На правах рукописи

МИХАЛЕВА Ульяна Анатольевна

ОЦЕНКА УЯЗВИМОСТЕЙ В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ ОРГАНИЗАЦИИ НА ОСНОВЕ СМЕШАННЫХ СТРАТЕГИЙ ТЕОРИИ ИГР

Специальность: 05.13.19 – Методы и системы защиты информации, информационная безопасность

Автореферат

диссертации на соискание ученой степени

кандидата технических наук

Уфа – 2010

Работа выполнена на кафедре технологии и средств связи
Уральского государственного технического университета – УПИ
им. первого Президента России Б. Н. Ельцина

Научный руководитель	д-р техн. наук, проф. **ЛИДСКИЙ** Эмануил Аркадьевич
Официальные оппоненты	д-р техн. наук, проф. **ВАСИЛЬЕВ** Владимир Иванович зав. каф. вычислительной техники и защиты информации Уфимского государственного авиационного технического университета
	д-р техн. наук, проф. **ПОРШНЕВ** Сергей Владимирович зав. каф. автоматики и информационных технологий Уральского государственного технического университета – УПИ
Ведущая организация	ФГУП «НПО автоматики имени академика Н. А. Семихатова» г. Екатеринбург

Защита состоится «__» _____ 2010 г. в 10:00 часов
на заседании диссертационного совета Д – 212.288.07
при Уфимском государственном авиационном техническом университете
по адресу: 450025, Уфа, ул. К. Маркса, 12

С диссертацией можно ознакомиться в библиотеке университета.

Автореферат разослан «___» _____ 2010 г.

Ученый секретарь
диссертационного совета
д-р техн. наук, проф. С. С. Валеев

Общая характеристика работы

Актуальность темы

Сегодня невозможно представить себе ни одну сферу человеческой деятельности без средств вычислительной техники и телекоммуникаций. Информационные технологии предлагают все новые и новые сервисы. Через Интернет становятся доступными электронные платежные системы, персональные финансовые порталы, электронные биржи и т. д. В связи с бурным развитием новых информационных технологий происходит усложнение задач обеспечения информационной безопасности (ИБ).

В работах отечественных исследователей проблематики ИБ А. А. Грушо, В. А. Герасименко, А. А. Кононова, А. А. Малюка, Д. С. Черешкина отмечается необходимость и актуальность системного подхода к решению задач защиты информации, обеспечивающего обоснованность, целостность и последовательность реализуемых мер, их максимальную эффективность. Такой подход позволяет систематизировать нормативно-правовые требования к ИБ и разработать на их основе научные, ориентированные на практическое применение методики, технологии и программы оптимизации деятельности по защите информации.

Так же в настоящее время известен ряд работ в области ИБ, например работы авторов: В. В. Дятчин, П. И. Тутубалин, К. В. Бормотов, А. П. Росенко, А. И. Захаров, Э. А. Лидский в которых применяются методы теории игр. В этих работах теория игр используется для выбора варианта размещения конфиденциальной информации; для оценки и прогнозирования достигнутого уровня защиты информации с учетом выбора наиболее целесообразной стратегии поведения игроков и т.д. В данной диссертации используется новый способ построения платежной матрицы типа смешанной игры атаки и защиты, что позволяет повысить эффективность выявления наиболее опасных уязвимостей организации.

Постановка задачи управления ИБ предполагает осведомленность о существующих угрозах сервису и оценку связанных с ними информационных рисков. Оценка рисков является комплексной задачей и включает анализ организационной и программно-технической составляющей ИБ.

В соответствии с положением стандарта ISO/IEC Guide 73:2002, в котором предлагается методология оценки рисков, величина риска определяется тремя основными факторами:

- степенью уязвимости информационной системы,
- возможностью реализации угрозы через данную уязвимость,
- уровнем ущерба, который может быть причинен в случае реализации угрозы.

В данный момент существуют ряд методик анализа рисков, связанных с угрозами ИБ, такие как Ra2 art of Risk, Risk Advisor, Risk Watch, CRAMM, Система «АванГард», Digital Security Office и т. д.

Все перечисленные методики по-разному, но вполне успешно решают поставленную задачу в рамках, которые предусмотрел их разработчик. Они направлены на оценку рисков, связанных с уровнем защиты ИБ организации. Конечная цель данных методов – на основе анализа существующих способов защиты ИБ, предпринятых в организации, дать рекомендации по организации защиты ИБ вплоть до рекомендации обучения соответствующего персонала. Таким образом, они направлены на создание преграды для угроз ИБ. В отличие от них, данная работа связана с непосредственным устранением самих угроз, конкретно, уязвимости в программном обеспечении.

Оба подхода являются необходимыми и совместимыми. В частности, на устранение угроз требуется время, например, когда обнаруживается уязвимость в программном обеспечении, много времени уходит на обновление программы, а некоторые угрозы устранить вообще невозможно. Выход в создании сетевых средств защиты, предупреждающих ущерб.

Проблема обнаружения уязвимости исследуется давно, и за время ее существования предпринимались различные попытки классифицировать уязвимости по различным критериям. Например, американские проекты Protection Analysis Project и RISOS, исследования лаборатории COAST или компании Internet Security Systems и т.д. Каждая организация проводила и обосновывала свою классификацию. Как показал анализ, нет четких определений и в названиях атак на информационный ресурс.

Для устранения неясности с определением уязвимости и наименованием атаки в 1999 году компания MITRE Corporation предложила решение, независимое от различных производителей средств поиска уязвимости. Это решение было реализовано в виде базы данных (БД) CVE (Common Vulnerability Enumeration), которая затем была переименована в Common Vulnerabilities and Exposures. Это позволило всем специалистам и производителям использовать единую классификацию.

На основе CVE разработаны специализированные открытые БД, содержащие информацию об известных уязвимостях в программных системах, степени их опасности, а также возможности проведения атак на эти уязвимости. Тем самым, возникла и стала актуальной задача эффективного использования имеющихся данных.

В данной работе на основе информации о программном обеспечении, установленном в организации, и использовании открытой БД об уязвимостях была разработана методика оценки рисков, связанных с конкретными уязвимостями в программном обеспечении. Результатом применения этой методики яв-

ляется множество наиболее опасных уязвимостей, которые необходимо устранять в первую очередь. Для оценки рисков были использованы методы теории игр. Параметры, определяющие стратегическое поведение партнеров игры, неизбежный риск и степень неопределенности избираются так, что они могут являться элементами множества, на котором строится игра. При этом удается связать эти элементы с задачей управления (устранение угроз). В диссертационной работе рассматривается решение актуальной задачи выбора параметров для построения игры, построение соответствующего множества их значений, оптимизации выбора решения партнерами игры.

Объект исследования – уязвимости в программном обеспечении организации.

Предмет исследования – эффективные алгоритмы оценки уязвимостей в программном обеспечении организации.

Цель диссертационной работы – повышение эффективности оценки уязвимостей в программном обеспечении организации на основе смешанных стратегий теории игр с учётом затрат на реализацию атак и системы защиты с использованием базы данных уязвимостей.

Основные задачи диссертационной работы

Для достижения поставленной цели в диссертационной работе решаются следующие задачи:

1. Разработка алгоритма построения платежной матрицы игры с учетом затрат на реализацию атак и системы защиты.
2. Разработка модели ситуации противоборства собственника и злоумышленника.
3. Разработка практической методики оценки уязвимостей в программном обеспечении организации.
4. Реализация исследовательского прототипа системы оценки уязвимостей в программном обеспечении организации.

Методы исследований

Для решения поставленных задач использовались положения теории вероятностей, математической статистики, теории игр, теории качественных решений.

Основные положения, выносимые на защиту

1. Алгоритм построения ПМ игры с учетом затрат на реализацию атак и системы защиты, использующий для учета риска модернизированную для исследуемой задачи систему CVSS.
2. Модель ситуации противоборства собственника и злоумышленника.
3. Практическая методика оценки уязвимостей в программном обеспечении организации на основе смешанных стратегий теории игр.
4. Исследовательский прототип системы оценки уязвимостей в программном обеспечении организации.

Научная новизна

Научная новизна работы заключается в следующем:

1. Разработан алгоритм построения платежной матрицы игры, в отличие от известных подходов, учитывающий затраты на реализацию атак и системы защиты и использующий модернизированный для исследуемой задачи метод учета риска CVSS. При этом, понятие риска определено как сочетание вероятности опасного события – успешной атаки, и ее последствий – уровня ущерба.

2. Разработана модель ситуации противоборства собственника и злоумышленника, основанная на использовании смешанных стратегий теории игр, в отличие от существующих, позволяющая определить основные этапы оценки уязвимостей в программном обеспечении организации.

3. Разработана практическая методика оценки уязвимостей в программном обеспечении, основанная на использовании инвентаризации программного обеспечения организации, позволяющая определить имеющиеся уязвимости и выявить наиболее опасные из них.

Практическая значимость

Практическая ценность результатов, полученных в диссертации, заключается в разработке:

– методики оценки уязвимостей в программном обеспечении организации, обеспечивающая выявление наиболее опасных угроз в программном обеспечении организации.

– программного обеспечения, выполняющего определение уязвимостей в заданной программном обеспечении организации, выявление наиболее опасных из них и формирование практических рекомендаций по улучшению защищенности информационных систем.

Апробация работы

Основные научные и практические результаты работ докладывались на следующих конференциях:

– Международная научно-практическая конференция «СВЯЗЬ-ПРОМ 2007», проведенная в рамках 4-го Евро-Азиатского международного форума «СВЯЗЬ-ПРОМЭКСПО 2007» (Отмечена золотой медалью, Екатеринбург, май, 2007);

– Международная научно-практическая конференция «СВЯЗЬ-ПРОМ 2008», проведенная в рамках 5-го Евро-Азиатского международного форума «СВЯЗЬ-ПРОМЭКСПО 2008» (Екатеринбург, май, 2008);

– Международная научно-техническая конференция «Инноватика-2008», проведенная Российской Академией Надежности (Сочи, октябрь, 2008);

– Международная научно-практическая конференция «СВЯЗЬ-ПРОМ 2009», проведенная в рамках Евро-Азиатского международного форума «СВЯЗЬ-ПРОМЭКСПО 2009» (Екатеринбург, май, 2009);

– Международная научно-техническая конференция «Инноватика-2009» проведенная Российской Академией Надежности (Сочи, октябрь, 2009);

– а также в ряде научно-технических конференций молодых ученых ГОУ ВПО «УГТУ-УПИ» (Екатеринбург, 2007 – 2009).

Личный вклад автора состоит в выполнении исследований по всем поставленным задачам, в том числе: моделирование ситуации противоборства на основе теории игр со смешанными стратегиями с учетом затрат, определение выражения для элемента платежной матрицы; разработка практической методики оценки уязвимостей в программном обеспечении в компьютерных сетях; разработка алгоритма и программного продукта для поиска наиболее опасных атак; составление рекомендаций участникам игры.

Публикации. По данной теме диссертации опубликовано 10 научных работ, в том числе 2 работы в изданиях, рекомендованных ВАК.

Структура и объем диссертационной работы. Диссертационная работа состоит из введения, 4 глав, заключения, 4 приложений и библиографического списка. Общий объем составляет 125 страниц, 28 таблиц и 20 рисунков.

СОДЕРЖАНИЕ ДИССЕРТАЦИОННОЙ РАБОТЫ

Во введении обоснована актуальность темы диссертационной работы, изложены цели и этапы диссертационной работы, определена научная новизна работы и показана практическая значимость полученных результатов, кратко изложено содержание диссертации.

Первая глава посвящена анализу существующих методов управления ИБ в программных системах. В данной главе приведена современная статистика, свидетельствующая о значительном неблагополучии в сфере обеспечения ИБ в современных программных системах. В ходе изучения было выяснено, что для построения эффективной защиты необходим анализ рисков информационной системы (в том числе анализ возможного ущерба), который является основой при выборе технических подсистем на основании экономического обоснования. Рассмотрен цикл работ для построения системы ИБ, включающий обязательный этап диагностического обследования с оценкой уязвимостей информационной системы, на основе чего производится проектирование системы и ее внедрение. Показано, что в результате ошибок проектирования, реализации и эксплуатации в программных системах возникают уязвимости, то есть свойства системы, использование которых злоумышленником может привести к ущемлению интересов владельца этой системы. Причем многие уязвимости обнаруживаются производителем на этапе разработки, тестирования и сопровождения

продуктов, однако, часть их обнаруживается также независимыми исследователями. Рассмотрены наиболее распространенные инструменты поиска уязвимостей в информационных системах и сервисах. Показано, что целенаправленное применение таких традиционных средств управления безопасностью, как антивирусное программное обеспечение, межсетевые экраны, средства криптографии и др., в значительной мере, предотвращает несанкционированный доступ к информации. Однако, степень их защиты зависит в значительной степени от своевременной установки программных обновлений, выпускаемых разработчиками. В таком случае большую роль играет человеческий фактор. Человек, конечный пользователь, оказывается самым слабым звеном системы ИБ, и злоумышленники, зная это, умело применяют методы социальной инженерии. Сложившаяся ситуация позволила говорить о том, что на сегодняшний день общепринятый подход к управлению обновлениями, как средству превентивной защиты от атак на программные системы, является несовершенным. Отмечено, что для управления безопасностью помимо учета степени опасности уязвимости, возможности успешного проникновения угрозы в информационную среду и ряда других моментов, необходимо учитывать стоимость обеспечения защиты информации. В диссертации предложен прогнозный подход для предотвращения нарушений безопасности в программных системах.

Сделан анализ существующих методов управления защитой информации. На основе этого анализа сделан вывод о том, что все алгоритмы управления, упомянутые в диссертации по-разному, но вполне успешно решают поставленную задачу в рамках, которые предусмотрел их разработчик.

Показано, что данная работа посвящена иному направлению в управлении ИБ, нежели существующие инструменты. Работа направлена на непосредственное устранение самих угроз, а не на создание преграды для угроз ИБ в компьютерных сетях.

Вторая глава посвящена обоснованию подхода к решению задач поставленных в работе.

В начале главы приведено обоснование целесообразности выбора открытой БД об уязвимостях в программном обеспечении. Такие БД содержат подробные сведения об уязвимостях в программном обеспечении, которые позволяют установить способ применения данной уязвимости, уровень ее опасности и последствия ее применения. В конечном счете, выделяются 3 типа последствий уязвимости:

- нарушение доступности (например, отказ в обслуживании),
- нарушение целостности (например, внедрение произвольного кода, подделка счета, нарушение идентификации),
- нарушение конфиденциальности (например, считывание информации).

Каждому виду уязвимости в составе типа назначен уникальный идентификатор в соответствии со стандартом CVE, который позволяет однозначно идентифицировать уязвимость по ее порядковому номеру и исключить возможность появления одной и той же уязвимости под различными идентификаторами в различных БД.

Объем рассматриваемых БД уязвимостей составляет десятки тысяч уязвимостей. Однако только часть из них представляет реальную угрозу безопасности для конкретной программной системы.

Выборка интересующих партнеров игры (атаки и защиты) уязвимостей из БД по определенным направлениям (ожидаемый результат, программное обеспечение и т.д.) дает множество стратегий игроков, включающее наборы из вероятностей выбора m атак и n защит. Задачей атаки/защиты является принятие решения о выборе наборов, обеспечивающих наибольший выигрыш для атаки и наименьший проигрыш для защиты.

Обоснованность применения теории игр для решения задачи противоборства сторон за информационный ресурс, следует из предложения об использовании игровых методов в такой задаче, сделанном Н. Н. Красовским и А. И. Субботиным в монографии «Позиционные дифференциальные игры», изд. «Наука», 1974.

Для дискретного случая упомянутое предложение сводится к использованию платежной матрицы (ПМ), выполненной специальным образом (табл. 1).

Элемент матрицы a_{ij} учитывает соотношение затрат, выделяемых атакующим на атаку и затрат, выделяемых защищающимся на защиту.

ПМ прилагается характер смешанной игры. Это выполняется следующим образом: задаются два множества стратегий $Q_n=\{Q_1,\ldots,Q_N\}$ (защита) и $P_m=\{P_1,\ldots,P_M\}$ (атака). Q_j и P_i суть распределения случайно избираемых номеров в БД $Q_j=\{q_1,\ldots,q_n\}_j$ и $P_i=\{p_1,\ldots,p_m\}_i$. Выбор стратегий далее означает назначение распределений Q_j и P_i.

Таблица 1 – Матрица игры

	1	**2**	**...**	**n**	$\sum_3^i = \sum_{j=1}^{n} q_j a_{ij}$
1	a_{11}	a_{12}	...	a_{1n}	$\sum_3^1$
2	a_{21}	a_{22}	...	a_{2n}	$\sum_3^2$
…	**...**	**...**	**...**	**...**	**...**
m	a_{m1}	a_{m2}	...	a_{mn}	$\sum_3^m$
$\sum_a^j = \sum_{i=1}^{m} p_i a_{ij}$	$\sum_a^1$	$\sum_a^2$	...	$\sum_a^n$	

Рекомендацией для выбора затрат на *j*-ю защиту может служить накопленный опыт, наличие информации о конкретной уязвимости и предположение о том, что защита требует бóльших затрат чем атака. Затраты же на *i*-ю атаку определяются сложностью использования уязвимости.

Проведение информационной разведки злоумышленником часто не дает возможности определить конфигурацию атакуемой системы и выявить ее уязвимые места. Принятие решений в условиях неопределенности, как и в условиях риска, требует определения альтернативных действий, которым соответствуют платежи, зависящие от случайного (неизвестного заранее) выбора соперника.

Таким образом, сделан вывод, что классическая схема игры в данном случае не может применяться, потому что ввиду отсутствия достоверной информации о принятых игроками целях в рассматриваемой задаче не следует доводить игру до конца и выбирать здесь пару «атака и защита» в качестве окончательного решения. Цель игры заключается в получении рекомендации о наиболее вероятных вариантах нападения на конкретную систему. Смешанные стратегии играют роль наиболее удобной формы для числовой оценки конфликтной ситуации.

Метод решения задачи отбора наиболее опасных угроз безопасности (наиболее эффективных атак) использует типичный для игры минимаксный критерий. Подразумевается, что атакующий действует, чтобы максимизировать наименьший ожидаемый выигрыш, а защита старается минимизировать свой максимальный проигрыш.

За наиболее опасные атаки в работе было принято считать, те которые имеют наибольшие значения средних эффективностей, определенных как

$$a_i = \sum\nolimits_a^i = \sum_{j=1}^{n} q_j a_{ij} \,. \tag{1}$$

Аналогичное определение эффективности было дано для защиты

$$b_j = \sum\nolimits_3^j = \sum_{i=1}^{m} p_i a_{ij} \tag{2}$$

с той разницей, что наилучшей защитой будет та, для которой b_j будет минимальна.

Каждый шаг процедуры выбора связан с изменением ПМ и, соответственно, с коррекцией стратегии и новыми значениями p_i и q_j. Коррекция на *k*-ом шаге проводится по формулам, в которых фигурируют результаты *k-1* шага:

$$p_i^k = \frac{a_i^{k-1}}{\sum_{s=1}^{m} a_s^{k-1}} \quad , \quad q_j^k = \frac{b_j^{k-1}}{\sum_{s=1}^{n} b_s^{k-1}} \,. \tag{3}$$

Алгоритм для разработки программного продукта включает следующие этапы:

1. построение матрицы игры при равновероятном выборе атак/защит;
2. присвоение вероятностей выбора атаки/защиты;
3. расчет средних эффективностей;
4. проверка выполнения условия удаления наименее эффективных из атак/защит и принятие решения о продолжении процедуры;
5. удаление наименее эффективных из атак или(и) защит;

Пункты 2 – 5 выполняются до тех пор, пока не выполнится условие останова процедуры минимизации ПМ.

В завершении главы были рассмотрены градации качества решений.

Лицо, принимающее решение (ЛПР) выполняет минимизацию ПМ на основании значений средних эффективностей атаки и защиты. При этом является важным соотношение значений средних эффективностей, так как ЛПР должно стремиться выявить группу наиболее опасных атак близких по средней эффективности и исключить из множества атак те, которые существенно менее эффективны. Исходя из этих соображений в работе используется шкала пропорциональных оценок.

Третья глава работы посвящена применению метода оценки уязвимостей в программном обеспечении и выявления наиболее опасных из них. Общая схема процедуры оценки и отбора наиболее опасных уязвимостей в программном обеспечении приведена на рис. 1.

В первой части главы изложено обоснование выбора БД, используемой при прогнозировании нарушений безопасности, описывается ее структура и, используемая в ней, общая система оценки уязвимости CVSS.

Выбор БД сделан в пользу базы NVD, так как она является наиболее полной, хорошо структурированной и содержит более подробную информацию о каждой уязвимости. Каждая уязвимость в ней имеет эмпирическую базовую оценку уязвимости, полученную по общей системе оценки уязвимости CVSS.

Далее в диссертации описана процедура выборки из общей БД тех уязвимостей, которые угрожают программным системам конкретной организации. Для этого необходимо задать:

1. мотивации атаки и защиты;
2. список программного обеспечения для каждой программной системы организации.

Выборка производится путем сравнения названия и версии программного обеспечения, подверженного определенной уязвимости, с программным обеспечением конкретной организации. Затем каждой уязвимости из полученной выборки защиты назначается значение затрат.

В третьей части главы описано построение игры в ситуации противоборства за информационный ресурс.

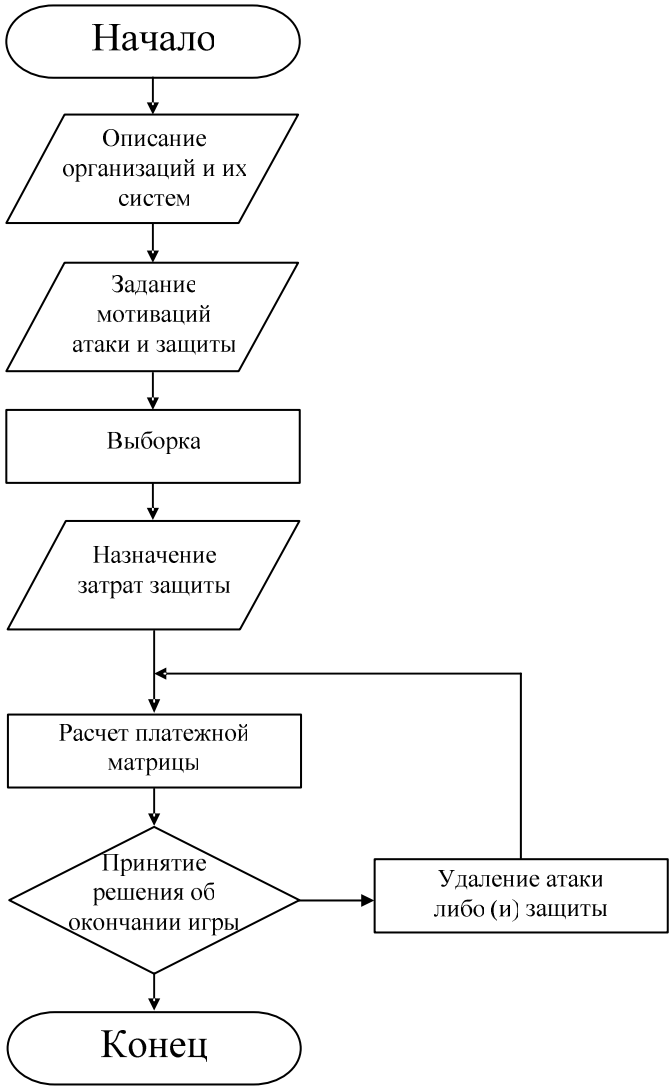

Рисунок 1 – Этапы построения игры атака/защита

Согласно приведенному выше обоснованию подхода к построению ПМ, элемент ПМ должен содержать сведения о выборе решения, как атакой, так и защитой. При совпадении решений *i, j* элемент матрицы a_{ij} равен нулю. В любом случае:

$$a_{ij} = I_i \varphi_{ij} R_i \ , \qquad (4)$$

где R_i – степень распространенности атаки в программных системах организации. Чем больше этот показатель, тем больше вероятность того, что организация подвергнется атаке, использующей определенную уязвимость. Этот показатель соответствует значению *TD* (target distribution) в системе оценки уязвимостей CVSS, который в свою очередь равен отношению количества программных систем, которым угрожает данная уязвимость, к общему числу программных систем в организации; I_i – характеризует влияние уязвимости на целостность, доступность и конфиденциальность системы. Это значение берется из

БД NVD; φ_{ij} – функция затрат на i–ую атаку и на j–ую защиту. Выбор функции $\varphi\left(c_j / c_i\right)$ производится, при следующих логически очевидных ограничениях:

- $\varphi_{ij}=0$ только при $c_j / c_i = 0$,
- $c_i \le c_j$, (5)
- $\varphi_{ij}=1$ только при $c_j = 0$.

При построении φ_{ij} используется экспоненциальная функция затрат, достаточно гибкая и легко согласуемая с ограничением (5):

$$\varphi_{ij} = 1 - e^{-a\frac{c_j}{c_i}}, \quad , \tag{6}$$

где c_j – затраты на j–ю защиту , c_i – затраты на i–ю атаку, a – управляющий множитель ($a>0$). Затраты на j–ю защиту (c_j) назначается ЛПР, а затраты на i–ю атаку (c_i) равны значению параметра Exploitability в БД NVD.

Атака выбирает вариант из множества P_m допустимых распределений $P_m = \{(p)_s\}_{s=1}^{s=M}$ $(p)_s=\{p_1,...,p_m\}$, чтобы максимизировать наименьший ожидаемый средний выигрыш:

$$\max_{P_m}\left\{\min\left(\sum_{i=1}^{m} a_{i1}p_i, \sum_{i=1}^{m} a_{i2}p_i, ..., \sum_{i=1}^{m} a_{in}p_i\right)\right\}. \tag{7}$$

Защита выбирает стратегию из множества Q_n допустимых распределений $Q_n = \{(q)_r\}_{r=1}^{r=N}$ $(q)_r=\{q_1,...,q_n\}$, чтобы минимизировать наибольший ожидаемый средний проигрыш:

$$\min_{Q_n}\left\{\max\left(\sum_{j=1}^{n} a_{1j}q_j, \sum_{j=1}^{n} a_{2j}q_j, ..., \sum_{j=1}^{n} a_{mj}q_j\right)\right\}. \tag{8}$$

Минимаксный ожидаемый проигрыш защиты больше или равен максиминного ожидаемого выигрыша атаки. В случае их равенства стратегия именуется оптимальной.

В качестве критерия останова избрано такое состояние процесса, когда наибольшее возможное уменьшение средних эффективностей $\sum_a^j = \sum_{i=1}^{m} p_i a_{ij}$ $\sum_3^i = \sum_{j=1}^{n} q_j a_{ij}$ становится меньше задаваемых ограничений:

$$\left|\sum_{j=1}^{n} q_j a_{ij} - \sum_{j=1}^{n} q_j a_{rj}\right| \le \varepsilon_1 \text{ при всех } i=\overline{1,m} \text{ и } r=\overline{1,m}, \tag{9}$$

$$\left|\sum_{i=1}^{m} p_i a_{ij} - \sum_{i=1}^{m} p_i a_{ir}\right| \le \varepsilon_2 \text{ при всех } j=\overline{1,n} \text{ и } r=\overline{1,n}. \tag{10}$$

Оставшиеся варианты считаются искомым решением игры.

В четвертой части главы был рассмотрен пример прогнозирования нарушений безопасности в информационной системе.

Четвертая глава посвящена особенностям практического применения результатов диссертационной работы и разработке программы «Vulnerability Analyzer».

Первая часть главы описывает программную реализацию разработанного метода оценки уязвимостей. Общая последовательность процедурных групп процесса выявления наиболее опасных уязвимостей показана на рис. 1.

В начале главы изложен вопрос импорта данных из БД NVD, при этом происходит преобразование исходной структуры данных к удобному для использования виду. Исходная БД NVD преобразуется в 3 таблицы. В одной таблице хранится описание уязвимости, во второй – описание программного обеспечения, третья таблица описывает связь между уязвимостью и программным обеспечением.

Таблица, описывающая уязвимости демонстрируется на примере в таблице 2:

Таблица 2 – Таблица уязвимостей

cve_id	**published**	**impact**	**Exploitability**	**access**	**conf**	**avail**	**int**	**descr**
CVE-2008-0073	24.03.2008	6,4	8,6	Network (сетевой)	True (Истина)	True (Истина)	True (Истина)	Array index error in the sdpplin_parse function in input/libreal/sdpplin.c in xine-lib 1.1.10.1 allows remote RTSP servers to execute arbitrary code via a large streamed SDP parameter (Ошибка индекса массива в функции sdpplin_parse в файле input/libreal/sdpplin.c в библиотеке xine-lib 1.1.10.1 позволяет удаленному серверу RSTP выполнить произвольный код через большие передаваемые SDP параметры)

Ниже приведено описание каждого поля таблицы 2:

1. cve_id – в этом поле содержится идентификатор уязвимости;

2. published – дата публикации;

3. impact – оценка влияния уязвимости на целостность, доступность и конфиденциальность системы.

4. exploitability – характеризует сложность использования уязвимости.

5. access – определяет тип доступа (локальный или сетевой), необходимый для использования уязвимости;

6. conf, avail, int – показывают может ли использоваться данная уязвимость для нарушения конфиденциальности, доступности и целостности; соответственно, таблица используется для разбиения уязвимости на категории согласно мотивации атакующей стороны.

7. descr – в этом поле приведено описание уязвимости;

Далее описан процесс построения выборки, максимально соответствующей особенностям защищаемой инфраструктуры. Основу такой выборки должен составлять перечень уязвимого программного обеспечения, используемого в данной программной системе. Для решения задачи выявления уязвимостей в программных системах в диссертационной работе предложен подход на основании инвентаризации инфраструктуры организации и сопоставления полученных результатов с данными об уязвимом программном обеспечении из БД NVD.

Затем приведена блок-схема алгоритма процедуры построения ПМ игры.

Во второй части главы приведены результаты внедрения программного продукта, «Vulnerability Analyzer», реализующего на практике разработанную методику прогнозирования нарушений безопасности в программных системах.

Внедрение проводилось в компании ЗАО «Форатек Коммуникейшн», являющейся региональным оператором связи.

Доступ работников компании в Интернет осуществляется через маршрутизатор Cisco 2691, посредством трансляции сетевых адресов (NAT). Тот же маршрутизатор выполняет ограничение доступа работников компании в Интернет и доступа из внешней сети в локальную сеть посредством DMZ, ACL и CBAC. Для доступа работников компании из внешней сети в локальную сеть используется ISA-сервер. На всех рабочих станциях установлены антивирусные средства с регулярно обновляемыми базами. Производится регулярное обновление системного программного обеспечения.

При определении мотиваций учитывались следующие факторы:

- так как к серверам не было прямого доступа, локальные атаки не рассматривались,
- так как компания является оператором связи, она имеет службы, для которых в совокупности являются критичными потери конфиденциальности, доступности и целостности.

После проведения инвентаризации с помощью разработанной приклад-

ной программы «Vulnerability Analyzer» было выявлено 7 уязвимостей.

При определении затрат защиты учитывались:

- стоимость трафика потраченного на загрузку обновления,
- оплата рабочего время затраченного работником на загрузку обновления и его установку.

В результате процедуры минимизации полученной ПМ, число прогнозируемых атак было сокращено до 3.

В результате внедрения системы прогнозирования инцидентов в ЗАО «Форатек Коммуникейшн», были выявлены возможные точки проникновения, содержащие уязвимости. С помощью метода, предложенного в диссертационной работе, были определены наиболее опасные из них. Использование их злоумышленником, могло бы привести к утечке конфиденциальной информации, недоступности каких-либо сервисов либо к получению контроля над компьютером. Были даны рекомендации, позволяющие локализовать выявленные уязвимости.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ И ВЫВОДЫ

Основные результаты работы заключаются в следующем:

1. Предложен способ построения платежной матрицы игры, при этом для учета риска использовалась система CVSS, модернизированная для исследуемой задачи. Понятие риска определено как сочетание вероятности опасного события – успешной атаки, и ее последствий – уровня ущерба. При расчете элемента платежной матрицы игры учитываются затраты в форме отношения расходов средств участниками игры.
2. Разработана модель ситуации противоборства собственника и злоумышленника на основе смешанных стратегий теории игр, позволяющая определить основные этапы оценки уязвимостей в программном обеспечении организации.
3. Разработана практическая методика оценки уязвимостей в программном обеспечении организации на основе смешанных стратегий теории игр.
4. Разработан исследовательский прототип системы оценки уязвимостей в программном обеспечении организации, позволяющий администратору информационной безопасности обнаружить известные уязвимости в защищаемой инфраструктуре, и с учетом предопределенной мотивации злоумышленника указать те из них, на которые защита должна обратить внимание в первую очередь.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

В рецензируемых журналах из списка ВАК

1. Качественные решения при выборе атаки/защиты информационного ресурса / А. И. Захаров, Э. А. Лидский, У. А. Михалева // Надежность. – 2005. – №3 (14). С. 12–20.

2. Оптимизация маршрута в ячеистых сетях связи / Э. А. Лидский, У. А. Михалева // Телекоммуникации. 2009. – №10. С.10–14.

В других изданиях

3. Неполнодоступная нагрузочная схема в системах связи / Э. А. Лидский, У. А. Михалева // Научные труды VIII отчетной конференции молодых ученых ГОУ ВПО УГТУ – УПИ. – Екатеринбург: УГТУ – УПИ, 2005. С. 285–286.

4. Применение линейного программирования в задаче построения сети / Э. А. Лидский, У. А. Михалева // Научные труды международной научно-практической конференции «СВЯЗЬ-ПРОМ 2005» в рамках 2-го Евро-Азиатского форума «СВЯЗЬ-ПРОМЭКСПО 2005». – Екатеринбург: ЗАО «Компания Реал-Медиа», 2005. С. 114–117.

5. Алгоритм построения неполнодоступной нагрузочной схемы со сдвигом на шаг / Э. А. Лидский, У. А. Михалева // Научные труды международной научно-практической конференции «СВЯЗЬ-ПРОМ 2005» в рамках 2-го Евро-Азиатского форума «СВЯЗЬ-ПРОМЭКСПО 2005». – Екатеринбург: ЗАО «Компания Реал-Медиа», 2005. С. 146–147.

6. Качественные решения в задачах информационной безопасности, (золотая медаль форума) / А. И. Захаров, Э. А. Лидский, У. А. Михалева // Научные труды международной научно-практической конференции «СВЯЗЬ-ПРОМ 2007» в рамках 4-го Евро-Азиатского форума «СВЯЗЬ-ПРОМЭКСПО 2007». – Екатеринбург: ЗАО «Компания Реал-Медиа», 2007. С. 225–229.

7. Учет затрат на атаку и защиту в конфликтной ситуации / Э. А. Лидский, У. А. Михалева // Научные труды международной научно-практической конференции «СВЯЗЬ-ПРОМ 2008» в рамках 5-го Евро-Азиатского форума «СВЯЗЬ-ПРОМЭКСПО 2008». – Екатеринбург: ЗАО «Компания Реал-Медиа», 2008. С. 439–440.

8. Учет затрат в сети безопасности / Э. А. Лидский, У. А. Михалева // Системные проблемы надежности, качества, информационно-телекоммуникационных и электронных технологий в управлении инновационными проектами (Инноватика – 2008): материалы Международной конференции и Российской научной школы. – М.: Энергоатомиздат, 2008. С. 71–72.

9. Прогноз нарушений безопасности в информационных системах / Э. А. Лидский, У. А. Михалева // Научные труды международной научно-практической конференции «СВЯЗЬ-ПРОМ 2009» в рамках 6-го Евро-Азиатского форума «СВЯЗЬ-ПРОМЭКСПО 2009». – Екатеринбург: УрТИСИ ГОУ ВПО «СибГУТИ», 2009. С. 372–374.

10. Выбор маршрута по критерию минимума затрат в ячеистой сети / Э. А. Лидский, У. А. Михалева // Системные проблемы надежности, качества, информационно-телекоммуникационных и электронных технологий в управлении инновационными проектами (Инноватика-2009): материалы Международной конференции и Российской научной школы. – М.: Энергоатомиздат, 2009. С. 65–66.

Диссертант У. А. Михалева

МИХАЛЕВА Ульяна Анатольевна

ОЦЕНКА УЯЗВИМОСТЕЙ В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ ОРГАНИЗАЦИИ НА ОСНОВЕ СМЕШАННЫХ СТРАТЕГИЙ ТЕОРИИ ИГР

Специальность: 05.13.19 – Методы и системы защиты информации, информационная безопасность

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

Подписано в печать 06.05.2010 Формат 60x84 1/16.
Бумага типографская. Плоская печать. Усл. печ.л. 7,0
Уч.-изд.л.0,5.Тираж 100 экз. Заказ №___

Редакционно-издательский отдел УГТУ-УПИ,
620002, Екатеринбург, Мира, 19
Ризография НИЧ УГТУ-УПИ
620002, Екатеринбург, Мира, 19