, RealSecure Server Sensor)**.** Но если необходимо защищать как сетевые, так и системные ресурсы, то желательно выбирать систему обнаружения атак, имеющую сетевой и системный компоненты. Примером такой системы является семейство RealSecure Protection System, позволяющее обнаруживать атаки на уровне сети (RealSecure Network Sensor), серверов (RealSecure Server Sensor) и рабочих станций (RealSecure Desktop Protector). Другими представителями можно назвать продукты компании Symantec, предлагающей системы NetProwler (обнаружение сетевых атак) и Intruder Alert (контроль журналов регистрации) или Cisco с ее системами Cisco IDS и Cisco IDS Host Sensor.

Создание в SDA-системе собственных контролируемых событий. Как бы часто ни обновлялась база данных сигнатур атак или уязвимостей системы, всегда проходит какое-то время между сообщением о новой атаке (уязвимости) и появлением сигнатуры для нее. Уменьшение этого интервала — одна из главных задач, стоящих перед эксплуатирующим SDA-систему подразделением. Один из путей ее решения — создание своих собственных сигнатур. Решаться это может двумя способами — использованием специального языка описания атак НСД (уязвимостей от НСД) или прямым заданием параметров атаки при помощи специальной подсистемы. Механизм описания своих проверок, уязвимостей, атак и иных контролируемых событий является очень полезной возможностью для администраторов, отслеживающих уязвимости, описанные в Bugtraq и иных списках рассылки.

Благодаря ей становится возможным быстро сформулировать новое правило и использовать его в своей сети. Однако следует заметить, что хотя данная возможность и является полезной, ее необходимость для конечного пользователя достаточно эфемерна. В практической деятельности мало организаций, которые могли бы себе позволить содержать целый штат, занимающийся исследованиями в области новых проверок и уязвимостей Интранет (мы не берем в расчет военные ведомства и иные организации, работающие в области защиты информации). Как правило, люди, отвечающие за обеспечение безопасности, не обладают глубокими познаниями в программировании. Кроме того, помимо написания новых правил, на них «висит» еще много других задач (контроль деятельности пользователей, установка прав доступа, противодействие ПЭМИН и т. д.), и они просто не имеют времени для такой творческой работы, как создание новых правил.

Однако наличие в системе обнаружения атак такого языка является дополнительным плюсом в пользу ее выбора. Например, применяются специальные языки P-BEST, N-Code, Attaks Signature Definition, RUSSEL, SNP-L Scripting Systems, SecureLogic, CASL, NASL, STAYL, Perl и C и др. Однако отметим, что, к сожалению, эти языки являются «вещью в себе», т. к. сигнатуры, написанные на них, не могут быть

перенесены в другие системы. Исключение составляет язык, используемый в системе Snort, который «понятен» и некоторым другим системам обнаружения атак, например, RealSecure Network Sensor. Для примера приведем некторые из них.

P-BEST (Production-Based Expert System Toolset) — это экспертная система со своим собственным языком, которая позволяет описывать различные нарушения политики безопасности. Данная система была разработана Аланом Вайтхастом (Alan Whitehurst) и использовалась в системе MIDAS для обнаружения атак на сеть Dockmaster NCSC. Позже, по заказу DARPA, разработка была функционально расширена в лаборатории SRI и задействована в системах IDES и NIDES.

Язык описания атак и злоупотреблений, реализованный в оболочке P-BEST, достаточно прост и позволяет, при должной сноровке, быстро формализовать практически любые несанкционированные действия. Например, попытка неудачного входа в систему описывается всего 9-ю строками (листинг 1).

Листинг 1. Пример правила обнаружения попытки неудачного входа в систему на языке P-BEST

```
rule [Bad_Login(#10;*):
        [+e:event| event_type = = login,
                return__code = = BAD_PASSWORD]
        [+bad_login| username = e.username, hostname = e.hostname] [-Ie]
         [!|printf("Bad login for user %s from host %s\n", e.username, e.hostname)]
]
```

Первая строка указывает на название правила (Bad_Login), его приоритет (10) и разрешение многократного применения (*). Все последующие строки описывают сам факт неудачного входа в систему и механизм уведомления. Кроме того, вырабатываемые правила могут быть легко интегрированы с языком C, что делает возможности P-BEST практически безграничными. За более чем 10 лет своего существования экспертная оболочка P-BEST была интегрирована с различными системами обнаружения атак, в т. ч. и с системой EMERALD, позволяющими идентифицировать атаки и злоупотребления для ОС Multics и UNIX (SunOS, Solaris, FreeBSD и Linux).

SNP-L Scripting System – язык, очень напоминающий C, реализованный в системе обнаружения атак SecureNet PRO и предназначенный для описания атак. Одна из отличительных особенностей языка SNP-L – наличие так называемой «песочницы» (sandbox), во многом схожей с аналогичной технологией, реализованной в языке Java. Все создаваемые сценарии атак выполняются в «песочнице», что позволяет защитить компьютер, на котором установлена система обнаружения атак, от отказов сценария или других нежелательных воздействий [Intrusionl-00].

Язык Attack Signature Definition (ASD), реализованный в системе обнаружения атак NetProwler, предназначен для создания сигнатур атак, отсутствующих в существующей базе данных. Этот процесс состоит из 4-х шагов.

1. *Генерация и сбор данных.* Все атаки, обнаруживаемые системой NetProwler, делятся на две категории – ориентированные на соединение (реализуемые по протоколу TCP) и неориентированные (для протоколов UDP и ICMP). На этом этапе вырабатывается трафик, который затем анализируется, сохраняется в текстовом файле и после этого из него выделяются атаки.

2. *Анализ данных.* Идентифицируется вся информация, которая позволит в дальнейшем описать сигнатуру атаки. Анализ происходит на основе файла, сохраненного на предыдущем этапе. Необходимо заметить, что анализ все-таки осуществляется вручную, и специалист, за него отвечающий, должен иметь соответствующую квалификацию, чтобы выделить в сетевом графике признаки атаки.

3. *Создание сигнатуры атаки.* При описании сигнатуры атаки используется ряд параметров:

- *тип атаки;* существуют три типа атак – Simple, Counter-based и Sequental-based; первый тип предназначен для простых атак, описываемых всего одним сетевым пакетом; второй – служит для описания атак, оперирующих несколькими пакетами в течение заданного интервала времени (например, три неудачных попытки удаленного входа в систему в течение 60 секунд); последний тип используется для самых сложных атак, которые пронизывают несколько сетевых пакетов, направленных к нескольким приложениям (или от нескольких приложений) и обнаруженных в определенной последовательности; скажем, такой атакой могут быть последовательные попытки аутентификации на сервисах Telnet, Riogin, Rsh, осуществляемые в течение 180 секунд;
- *свойства* – расширенное описание некоторых атак, например, при помощи одного из свойств можно указать, что 4 неудачные попытки аутентификации с 4-х разных узлов не являются атакой, а те же 4 неудачные попытки с одного узла явно характеризуют атаку;
- *операционные системы и приложения*, подверженные атаке;
- *приоритет;* данный параметр позволяет назначить приоритет создаваемой сигнатуре атаки – низкий, средний и высокий;

- *категория;* задает категорию создаваемой сигнатуры; надо заметить, что категории согласно данной классификации абсолютно идентичны категориям, имеющимся в системе обнаружения атак RealSecure; к ним относятся: «отказ в обслуживании», «предварительные действия перед атакой», «попытки неавторизованного доступа», «подозрительная активность», «сетевой протокол» и «разное»;

- *критерии поиска;* к таким критериям причисляются различные дополнительные признаки, характеризующие атаку, такие как ключевые слова или регулярные выражения.

4. Тестирование и отладка сигнатуры.

В процессе описания сигнатур можно использовать различные предопределенные переменные, облегчающие работу администратора безопасности (например, IP_SRC_ADDRESS или ICMP_TYPE). К указанным переменным могут быть применены различные арифметические, логические и иные операторы - «И», «ИЛИ», «НЕ», «<>=», «!=»,»+», «/» и т. д.

CASL (Custom Audit Scripting Language, прежнее название – Custom Attack Simulation Language) — это язык и одноименная подсистема, входящие в состав системы анализа защищенности CyberCop Scanner. Они были разработаны компанией Network Associates, а, точнее Secure Networks, для расширения возможностей своего сканера Ballista, впоследствии переименованного в CyberCop Scanner. В настоящий момент подсистема CASL выделена в отдельный, функционирующий под управлением ОС Windows NT и Linux, продукт, который можно загрузить с сервера компании Network Associates. Язык CASL достаточно прост и позволяет описывать любые поля заголовков пакетов для различных протоколов, базирующихся на ICMP, IP, TCP и UDP [CyberCopl-00]. CASL оперирует переменными, операторами и пакетами и очень похож на N-Code. Например, параметр ip. src в языке N-Code аналогичен параметру ip_source в языке CASL (листинг 2).

Листинг 2. Пример описания скрытого TCP-сканирования на языке CASL

```
#include “tcpip.casi”
#include “packets.casi” for(i =1; i <1023; i =i +1)( OurSYN = copy SYN;
        OurSYN.tcp_source = 10;
        OurSYN.tcp_destination = i;s
        OurIP = copy TCPIP;
        OurIP.ip_source = 127.0.0.1;
        OurIP.ip_destination = 127.0.0.2;
        OurPacket = [ OurIP, OurSYM ] ;
        ip_output(OurPacket) ;
        OurFilter = [ “src host «, 127.0.0.2, « and tcp src port «, i ];
        ReadPacket = ip_input(2000, OurFilter);
        if(!ReadPacket)
                continue;
        if(size(ReadPacket) < size(IP) + size(TCP))
                continue;
        ReadIP=extract ip from ReadPacket;
        ReadTCP=extract tcp from ReadPacket;
        if(ReadTCP.tcp_ack != 1
                        I| ReadTCP.tcp_syn != 1 II ReadTCP.tcp_rst == 1)
                continue;
        print(«Порт «, i, « открыт»);
```

NASL (Nessus Attack Scripting Language) — это язык описания атак, разработанный для системы анализа защищенности Nessus. Он очень похож на язык C**,** но, по мнению разработчиков, по многим параметрам (например, скорости исполнения сценария) уступает другим языкам, таким как Tel, Python, Peri. Однако те задачи, для решения которых он был создан, этот язык выполняет с достаточной эффективностью (листинги 3 и 4). Как и многие другие языки описания атак, NASL помимо переменных, операторов, функций и других элементов может оперировать сетевыми пакетами, что существенно облегчает работу администратора безопасности.

Листинг 3. Фрагмент сценария на языке NASL для описания проверки, позволяющей обнаружить уязвимость Web-сервера

```
if(is_cgi_installed(“php.cgi”)){ display(«CGI-сценарий php.cgi установлен в каталоге /CGI-bin\n”);
}
```

Листинг 4. Фрагмент сценария на языке NASL для описания проверки, позволяющей обнаружить уязвимость FTP-сервера

```
soc = open_sock_tcp(21) ;
```

```
if(ftp_log_in(socket:soc, user:"ftp", pass:"luka@")) (
    port = ftp_get_pasv_port(socket:soc);
    if(port) (
                soc2 = open_sock_tcp(port);
    data = string("RETR /etc/passwd\r\n") ;
    send(socket:soc, data:data);
password_file = recv(socket:soc2, length:10000);
    display(password file);
                close(soc2);
    ) close(soc) ;
```

VDLnVEL. Очень удобными с точки зрения конечного пользователя, не знакомого с языками C, Peri или Tc1, являются языки VDL (Vulnerability Descriptive Language) или VEL (Vulnerability Exploit Language). Оба они созданы компанией Cisco Systems и используются в системе анализа защищенности Cisco Secure Scanner. Проверки, описываемые этими языками, основаны на простых логических утверждениях (листинг 5), и пользователь может в течение нескольких секунд добавить нужные правила. К сожалению, данный продукт больше не выпускается компанией Cisco.

Листинг 5. Пример правила на языке VDL. Определение наличия сервиса Telnet

Секция описания сервисов: На анализируемом узле найден Telnet port 23 using protocol tcp => Service:Remote-Access:my telnet

Данная проверка описывает правило, которое определяет наличие сервиса Telnet на 23-м TCP-порту анализируемого узла. Следующее, более сложное, правило идентифицирует запущенное приложение SuperApp устаревшей версии по заголовку, возвращаемому на запрос, обращенный к портам 1234 или 1235 (листинг 6).

Листинг 6. Пример правила на языке VDL. Определение наличия приложения SuperApp

Пользовательская проверка: Приложение SuperApp 1.0 запущено

на сканируемом хосте

(scanfor "SuperApp 1.0» on port 1234) |[(scanfor "SuperApp 1.0 Ready" on port 1235) => VUL:3:01d-Software:Super-App-Ancient:Vp:10003

Данная потенциальная уязвимость (vp), имея приоритет 3, относится к типу «устаревшего (потенциально уязвимого) программного обеспечения» (old-software) и носит название supper-App-Ancient, задаваемое пользователем. Число определяет уникальный номер записи в базе данных уязвимостей системы Cisco Secure Scanner (Network Security Database, NSDB).

При помощи языка VDL можно описывать три категории правил, позволяющие идентифицировать [Cisco 1-99] сетевые сервисы, тип операционной системы, уязвимости.

Компания Cisco Systems делит все уязвимости на два класса:

– потенциальные (potential) — вытекающие из проверок заголовков и так называемых активных «подталкиваний» (nudge) анализируемого сервиса или узла; потенциальная уязвимость, возможно, существует в системе, но активные зондирующие проверки не подтверждают этого; данный тип проверок идентифицируется ключевым словом vp;

– подтвержденные (confirmed) – выявленные и существующие на анализируемом хосте; данному типу проверок соответствует ключевое слово vc.

Проверки на потенциальную уязвимость реализуются через анализ заголовков и с помощью «несильных подталкиваний». «Подталкивание» используется для сервисов, не возвращающих заголовки, но реагирующих на простые команды, например, посылку команды HEAD для получения версии HTTP-сервера. Как только эта информация получена, система Cisco Secure Scanner задействует специальный механизм (rules engine), который реализует ряд правил, подтверждающих или не подтверждающих существование потенциальной уязвимости. Таким образом, администратор знает, какие из обнаруженных уязвимостей действительно присутствуют в системе, а какие требуют подтверждения.

Однако можно заметить, что язык, встроенный в систему Cisco Secure Scanner и описывающий эти правила, достаточно элементарен и может помочь только в самых простых случаях. В сложных ситуациях, когда проверку нельзя записать одним правилом, необходимо строить более сложные сценарии, что можно достигнуть применением языков Peri, Tel или C.

STATL (State Transition Analysis Technique Language). Язык был разработан в университете Калифорнии и позволяет описать компьютерное вторжение как сценарий атаки, представляющий последовательность переходов между состояниями безопасности системы. Этот метод был впервые применен в системах обнаружения атак USTAT и NetSTAT.

Perl и C. Попытки добавить новое в механизмы описания уязвимостей, проверок и т. д. велись давно, и практически ни одна компания-разработчик не осталась в стороне. Первая такая попытка была предпринята Витсом Венема и Деном Фармером – создателями системы анализа защищенности SATAN. Описание новых уязвимостей в данной системе, точнее их проверок, осуществлялось при помощи языка Perl. Эта достаточно нетривиальная задача требовала обшиирных знаний как языка Perl, так и архитектуры стека протоколов TCP/IP и сканируемой операционной системы. По тому же пути (снова Perl) пошли шзработчики системы WebTrends Security Analyzer. Язык Perl, наряду с языком C, используется и в системе Internet Scanner. Достоинство языков Perl или C в том, что проверки и правила, написанные для одной системы, практически без изменений могут быть перенесены в другую систему.

Система подсказки по каждой атаке НСД. Не надо доказывать тот факт, что очень трудно быть специалистом по операционным системам и приложениям, используемым в корпоративной сети. Также нельзя досконально разбираться во всем многообразии существующих атак. Поэтому еще одним критерием при выборе системы обнаружения вторжения является наличие подсказки по каждой из обнаруживаемых атак, описывающей не только механизм ее реализации, но и уязвимые платформы, варианты ложного срабатывания (false positives и Ise negatives) и т. п.

Варианты реагирования на атку НСД. Мало выявить и идентифицировать атаку НСД – необходимо на нее соответствующим образом отреагировать. Именно варианты реагирования во многой определяют эффективность системы обнаружения атак. Все варианты реагирования, которые могут быть задействованы системой обнаружения атак при идентификации несанкционированной деятельности, делятся на две категории:

пассивные варианты реагирования, заключающиеся в обычном информировании персонала об обнаруженных атаках, злоупотреблениях и иных аномальных проявлениях; к данной категории могут быть отнесены — уведомление на консоль системы обнаружения атак, генерация управляющих SNMP-последовательностей для систем сетевого управления, регистрация события в базе данных и т. д.;

активные варианты реагирования, включающие разрыв соединения с атакующим узлом или блокировку учетной записи нарушителя, реконфигурацию сетевого оборудования и средств защиты, автоматическое устранение уязвимости и т. д.

Уведомление об атаке НСД. Самый первый вариант реагирования, который был реализован в системах обнаружения атак – это уведомление администратора безопасности или оператора системы обнаружения атак. В современных средствах предусмотрен полный спектр различных вариантов реагирования, начиная от посылки сообщений на консоль системы обнаружения атак и заканчивая отправкой звукового оповещения на телефон. Обычно в системе обнаружения атак предусмотрено 2 – 3 варианта реагирования: посылка уведомления на консоль системы обнаружения атак, генерация сообщения электронной почты (по протоколу SMTP) и сообщения для системы сетевого управления (по протоколу SNMP). В некоторых разработках существуют и другие варианты уведомления. Например, в системах NetProwler и eTrust IDS реализован сигнальный механизм для пейджера администратора безопасности, а в программе eTrust IDS каждое обнаруживаемое событие может быть обозначено звуковым сигналом или информация о нем может быть послана по факсу. В системе RealSecure возможностей посылки факсимильных уведомлений или на пейджер нет, однако RealSecure может быть интегрирована с системой AlarmPoint компании Singlepoint Systems. Данная система предназначена для реализации различных сценариев оповещения при помощи разнообразных средств – факса, телефона, пейджера, мобильного телефона, электронной и голосовой почты и т. д.

Очень интересная, хотя и редко применяемая, возможность имеется в системе RealSecure Server Sensor. С ее помощью оповещение об обнаружении несанкционированной деятельности посылается не администратору, а злоумышленнику. По мнению разработчиков системы RealSecure, это дает понять нарушителю, что его обнаружили, и вынуждает его прекратить свои действия. И еще один вариант уведомления, который также реализован в системе RealSecure, когда информация об атаке посылается на консоль межсетевого экрана. Если речь идет о системе обнаружения атак RealSecure Network Sensor, разработанной компанией ISS, то в качестве межсетевого экрана выступает Lucent Managed Firewall компании Lucent. Для системы RealSecure, выпускаемой компанией Check Point в соответствии с соглашением с компанией Internet Security Systems, таким межсетевым экраном является Firewall-1. Учитывая повальный спрос и распространение средств мобильной связи, можно предположить, что в системах обнаружения атак скоро появится механизм уведомления по SMS.

Регистрация событий. Регистрация обнаруживаемых событий – обязательное условие для любой системы обнаружения атак. Можно отметить два аспекта – куда и в каком объеме записываются события. В качестве журнала регистрации может выступать текстовый файл, системный журнал (например, в системе Cisco IOS Firewall Feature Set), текстовый файл специального формата (например, в системе

Snort), локальная база данных MS Access (как в системе Internet Scanner), SQL-база данных (в системе Spitfire или RealSecure). Желательно, чтобы в системе обнаружения атак был реализован механизм работы с базой данных, ориентированный не на специалиста. В противном случае может возникнуть ситуация, когда, например, SQL-база переполнилась, и необходимо произвести ее очистку или резервирование, а сделать это может только специалист по SQL, который отсутствует в данный момент на рабочем месте. Во всех случаях стоит помнить о скорости обработки данных. Ведь в базу попадают сотни тысяч сообщений в день, и если взаимодействие между консолью и базой данных будет неэффективным, то пользоваться такой системой будет очень неудобно, а, подчас, и невозможно.

Тестировапние систем обнаружения атак. Эта процедура является обязательной для проверки соответствия заявленных возможностей системы обнаружения атак применительно к конкретной конфигурации Интранет своей организации. Администратор безопасности Интранет при приобретении системы обнаружения атак не должен безоглядно доверять всем заявлениям продавца или разработчика, даже документально описанных.

Практически во всей существующей открытой литературе нет описания методов тестирования, каждая организация/компания, проводящая испытания, разрабатывает свою методику тестирования, которая является ноу-хау компании, держащимся в большом секрете. Исключением является Лаборатория Линкольна, которая разрабатывает стандарт тестирования средств обнаружения атак, функционирующих на уровне сети. Однако доступ к этим материалам ограничен, получить их очень трудно и цитировать их запрещено. Желающих попробовать ознакомиться с ними можно направить на Web-сервер с ограниченным доступом http://ideval.ll.niit.edu**.** А совсем недавно появился стандарт OSEC (Open Security Evaluation Criteria), который также предназначен для тестирования средств защиты информации. Первыми были выпущены критерии для сетевых систем обнаружения атак **(**http://osec.neohapsis.com/**).**

Отсутствие единой методологии приводит к тому, что каждая организация, проводящая тестирование, разрабатывает свою методику. Поэтому бывают курьезные случаи, когда одна и та же система показывает противоположные результаты в разных тестах. Это происходит потому, что каждая тестирующая лаборатория отличается не только проводимыми тестами, но и средой, в которой проводится тестирование, уровнем квалификации специалистов, приоритетом оцениваемых критериев и т. д.

Предлагаем несколько советов, облегчающих эту задачу. Все тесты можно условно разделить на классы в соответствии с группами описанных ранее критериев оценки систем обнаружения атак [5].

- **Обнаружение атак** – данный класс один из важных, и именно эти тесты проводятся всеми тестовыми лабораториями. Однако, как уже упоминалось выше, важно не количество сигнатур, содержащихся в базе данных системы обнаружения атак, а то, как эффективно IDS может обнаружить атаку в обычном графике. То есть насколько эффективно система обнаружения атак может идентифицировать признаки вторжения в шумовом, фоновом графике. Это все равно, что искать иголку в стоге сена. А ведь в лабораторных условиях, как правило, проверяется именно первый, а не второй критерий. В эту же категорию тестов входит и проверка обнаружения атак, типичных для вашей сети Интранет, и способность настройки существующих и создания новых сигнатур атак и т. п. Если вы не в состоянии проверить все возможные атаки, то попробуйте «натравить» на тестируемую систему атаки из «горячей двадцатки» SANS — The Twenty Most Critical Internet Security Vulnerabilities. Можно предположить, что производители должны в первую очередь обнаруживать именно эти атаки, однако это происходит далеко не всегда, что удивительно, т. к. именно эти нападения являются самыми распространенными в мире.

- **Производительность** – эффективность системы обнаружения атак не ограничивается способностью обнаруживать атаки в обычном графике. Грамотно разработанная система не спасует и перед стресс-тестами, в рамках проведения которых интенсивность генерации графика существенно повышается по сравнению с обычными условиями. Например, лаборатория NSS проводила свои тесты при нагрузке в 25, 50, 75 и 100 Мбиг/с, а компания Miercom – при нагрузке 40, 60 и 90 Мбит/с. Только в том случае, если система обнаружения атак может выявлять атаки в сильнонагруженных сетях, она может считаться действительно эффекгивной. Помимо нагрузки, еще одним параметром, который должен учитываться в тестах, является длина пакета. При тестировании сетевых систем обнаружения атак режим передачи пакетов минимальной длины для каждого протокола является самым сложным тестом, позволяющим проверить функциональность IDS при наихудшем сочетании параметров графика. Вновь обращаясь к тестам NSS, можно выделить 3 теста, учитывающих этот критерий, – идеальные условия (длина всех IP-пакетов максимальна и равна 1514 байта для Ethernet), наихудшие условия (длина всех IP-пакетов равна 64 байтам) и обычные условия, в которых средняя длина пакета составляет около 300 байтов. Кстати, при всех прочих равных условиях система обнаружения атак в сети FDDI будет более эффективна, чем в сети Ethernet. Это связано с тем, что значение MTU для FDDI равно 4352, а для Ethernet — 1500 байтов.

Собственная защита – являясь средством защиты, система обнаружения атак не должна быть

причиной снижения защищенности защищаемой с ее помощью корпоративной сети. Поэтому к третьему классу тестов можно отнести тесты на защищенность системы обнаружения атак, т. е. проверку работоспособности в stealth-режиме, защиту собранных данных и данных, передаваемых между сенсорами и консолью управления, возможность ролевого управления доступом и т. д. Классом, который находится на стыке собственной защиты и обнаружения атак, можно назвать категорию тестов, направленных на способность системы обнаружения атак выявлять нападения, специально разработанные для обхода IDS • (Stick, Snot, ADMutate и т. д.).

- **Управление** – этот класс тестов является очень важным, особенно в крупных, территориально-распределенных сетях, в которых насчитываются десятки сенсоров.

- **Функциональные возможности** — *к* данному классу тестов относится все то, что не вошло в другие категории, и это закономерно. Производители, желая привлечь клиента на свою сторону, предлагают ему не только функции, связанные с обнаружением атак, но и множество других, направленных на снижение неудовлетворенности клиента.

Базовый состав стенда для тестирования сетевой системы обнаружения атак на Интранет приведен на рис. 4. В этом варианте не тестируется возможность интеграции системы обнаружения атак с другими средствами, различные схемы управления сенсорами и т. д.

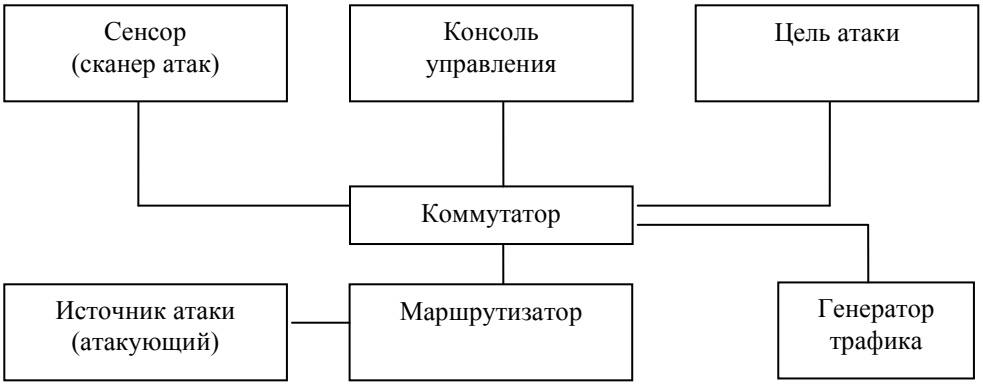

Рисунок 4 – Простейший состав стенда для тестирования сетевой системы обнаружения атак

Для тестирования средств обнаружения атак могут применяться различные программные средства. Например, очень интересным решением является система IDS Informer компании Blade Software. Однако если у вас нет возможности приобрести такие специализированные системы тестирования, можно порекомендовать использование обычных сканеров безопасности, которые имитируют действия настоящих хакеров. Если уж и этот способ недоступен, остается только одно – на любом из множества сайтов соответствующей тематики можно загрузить уже готовые атаки (exploit), которые и запустить для тестирования выбираемой системы обнаружения вторжений. Однако здесь надо помнить, что такая атака может нанести немалый ущерб, и поэтому такое тестирование лучше проводить в изолированной сети.

Выводы

1. Рассмотренный обзорно-аналитический материал по системам обнаружения атак, особенно наиболее опасных из них – атак НСД, позволяет сделать вывод о перспективности этих систем адаптивной безопасности для защиты информационных ресурсов корпоративных сетей Интранет, имеющих постоянное или временное соединение с Интернет. Это актуально, так как все локальные сети организаций / компаний, как правило, активно используют ресурсы Интернет.

2. Традиционные средства защиты с появлением новых систем обнаружения атак не теряют своей актуальности и используются как дополнение к ним при защите ресурсов Интранет.

3. Приведенные рекомендации и советы для выбора / создания систем обнаружения атак по совокупности критериев оценки и тестирования, а также краткий обзор еще раз подчеркивают их актуальность и перспективность.

*Литература: **1**. Шорошев В. В. Недостатки традиционных средств защиты корпоративных сетей Интранет и необходимость применения новых методов их защиты. Бизнес и безопасность № 2, 2003, С. 54 – 59. **2**. В. Шорошев. Перспективный метод защиты информационных ресурсов корпоративных сетей Интранет. Бизнес и безопасность № 6, 2003. С. 38 – 46. **3**. В Шорошев. Перспективный метод защиты информационных ресурсов корпоративных сетей Интранет. Науково-технічний збірник "Правове,*

нормативне та метрологічне забезпечення систем захисту інформації в Україні", НТУ України "КПІ" Міносвіти і науки України, ДСТСЗІ СБ України, випуск № 7, 2003. С. 62 – 77. ***4****. Шорошев В. В., Проскурін В. М., Маєвський Є. Л. Три узагальнених критерії замість сукупності часткових щодо експертної оцінки захищеності інформації від несанкціонованого доступу в автоматизованих (комп'ютерних) системах. Журнал Держкомзв'язку та інформатизації України "Зв'язок" № 5, 2003р. С. 50 – 56.* ***5****. Лукацкий А. В. Обнаружение атак. – 2-е изд., СПб.: БХВ-Петербург, 2003. – 608с.:ил.*

УДК 65.012.8.

МЕТОД ПРОЕКТИРОВАНИЯ ОПТИМАЛЬНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Виталий Носов, Александр Манжай
Национальный университет внутренних дел, г. Харьков

Анотація: **Пропонується модель побудови системи захисту інформації, метод оцінки її ефективності та можливі критерії оптимізації.**
Summary: **The construction model of the defence information system, its efficiency estimation method and possible criteria of optimization, are offered.**
Ключевые слова: **Информационная безопасность, система защиты информации, модель системы защиты информации, оценка рисков, критерии оптимизации системы защиты информации.**

I Введение

Актуальность информационной безопасности в современном, стремительно развивающемся информационном сообществе не вызывает сомнений. За последнее время было опубликовано и издано большое количество трудов, посвященных различным аспектам защиты информации, и все они решали вполне конкретные задачи в этой многогранной проблеме. Как и в большинстве прикладных областей научных знаний, в теории и практике защиты информации постоянно идёт процесс развития и корректировки основных положений, что связано, прежде всего, с развитием самих информационных технологий.

Закрепление тех или иных результатов исследований в области информационной безопасности происходит в виде национальных или международных стандартов и других нормативных документов. На сегодняшний день существует достаточное количество как отечественных, так и зарубежных стандартов и нормативных документов, регламентирующих отдельные аспекты информационной безопасности. Тем не менее, пока в этих документах не определены общепризнанные подходы по оптимизации по различным критериям создаваемой системы защиты информации (СЗИ). Определение этих подходов, их апробация и нормативное закрепление позволит на практике системно и комплексно проектировать СЗИ с последующей обоснованной оценкой её эффективности.

В качестве одного из возможных вариантов предлагается метод проектирования оптимальной СЗИ, учитывающий структуру взаимосвязей объектов защиты внутри информационной системы (ИС), источников угроз, угроз, уязвимостей ИС и механизмов защиты.

II Постановка задачи

Общую зависимость указанных выше основных понятий информационной безопасности (владельцы информации, нарушители, угрозы, уязвимости, риски, контрмеры, информационные ресурсы) весьма наглядно представляет международный стандарт ISO/IEC 15408 "Общие критерии оценки безопасности информационных технологий" (рис. 1).

Анализ отечественной нормативной базы в области информационной безопасности позволил выделить семь этапов в создании СЗИ.

1. Определение информационных ресурсов (ИР), подлежащих защите.
2. Выявление полного множества угроз безопасности ИР, подлежащих защите.
3. Проведение оценки уязвимости и рисков для ИР, подлежащих защите, при выявленном множестве угроз.
4. Разработка проекта (плана) системы защиты информации, снижающего по выбранному критерию риски для ИР, подлежащих защите, при выявленном множестве угроз.
5. Реализация проекта (плана) защиты информации.
6. Определение качества реализованной системы защиты.