Иван Андреевич Трещев
Антон Александрович Воробьев

Методы и модели защиты информации

Часть 1. Моделироваание и оценка

Антон Александрович Воробьев
Иван Андреевич Трещев

Методы и модели защиты информации. Часть 1. Моделироваание и оценка

http://www.litres.ru/pages/biblio_book/?art=55731541
ISBN 9785449893451

Аннотация

В книге рассмотрены вопросы моделирования и обеспечения защиты информации при наличии программно-аппаратных уязвимостей. Проведен анализ зарубежных банков данных уязвимостей

Содержание

Методы и модели защиты информации Часть 1. Моделироваание и оценка

Иван Андреевич Трещев
Антон Александрович Воробьев

Общий анализ Анастасия Сергеевна Ватолина

© Иван Андреевич Трещев, 2020
© Антон Александрович Воробьев, 2020

ISBN 978-5-4498-9345-1 (т. 1)
ISBN 978-5-4498-9346-8
Создано в интеллектуальной издательской системе Ridero

Список сокращений

CCE – Common Configuration Enumeration;

CERT – Computer Emergency Response Team;

CPE – Common Program Enumeration;

CVE – Common Vulnerability Enumeration;

CVSS – Common Vulnerabilities Scoring System;

HTML – Hyper—Text Markup Language;

NVD – National Vulnerability Database;

OVAL – Open Vulnerability Assessment Language;

SCAP – Security Content Automation Protocol;

XCCDF – The Extensible Configuration Checklist Description Format;

XML – extensible markup language;

XSD – XML Schema Definition;

АИС – автоматизированная информационная система;

АРМ – автоматизированное рабочее место;

БД – база данных;

ВС – вычислительная система;

ГНИИИ ПТЗИ ФСТЭК России – Государственный научно—исследовательский испытательной институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю России;

ГОСИБ – глобальные открытые сети информационного обмена;

ИС – информационная система;

ИСПДн – информационная система персональных данных;

КИ – конфиденциальная информация;

КНПИ – канал несанкционированной передачи информации;

КС – корпоративная сеть;

ЛВС – локальная вычислительная сеть;

МЭ – межсетевой экран;

НМД – нормативно—методическая документация;

НСД – несанкционированный доступ;

ОРД – организационно—распорядительная документация;

ПДн = персональные данные;

СД – сервер доступа;

СЗИ – система защиты информации;

СКЗИ – средства криптографической защиты информации;

СКО – среднеквадратичное отклонение;

СОВ – система обнаружения вторжений;

СУБД – система управления базами данных;

ФСБ – Федеральная служба безопасности;

ФСТЭК – Федеральная служба по техническому и экспортному контролю;

ЭДО – электронный документооборот.

Список обозначений

$\#\Psi$ – мощность множества Ψ;

$\{X_i\}$ – конечное семейство классов характеристик уязвимостей;

2^X – множество всех подмножеств множества X;

G – пространство декартового произведения множеств всех подмножеств семейства характеристик $\{X_i\}$;

M – функционал $G \to [0; \alpha] \in R$, α – const;

B – булева алгебра с носителем элементов G;

$\mu(x)$ – вещественная счетно—аддитивная существо положительная функция, заданная на алгебре B;

$\mu_N(x)$ – нормированное значение функции $\mu(x)$;

Введение

Актуальность работы.

Защита информационных ресурсов от угроз безопасности на сегодня является одним из приоритетных направлений, как отдельного предприятия, так и государства в целом.

На сегодня регулирование деятельности по защите информации на автоматизированных объектах информатизации в Российской Федерации осуществляет Федеральная служба по техническому и экспортному контролю России(ФСТЭК) при поддержке ГНИИИ ПТЗИ ФСТЭК России, которая разработала ряд руководящих(РД) и нормативных документов(НД). Среди последних, основополагающими являются документы о базовой модели угроз информационных систем персональных данных (ИСПДн) и ключевых систем информационной структуры (правительственные объекты и объекты, непосредственно влияющие на обороноспособность государства). В соответствии с РД и НД, частным случаем угрозы является понятие уязвимости, применяемое к информационным системам (ИС), – «свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации» или «некая слабость, которую можно использовать для на-

рушения системы или содержащейся в ней информации».

Однако разработанные методы, модели оценки и контроля защищенности ИС при наличии программно-аппаратных уязвимостей относятся непосредственно к системам защиты информации, созданных как элемент частной модели угроз определенных предприятий на основе базовой модели с использованием методик ГНИИИ ПТЗИ ФСТЭК России, причем отсутствие численных критериев их оценки затрудняет или делает невозможным проведение контроля и аудита защищенности ИС. Проблема отсутствия данных критериев описана в РД и НД регуляторов, и заявлена как исследовательская. Для ее решения ФСТЭК России рекомендует систематизировать уязвимости на основе существующих зарубежных баз данных(БД), используя их в качестве источников информации. Наиболее распространенной базой данных об уязвимостях является БД National Vulnerability Database(NVD), основанная на объединении информации из ранее созданных баз данных (CPE – Common Platform Enumeration, CVE – Common Vulnerabilities and Exposures, и др.)

Целью является разработка математических методов и моделей с количественными критериями численной оценки защищенности вычислительных систем при наличии программно—аппаратных уязвимостей с использованием ис-

точника данных (NVD).

В ходе достижения цели решены следующие задачи:

Создана математическая модель для исследования характеристик программно-аппаратных уязвимостей с учетом специфики классификации базы данных (БД) NVD;

Сформирована математическая модель оценки защищенности автоматизированного рабочего места (АРМ);

Разработаны методы и количественные критерии численной оценки защищенности АРМ;

Развита математическая модель оценки защищенности вычислительной системы как совокупности АРМ;

Разработаны методы и количественные критерии численной оценки защищенности вычислительных систем;

Предложена методика расчета нормированных значений критериев численной оценки защищенности АРМ и ВС.

Основные **методы исследования** базируются на математическом аппарате булевых алгебр, теории вероятностей и математической статистики, теории случайных процессов, теории меры, теории графов и имитационном моделировании. Для последнего использована среда VMWare ESXi 5.1 с VMWare Converter 5.1 для виртуализации вычислительных систем. Сбор информации об уязвимостях осуществлялся референсной утилитой языка OVAL – OVALDI 5.10.1.5.

Численная обработка данных производилась в среде программирования MS Visual Studio 2010 SP3(C# .NET 4.5) с использованием MS SQL Server 2012 в качестве СУБД.

Достоверность полученных в диссертации результатов подтверждается: строгим математическим доказательством всех предложений и теорем, представленных в работе, результатами расчетов предлагаемых количественных критериев численной оценки защищенности для вычислительной подсети.

Предметом исследования являются математические модели и методы оценки защищенности вычислительных систем при наличии программно—аппаратных уязвимостей.

Объектом исследования являются программно-аппаратные уязвимости в вычислительных системах.

Научная новизна работы:

Разработана математическая модель для исследования характеристик программно-аппаратных уязвимостей на базе классификаций с использованием источника данных NVD;

Сформированы математические модели оценки защищенности автоматизированного рабочего места и вычислительных систем при исследовании характеристик программно-аппаратных уязвимостей;

Доказано, что предлагаемая математическая модель оценки защищенности АРМ является булевой алгеброй B, на которой введена счетная, аддитивная и существенно положительная вещественная функция μ (x), являющаяся мерой;

Показано, что предложенная булева алгебра B является алгеброй событий, где аналогом значения вероятности является значение нормированной меры μ_N (x);

Введена характеристика в виде критерия «степень уязвимости» для автоматизированного рабочего места, и получен его количественный эквивалент как осредненная степень уязвимости;

Разработана математическая модель защищенности вычислительной системы, и критерий оценки ее защищенности по корреляционному признаку;

Разработана вспомогательная математическая модель для подготовки к расчетам численных нормированных значений количественных критериев оценки защищенности автоматизированного рабочего места и вычислительной системы предприятия;

Предложен метод снижения критерия защищенности ВС на основе метода ветвей и границ и двоичного поиска.

Научная и практическая значимость работы:

Основные результаты диссертационной работы были получены автором при проведении исследований, выполнявшихся в 2010 – 2013 гг, в том числе при поддержке

НИОКР Министерства образования и науки РФ №10—11/2723 от 21.12.2012 «Проектирование электронной системы университета и разработка модуля «Мониторинг деятельности подразделений ВУЗа», темы НИР «Разработка и исследование математических моделей атак на локальные вычислительные сети» В/Б-010/12, темы НИР «Исследование создания автономного источника питания на основе перепада температур для измерительной аппаратуры» В/Б-004/13.

Практическая ценность результатов, полученных в диссертации, заключается в разработке численных критериев оценки защищенности автоматизированных рабочих мест и вычислительных систем совместно с методикой расчета их нормированных значений.

Предложенная математическая модель и методика для исследования характеристик программно-аппаратных уязвимостей может быть полезна широкому кругу экспертов и исследователей при решении задач различных областей.

Апробация работы.

Основные результаты работы обсуждались на 12—м конкурсе—конференции студентов и аспирантов по информационной безопасности «SIBINFO—2012» в институте системной интеграции и безопасности ТУСУР г. Томск, где автор занял третье место среди аспирантских работ; XIII Всероссийской научно—практической конференции «Пробле-

мы информационной безопасности государства, общества и личности» г. Новосибирск в результате которой был опубликован доклад в журнале «Доклады ТУСУРа» г. Томск; конкурсе на лучшую научно-исследовательскую работу аспиранта и молодого ученого «КнАГТУ», г. Комсомольск-на-Амуре; Открытом Дальневосточном конкурсе программных средств студентов, аспирантов и специалистов «Программиист-2009», г. Владивосток; Открытом Дальневосточном конкурсе программных средств студентов, аспирантов и специалистов «Программиист-2010», г. Владивосток; Сорок второй конференции «Научно-техническое творчество аспирантов и студентов» ФГБОУ ВПО «КнАГТУ», г. Комсомольск-на-Амуре; заседаниях кафедры «Информационная безопасность автоматизированных систем» ФГБОУ ВПО «КнАГТУ».

Публикации:

1. Воробьев А. А. Визуализация процессов работы алгоритмов шифрования с дополнением преобразования сферой Римана // Открытый Дальневосточный конкурс программных средств студентов, аспирантов и специалистов «Программист—2010». Владивосток: Дальневосточный Государственный Университет. 2010. С. 7—9.

2. Воробьев А. А., Коньшин А. В. Программно—аппаратный комплекс защиты персональных данных // Открытый Дальневосточный конкурс программных средств сту-

дентов, аспирантов и специалистов «Программист—2010». Сборник докладов. Владивосток: Дальневосточный Государственный Университет. 2010. С. 42—44.

3. Воробьев А. А., Котляров В. П. О проблеме взлома перебором и потенциальных решениях с помощью сферы Римана и варьирования запятой // Научная сессия ТУСУР—2010. Томск. 2010. Т. 3. С. 230—235.

4. Воробьев А. А., Котляров В. П. О решениях повышения криптостойкости шифров с помощью континуального множества. Ученые записки Комсомольского—на—Амуре государственного технического университета изд. Комсомольского—на—Амуре государственного технического университета, 2010 № II—1 (2), серия «Науки о природе и технике», ISSN 2076—4359, с. 58—64.

5. Воробьев А.А, Трещев И. А., Григорьев Я. Ю. Подход к распределению ролей при проектировании информационной системы «Электронный университет» ФГБОУ ВПО КнАГТУ // Научный электронный архив. URL:http://econf.rae.ru/article/7794 (дата обращения: 06.10.2013).

6. Воробьев А.А, Трещев И. А., Середнев А. А. Практические аспекты развертывания виртуальной инфраструктуры организации для обеспечения коллективной работы пользователей ФГБОУ ВПО КнАГТУ // Научный электронный архив. URL:http://econf.rae.ru/article/7793 (дата обращения: 06.10.2013).

В ведущих рецензируемых журналах, рекомендуе-

мых ВАК:

7. Воробьев А. А. «Алгебраические методы исследования таксономий уязвимостей вычислительных сетей и компьютерных систем» Доклады ТУСУРа, Т. 1 (25), № часть 2, 2012. С. 12—15.

8. Воробьев А. А. «Исследование криптостойкости модификации шифра гаммирования по операции XOR при использовании континуального множества». Ученые записки Комсомольского—на—Амуре государственного технического университета изд. Комсомольского—на—Амуре государственного технического университета, 2012 № IV—1 (12), серия «Науки о природе и технике», ISSN 2076—4359, с. 36—44.

9. Воробьев А. А., Григорьев Я. Ю., Трещев И. А., «Система защиты конфиденциальной информации для высших учебных заведений «Электронный университет» // Интернет-журнал «Науковедение». 2013 №1 (14) [Электронный ресурс]. – М. 2013. – Режим доступа: http://naukovedenie.ru/PDF/44tvn113.pdf, свободный – Загл. с экрана.

10. Воробьев А. А., «Моделирование и оценка системы защиты конфиденциальной информации для высших учебных заведений» // Интернет-журнал «Науковедение». 2013 №5 (18) [Электронный ресурс]. – М. 2013. – Режим доступа: http://naukovedenie.ru/PDF/34tvn513.pdf, свободный – Загл. с экрана.

11. Воробьев А. А., «Анализ уязвимостей вычисли-

тельных систем на основе алгебраических структур и потоков данных National Vulnerability Database» // Интернет-журнал «Науковедение». 2013 №5 (18) [Электронный ресурс]. – М. 2013. – Режим доступа: http://naukovedenie.ru/PDF/33tvn513.pdf, свободный – Загл. с экрана.

Структура и объем работы

Диссертационная работа состоит из введения, четырех глав, заключения, списка цитируемой литературы и приложений. Работа изложена на 131 странице основного текста, содержит 11 рисунков и 10 таблиц, 106 наименований библиографических источников.

Автор выражает искреннюю благодарность своему руководителю кандидату технических наук, профессору Котлярову В. П., заместителю декана Факультета Компьютерных Технологий, кандидату физико-математических наук, доценту Григорьеву Я. Ю., заведующему кафедрой «Информационная безопасность автоматизированных систем», кандидату технических наук, Трещеву И. А. и профессору кафедры «Информационная безопасность автоматизированных систем», доктору технических наук, Челухину В. А. за внимание к работе.

Основные положения, выносимые на защиту:

· Математическая модель для исследования программно-аппаратных уязвимостей, основанная на аппарате буле-

вых алгебр, позволяющая описывать их закономерности;

· Математическая модель оценки защищенности автоматизированного рабочего места, предоставляющая численный критерий оценки защищенности АРМ при наличии программно—аппаратных уязвимостей и методику расчета его нормируемого значения;

· Математическая модель оценки защищенности вычислительной системы, предоставляющая численный критерий оценки ее защищенности при наличии программно—аппаратных уязвимостей и методику расчета нормируемого значения для предприятий.

Основное содержание работы.

Во введении обосновывается актуальность темы, характеризуются научная новизна и методы исследования, формулируются выносящиеся на защиту положения, цели и задачи диссертационного исследования.

В первой главе производится исследование существующих классификаций, таксономий уязвимостей, описываемых в хронологическом порядке совместно с их анализом, в частности классификация уязвимостей базовой модели угроз ИСПДн ФСТЭК России. Также рассматриваются существующие математические модели защиты информации, основной недостаток которых заключается в тесной связи с конкретными прикладными задачами.

Во второй главе предложена математическая модель

для описания классификаций уязвимостей на основе концепции измерений, разработка которой обуславливается тем, что классификации уязвимостей ФСТЭК России, комбинированные древовидные классификации Бишопа, Хэнсмэна, и т. д. легко преобразуются в классификации на основе концепции измерений путем переноса листьев дерева на оси измерений, причем последние образуются вершинами дерева с высотой, равной одному.

С целью построения математического аппарата исследования уязвимостей вычислительных систем с классификацией на основе концепции измерений, решается задача о представлении уязвимостей в виде точек некоторого многомерного пространства, где в качестве основного инструмента применена теория булевых алгебр.

На основе данной математической модели предлагается математическая модель оценки защищенности от утечек информации при наличии программно-аппаратных уязвимостей для автоматизированного рабочего места совместно с количественным критерием численной оценки защищенности АРМ

В третьей главе рассматривается дополнительная модель вычислительной сети информационной системы типового предприятия, выделяющая пять типов рабочих мест, на которых обрабатывается конфиденциальная информация:

· Имеющие подключение к информационной системе

(ИС) организации, но не имеющие подключения к глобальным открытым сетям информационного обмена (ГОСИБ).

· Имеющие подключение к ГОСИБ, но не имеющие подключения к ИС организации.

· Имеющие подключение как к ГОСИБ, так и к ИС организации.

· Не имеющие подключения к ИС организации и к ГОСИБ.

· Удаленные рабочие места в ГОСИБ.

На ее базе разрабатывается математическая модель в виде ориентированного, взвешенного, раскрашенного мультиграфа.

На основе существующей вычислительной системе предприятия, с учетом требований к решаемым предприятием задач, возможно построить необходимую модель вычислительной системы в защищенном исполнении, на базе которой вычисляются нормированные значения критериев защищенности предприятия. На практике, задача определения нормируемых значений предлагаемых критериев оценки защищенности, решается специалистом по защите информации, и для ее решения на определенном предприятии, предлагается вспомогательная математическая модель, с помощью которой производится преобразование существующей вычислительной системы к модели системы в защищенном исполнении.

Критерии оценки защищенности АРМ недостаточны для

обеспечения контроля защищенности вычислительной системы. Обнаружение и устранение уязвимостей, в общем случае, является процессом случайным, который имеет большие отклонения с течением времени от своего математического ожидания. Тем самым, для рассмотрения оценки защищенности ВС, производится переход в область случайных процессов, и предлагается математическая модель уязвимостей вычислительной системы на основе теории случайных процессов совместно с интегральным критерием численной оценки защищенности от программно—аппаратных уязвимостей по корреляционному признаку.

В четвертой главе представлен состав экспериментального стенда и произведен анализ вычислительной подсистемы лабораторий факультета компьютерных технологий Федерального Государственного Бюджетного Образовательного Учреждения «Комсомольский—на—Амуре Государственный Технический Университет» на наличие программно—аппаратных уязвимостей, получены численные значения количественных критериев оценки защищенности (в том числе нормированные), и даны рекомендации по их устранению.

В заключении приведены основные результаты, полученные в диссертационной работе.

В приложении приводятся доказательства некоторых вторичных утверждений.

1 Анализ классификаций и математических методов описания уязвимостей

1.1 Постановка задачи

В области информационной безопасности под уязвимостью понимается недостаток в вычислительной системе, используя который возможно нарушить ее целостность и вызвать некорректную работу.

Попытка реализации уязвимости называется атакой.

Цель данной главы – проведение обзора способов классификаций и математических моделей систем защиты информации от утечки информации.

Для достижения поставленной цели, необходимо провести обзор:

· и анализ классификаций уязвимостей автоматизированных систем;

· базы данных уязвимостей NVD (National Vulnerability Database) и ее компонент;

· множества протоколов SCAP (Security Content Automation Protocol) как средства управления уязвимостями базы данных NVD, и языка Open Vulnerability Assessment

Language как справочной реализации подмножества SCAP;
· математических моделей систем защиты информации.

1.2 Классификации уязвимостей автоматизированных систем

С целью изучения и анализа уязвимостей, а также способов их реализации в автоматизированных системах, исследователи предлагают различные виды классификации уязвимостей и их реализаций. Формально, задача классификации состоит в создании системы категорирования, а именно, – в выделении категорий и создании классификационной схемы, как способа отнесения элемента классификации к категории.

При использовании заданной терминологии, неизбежно возникают разночтения между понятиями классификация и классификационная схема. Для устранения данного недостатка, в дальнейшем, используется термин «таксономия». Данный термин имеет греческое происхождение: от слов taxis – порядок и nomos – закон.

Таксономия – это «классификационная схема, которая разделяет совокупность знаний и определяет взаимосвязь частей». Ярким примером таксономий является таксономия растений и животных Карла Линнея.

В области защиты информации выделяют три группы таксономий:

– Таксономии атак,,,,,.

– Таксономии уязвимостей,,.

– Таксономии инцидентов.

К проблеме классификации атак имеется несколько подходов. Классически атаки разделяют на категории в зависимости от производимого эффекта, :

– нарушение конфиденциальности информации;

– нарушение целостности информации;

– отказ в обслуживании (нарушение доступности информации).

Главным недостатком подобной классификации является слабая информативность (а, следовательно, и применимость), так как по информации о классе атаки практически невозможно получить информацию об ее особенностях. Однако, эффект атаки является важным ее свойством и данный параметр в том или ином виде применяется в ряде таксономий (,,).

Другим подходом к классификации является классификация уязвимостей аппаратного и программного обеспечения информационно—вычислительных и телекоммуникационных систем. Одним из первых исследований в этом направлении является работа Атанасио, Маркштейна и Филлипса. Частично деление по типу уязвимости было использовано Ховардом и Лонгстаффом. Далее этот подход получил продолжение, которое в результате предлагает исследователям достаточно подробную классификация уязвимостей. Однако данный подход является слишком узким и зачастую не отражает в должной мере специфику атаки, поэтому применяет-

ся, в основном, лишь для специальных классов задач (при тестировании программного обеспечения и др.).

Другим возможным вариантом классификации является деление на основе начального доступа, которым обладает атакующий. Примером подобного подхода является матрица Андерсона. В своей работе Джеймс Андерсон (James P. Anderson) предложил основу классификации как наличие или отсутствие возможности доступа, атакующего к вычислительной системе (ВС) или к ее компонентам. Таким образом, категория, к которой принадлежит атака, зависит от начальных привилегий атакующего. Таксономия Андерсона предлагает матрицу 2 на 2.

Из приведенной таблицы (таблица 1) можно сделать заключение, что все атаки разделяются на три категории. Ситуация, когда атакующий имеет право запуска или использования программы в отсутствии доступа к вычислительной системе, – невозможен.

Таблица 1 – Матрица таксономии Андерсона

	Атакующий не имеет право запуска /использования программы /информации	Атакующий имеет право запуска/использования программы/информации
Атакующий не имеет доступ к ВС	Категория А Внешнее вторжение	–
Атакующий имеет доступ к ВС	Категория В Внутреннее вторжение	Категория С Злоупотребление полномочиями

Категория В подразделяется Андерсоном дополнительно на три подкатегории. Следовательно, полный список категорий атак имеет следующий вид:

– Внешнее вторжение
– Внутреннее вторжение
– Masquerader – ложный пользователь.
– Legitimate user – легальный пользователь.
– Clandestine user – скрытый пользователь.
– Злоупотребление полномочиями.

Главным отличием между ложным, легальным и скрытым пользователями заключается в том, что ложный пользователь маскируется под легального пользователя, и, с точки зрения вычислительной системы, неотличим от него. Скрытый пользователь ориентируется на работу с вычислительной системой, при которой он остается незамеченным для систем обнаружения вторжений.

Рассматривая развитие классификационных подходов во времени, можно заметить, что ряд исследователей стара-

лись абстрагироваться от свойств состава атак, с целью создания общего списка типов атак. Наиболее известны в данном направлении работы Ноймана и Паркера,,,. Аналогичную цель преследовал в своей работе Саймоном Хансмэном. Важным достоинством данного подхода является прикладная составляющая, так как в большинстве случаев информация о специфики атаки дает существенно больше, нежели знание каких—либо ее свойств. Однако недостатком данного подхода является наличие сильно пересекающихся категорий атак, а полнота классов зачастую недостижима.

В своей работе, П. Нойман и Д. Паркер представили 9 категорий способов вторжений (табл. 2).

Таблица 2 – Категории способов вторжения

№	***Категория способа вторжения***
1	Внешнее вторжение
2	Аппаратное вторжение
3	Маскируемые вторжения
4	Вредоносные программы
5	Обход механизмов безопасности
6	Активное злоупотребление
7	Пассивное злоупотребление
8	Неактивное злоупотребление
9	Косвенное злоупотребление

На основе данных категорий П. Нойман разработал 26 видов атак (табл. 3)

Таблица 3 – Виды атак

Категория/Вил атаки	Описание
Внешнее вторжение	
Визуальное наблюдение	Наблюдение за монитором или клавиатурой (визуальный канал утечки информации)
Обман	Обман пользователей и администраторов
Извлечение мусора	Извлечение информации из виртуальных корзин
Аппаратное вторжение	
Восстановление	Извлечение информации с выброшенных/украденных носителей
Прослушивание	Перехват данных по техническим каналам
Вмешательство	
Физическая атака	Разрушение или повреждение оборудования, источников питания
Физическое удаление	Изъятие оборудования и хранилищ данных
Маскируемые вторжения	
Имитирование	Использование ложных идентификаторов
Скрытый захват линий связи или хостов	
Атаки с подменой параметров	
Запутывание сетей	Маскировка физического месторасположения или маршрута
Вредоносные программы	
Троянские кони	Внедрение вредоносного кода
Логические бомбы	Разновидность троянских коней
Черви	Овладение распределенными ресурсами
Вирусы	Прикрепление к программам и размножение
Обход механизмов безопасности	
Эксплуатация уязвимостей	
Взлом паролей	
Активное злоупотребление	
Основной	
Инкрементальные атаки	Постепенная эскалация привилегий, медленное продвижение к цели
Отказ в обслуживании	Совершение массивных атак
Пассивное злоупотребление	
Обзор	Случайный или выборочный поиск
Сбор и вывод данных	Использование баз данных и анализ трафика

Категория/Вил атаки	Описание
Инертное злоупотребление	Косвенное злоупотребление
Косвенное злоупотребление	

В силу необходимости практической применимости таксономий, наиболее выгодными считаются комбинированные подходы, которые в некоторой степени реализуют все вышеописанные методы,,. Однако, способы комбинирования методов могут быть различны.

Один из способов комбинирования приводится в своей работе Саймон Хэнсмэн, – все анализируемые параметры разносятся отдельно и считаются попарно некоррелированными. Для достижения данной цели, автор использует концепцию «измерений», которая впервые была применена в работе Бишопа о классификации уязвимостей UNIX—систем.

Главную цель, которую преследовал Саймон Хэнсмэн, была разработка «прагматичной таксономии, которая полезна при ведении непрерывной работе над атаками». Первоначально производилась разработка таксономии древовидной структуры, подобно классификациям природного царства, – более общие категории находятся выше по высоте дерева, а нижние по высоте представляют более подробное описание категорий. Но на практике, в применении подобных класси-

фикационных схем имеется ряд неудобств. Во—первых, атаки зачастую несут смешанный характер. То есть складывается ситуация, при которой одна атака тесно зависит от другой или вложена в нее. Данная проблема, с одной стороны, решается путем введения межузловых ссылочных дуг между вершинами дерева, то есть при заполнении классификационной схемы образуется нагруженный граф. Однако это неизбежно сводится к беспорядку в структуре и сложностям при классификации. С другой стороны, возможно введение рекурсивных деревьев, где каждый лист дерева также является деревом. Но данное решение также сводится к беспорядочному росту структуры, и ограничению их применения. Во—вторых, атаки, в отличие от животных, не имеют обширного числа общих черт, вследствие чего имеют место сложности в формулировке классификационных групп верхних уровней. Действительно, у вредоносных программ типа «черви» или «вирусы» имеется достаточного много общих черт, однако непосредственных аналогий с атаками типа DoS (Denial of Service – отказ в обслуживании) и троянскими программами у них немного. Данная проблема ведет к разрастанию дерева на некоторое количество несвязанных между собой категорий, то есть до леса. Таким образом, древовидные классификации для практических задач.

Иной подход к созданию таксономий заключается в виде использования списочных структур. Таксономии, основанные на списочных структурах, представляются как сово-

купность списков категорий атак. С одной стороны, возможна организация общих классов категорий атак, с другой – возможно создание объемного количества списков, каждый из которых детально описывает уникальный класс категорий. Данные подходы также слабо применяются на практике, так как для первого случая организуются наборы крайне обобщенных категорий атак, а во—втором случае, детализация списков категорий бесконечна.

В предлагаемой Саймоном Хэнсмэном таксономии используется иной подход, основанный на концепции «измерений» Бишопа. Введение «измерений» позволяет комплексно рассматривать каждую атаку отдельно. В таксономии рассматривается четыре измерения для классификации атак:

1. Первое (базовое) измерение используется для категорирования атаки относительно классов атак на основе вектора атаки. Под вектором атаки понимается метод, с помощью которого атака достигает своей цели. При отсутствии подходящего вектора, атака классифицируется в ближайшую по смыслу категорию (табл. 4).

Таблица 4 —Значения вектора атак таксономии Хэнсмэна по уровням детализации

Уровень 1	Уровень 2	Уровень 3
Вирусы	Файловые вирусы	
	Вирусы, поражающие загрузочные записи	
	Макровирусы	
Черви	Массовые рассылки СПАМа	
	Сетевые черви	
Переполнение буфера	Стэк	
	Куча	
Отказ в обслуживании	Локальные	Исчерпание ресурсов
		Программное «обрушение»
	Сетевые	TCP–флуд
		UDP–флуд
		ICMP–флуд
	Распределенные	
Сетевые атаки	Спуфинг	
	Воровство сессии	
	Беспроводные атаки	Взлом WEP
	Атаки на веб–приложения	Cross–site scripting
		Подбор параметров
		Паразитные cookie
		Атаки на базы данных
		Манипулирование со скрытыми полями
Физические атаки	Базовые	
	Энергетическое оружие	Высокочастотное радиоактивное облучение
		Повышенная частота выброса заражающих веществ
		Электро–магнитный импульс
	Проверки ошибок вычислительной сети с дополнительными функциями и услугами	
Атаки на пароли	Отгадывание	Перебором
		По словарю
	Реализация эксплоита	
Разведка	Сниффинг	Сниффинг пакетов
	Выявление структуры	

2. Вторым измерением, атака классифицируется по цели атаки. Степень детализированности измерения достигается указанием конкретной версии продукта, например Linux Kernel 3.5.1rc—1, или же покрывается определенным классом возможных целей, например Linux Kernel (табл. 5).

Таблица 5 – Список целей атак таксономии Хэнсмэна по уровням детализации

Аппаратное обеспечение	Компьютер	Жесткие диски	…		
		Сетевое оборудование	Роутеры		
			Свитчи		
			Хабы		
			Кабеля		
			…		
		Периферия	Монитор		
			Клавиатура		
			…		
Программное обеспечение	Операционная система	Семейство Windows	Windows XP		
			Windows Server 2003		
		Семейство UNIX	Linux	RedHat Linux 6.0	
				RedHad Linux 7.0	
				…	
			FreeBSD	4.8	
				5.1	
				…	
			…		
	Приложение	Серверное	База данных	MySQL	5.5
			Сервер Email		
			…		
		Клиентское	Текстовый редактор	MS Word	2007
		…	…	…	…
	Сеть	Протоколы	Транспортный уровень	IP	
				Сетевой уровень	TCP
		…	…	…	…

3. Третье измерение используется для описания уязви-

мостей и эксплоитов, которыми реализуется данная атака. Измерение представляется списоком номеров CVE (Common Vulnerabilities and Exposures) известных уязвимостей по классификации проекта CVE **[12]**.

Идея проекта CVE была предложена Мэнном (Mann) и Кристли (Christley) **[24]** и предлагает унифицированный способ представления определений уязвимостей. На данный момент, проект является стандартом де—факто описания уязвимостей, и его применение является желательным в таксономиях прикладного направления.

Дополнительно, в таксономии Хэнсмэна предполагается ситуация, когда на момент классификации атаки не существует ее описания (CVE—номера) уязвимости. В этом случае, предлагается использовать общие классы категорий атак процессной таксономией компьютерных и сетевых атак Ховарда **[13]**, – уязвимость в реализации (логические ошибки в текстах программ), уязвимость в проекте, уязвимость в конфигурации. В данной таксономии рассматривается в качестве центрального понятия инцидент – совокупность атакующего, атаки и цели атаки. Главным ее отличием является наличие структурных элементов: инцидентов и события, – совокупности действия и целевого объекта. Предусматривается возможность комбинирования событий. Таким образом, в инциденте возможно вложение последовательность атак. Полезным свойством таксономии Ховарда является возможность описания неатомарных (состав-

ных) атак и учет их сценариев проведения. Однако, как указывается в тезисах докторской диссертации Лауфа, процессная таксономия привносит двусмысленность при классификации атаки на практике, так как нарушается свойство взаимного исключения.

4. Четвертое измерение используется для классификации атаки по наличию и виду полезной нагрузки (payload) или реализуемого эффекта. В большинстве случаев, в результате своей работы, с атакой привносится дополнительный эффект. Например, «вирус», используемый для установки потайного входа (backdoor) очевидно остается «вирусом», но несет в качестве полезной нагрузки программу потайного входа.

В качестве классов категорий полезной нагрузки, Хэнсмэн выделяет:

– Полезная нагрузка первого измерения – собственно полезная нагрузка является атакой;

– Повреждение информации;

– Раскрытие информации;

– Кража сервиса (подмена сервиса);

– Subversion – полезная нагрузка предоставляет контроль над частью ресурсов цели и использует их в своих целях.

В 1995 году, Бишоп [10] предложил классификацию относительно уязвимостей для UNIX—систем. Отличительная особенность его работы заключается в создании принципиально новый схемы классификации. Шесть «осей коорди-

нат» представляются компонентами [7], [10]:

– Природа уязвимости – описывается природа ошибки в категориях протекционного анализа;

– Время появления уязвимости;

– Область применения – что может быть получено через уязвимость;

– Область воздействия – на что может повлиять уязвимость;

– Минимальное количество – минимальное количество этапов, необходимых для атаки;

– Источник – источник идентификации уязвимости.

Особенностью классификации Бишопа является использование подхода на основе концепции измерений, вместо табличных и древовидных классификаций. Каждая координатная ось представляется классификационной группой, отсчеты по которой являются элементы группы, а уязвимость описывается в виде некоторой точке в «пространстве» координатных осей. Данная схема именуется таксономией уязвимостей в концепции измерений. Таксономия Бишопа является ярким представителем групп таксономий уязвимостей.

Важной основой для разработки новых таксономий уязвимостей в области информационной безопасности послужили работы Бисби (Bisbey) и Холлингворса (Hollingworth), посвященные протекционному анализу [25], а также работы по исследованию защищенных операционных систем (RI SOS) Аббота (Abbott), Вебба (Webb) и др. [4]. Обе таксоно-

мии фокусируют внимание на классифицировании ошибок в программном обеспечении и приблизительно схожи между собой.

Непригодность практического применения таксономий [25], [4] в своей дальнейшей работе описали Бишоп и Бэйли [11] . Проблемой предложенных таксономии является двусмысленность в определениях своих классов, то есть в определениях нескольких классов некоторые уязвимости равносильны, что приводит к нарушению правила взаимоисключения между классами, и тем самым представляются малопригодными в прикладном смысле. Однако, данные работы [25], [4] заложили основу ценным концепциям, которые получили свое развитие в последующих исследованиях [10], [26], [].

Комбинированный подход к классификации уязвимостей прослеживается и в нормативно—распорядительной документации ФСТЭК России. В классификации уязвимостей, предлагаемой базовой моделью угроз ИСПДн (рисунок 1), также применяется комбинированный подход, основанный на идеях работ Ховарда, Хэнсмэна, Бишопа и др.

Более того, для систематизации уязвимостей в соответствии с классификацией на практике, в документах предлагается использовать существующие зарубежные базы данных (БД) уязвимостей в качестве источников информации. Наиболее распространенной базой данных об уязвимостях является БД National Vulnerability Database (NVD), которая

основывается на объединении информации из более ранних баз данных (CPE, CVE, и др.)

1.3 Математические модели систем защиты информации

В работе [23] рассматривается вероятностная модель, в которой система защиты информации (СЗИ) представлена неконтролируемыми преградами вокруг предмета защиты. В общем случае модель элементарной защиты предмета может быть в виде защитных колец (рисунок 2). В качестве предмета защиты выступает один из компонентов информационной системы (ИС).

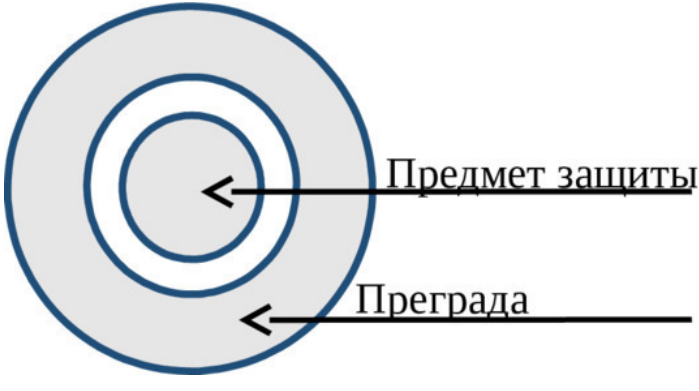

Рисунок 2 – Модель элементарной защиты

Вероятность невозможности преодоления преграды нарушителем обозначается как $P_{сзи}$, вероятность преодоления

преграды нарушителем через $P_{нр}$ соответственно сумма вероятностей двух противоположных событий равна единице, то есть:

$$P_{сзи} + P_{нр} = 1$$

$$P_{сзи} = \left(1 - P_{нр}\right)$$

В модели рассматриваются пути обхода преграды. Вероятность обхода преграды нарушителем обозначается через $P_{обх}$, которое представляется в виде:

(1)

$$P_{сзи} = \min\left\{\left(1 - P_{нр}\right), \left(1 - P_{обх}\right)\right\}$$

В случае, когда у преграды несколько путей обхода:
(2)

$$P_{сзи} = \min\left\{\left(1 - P_{нр}\right), \left(1 - P_{обх_1}\right), \left(1 - P_{обх_2}\right), \left(1 - P_{обх_3}\right), \ldots, \left(1 - P_{обх_k}\right)\right\}$$

где – k количество путей отхода.

Для случая, когда нарушителей более одного, и они действуют одновременно (организованная группа) по каждому пути, это выражение с учетом совместности событий выглядит как:
(3)

$$P_{сзи} = \left(1 - P_{нр}\right), \left(1 - P_{обх_1}\right), \left(1 - P_{обх_2}\right), \left(1 - P_{обх_3}\right) \ldots \left(1 - P_{обх_k}\right)$$

Учитывая, что на практике в большинстве случаев защитный контур (оболочка) состоит из нескольких «соединенных» между собой преград с различной прочностью, рассматривается модель многозвенной защиты (рисунок 3).

Выражение прочности многозвенной защиты из неконтролируемых преград, построенной для противостояния одному нарушителю, представлено в виде:

(4)

$$P_{зи} = \min\left\{ P_{сзи_1}, P_{сзи_2}, \ldots, P_{сзи_i}\left(1 - P_{обх_1}\right), \left(1 - P_{обх_2}\right) \ldots \left(1 - P_{обх_k}\right) \right\}$$

где – $P_{сзи}$ прочность i—й преграды, $P_{обх}$ – вероятность обхода преграды по k —му пути.

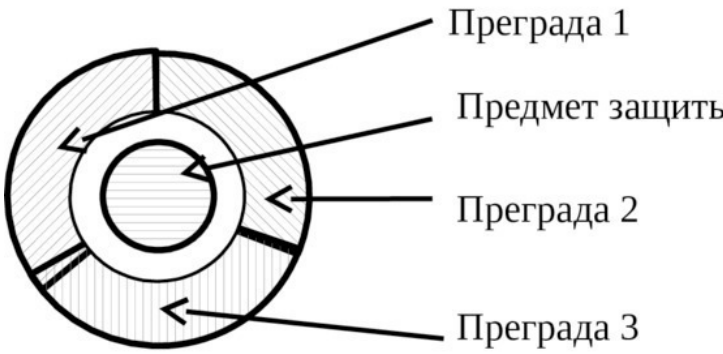

Рисунок 3 – Модель многозвенной защиты

Выражение для прочности многозвенной защиты, построенной из неконтролируемых преград для защиты от организованной группы квалифицированных нарушителей—профессионалов, с учетом совместности событий представляется в виде:

(5)

$$P_{зи0} = P_{сзи_1} \cdot P_{сзи_2} ¿ \ldots \cdot P_{сзи_i} ¿ \left(1 - P_{обх_1}\right) ¿ \left(1 - P_{обх_2}\right) ¿ \ldots \cdot \left(1 - P_{обх_k}\right)$$

В случае, когда какие—либо преграды дублируются, а их

прочности равны соответственно $P_1, P_2, P_3, \ldots, P_i$ то вероятность преодоления каждой из них нарушителем соответственно равна $(1 - P_1), (1 - P_2), (1 - P_3), \ldots, (1 - P_i)$.

Учитывая, что факты преодоления этих преград нарушителем события совместные, вероятность преодоления суммарной преграды нарушителем формально представляется в виде:

(6)

$$P_{нр} = (1 - P_1)(1 - P_2)(1 - P_3)\ldots(1 - P_i)$$

Вероятность невозможности преодоления дублирующих преград (прочность суммарной преграды) как противоположное событие определяется выражением:

(7)

$$P = 1 - P_{нр} = 1 - \left(1 - P_1\right)\left(1 - P_2\right)\left(1 - P_3\right)\ldots\left(1 - P_i\right)$$

где – i порядковый номер преграды, P_i прочность i– й преграды.

Также в работе представлена модель многоуровневой системы защиты (рисунок 4).

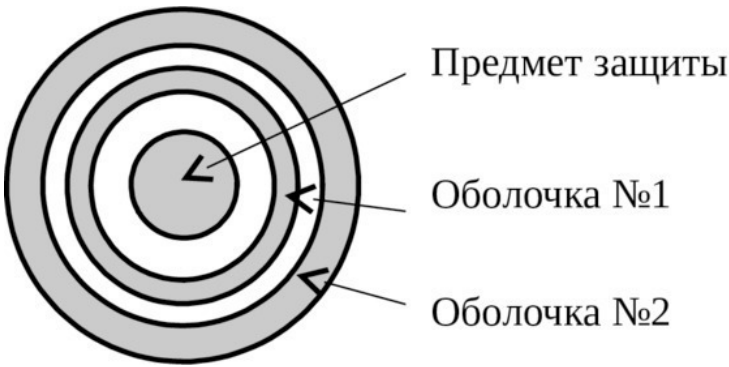

Рисунок 4 – Модель многоуровневой защиты

При расчете суммарной прочности нескольких оболочек (контуров) защиты в формулу (7) вместо P_i, включается P_{ki} – прочность каждой оболочки (контура), значение которой

определяется по одной из формул (4), (5) и (6):

(8)

$$P = 1 - P_{нр} = 1 - \left(1 - P_{k_1}\right)\left(1 - P_{k_2}\right)\left(1 - P_{k_3}\right)\ldots\left(1 - P_{k_i}\right)$$

При $P_{ki} = 0$ данная оболочка (контур) в расчет не принимается. При $P_{ki} = 1$, остальные оболочки защиты являются избыточными. Данная модель справедлива лишь для замкнутых оболочек защиты, перекрывающих одни и те же каналы несанкционированного доступа к одному и тому же предмету защиты.

В случае контролируемой преграды, т.е. когда преграда связана с каким—либо тревожным датчиком, который может подать сигнал в случае попытки преодоления преграды.

Исходя из данной временной диаграммы процесса контроля и обнаружения несанкционированного доступа (НСД) (рисунок 5), в работе [27] приводятся формулы для расчета вероятности обнаружения и блокировки НСД $P_{обл}$ и $P_{отк}$ вероятности отказа системы обнаружения :

(9)

$$P_{обл} = \frac{t_{пр}}{T_{обл}}$$

(10)

$$P_{отк}(t) = e^{-\lambda t}$$

где λ – интенсивность отказов группы технических средств, составляющих систему обнаружения и блокировки НСД, *t* – рассматриваемый интервал времени функционирования системы обнаружения и блокировки НСД.

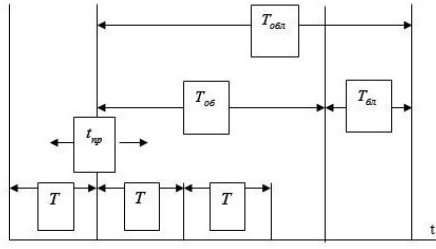

Рисунок 5 – Временная диаграмма процесса контроля НСД

(T – период опроса датчиков; $T_{об}$ – время передачи сигнала и обнаружения НСД; $T_{бл}$ – время блокировки доступа; $T_{обл}$ – время обнаружения и блокировки; – время простоя)

Учитывая, что отказ системы контроля и НСД могут быть совместными событиями, формула прочности контролируемой преграды для элементарной защиты принимает вид:

(11)

$$P_{сзи_k} = \min\left\{P_{обл}, \left(1 - P_{отк}\right), \left(1 - P_{обх_1}\right), \left(1 - P_{обх_2}\right), \ldots, \left(1 - P_{обх_k}\right)\right\}$$

где $P_{обл}$ и $P_{отк}$ определяются соответственно по формулам (9) и (10), $P_{обх}$ и количество путей обхода к определяются

экспертным путем на основе анализа принципов построения конкретной системы контроля и блокировки НСД.

Выражение для прочности многозвенной защиты с контролируемыми преградами для защиты от одного нарушителя будет в следующем виде

(12)

$$P_{зи_k} = \min\left\{ P_{сзи_{k_1}}, P_{сзи_{k_2}}, \ldots, P_{сзи_{k_n}}, \left(1 - P_{обх_1}\right), \left(1 - P_{обх_2}\right), \ldots, \left(1 - P_{обх_j}\right) \right\}$$

где $P_{сзиkn}$ прочность n—й преграды, $P_{обхn}$ – вероятность обхода преграды по j —му пути.

Формула для расчета прочности защитной оболочки с контролируемыми преградами для защиты от организованной группы нарушителей представлена в виде:

(13)

$$P_{зи_0} = P_{сзи_{k_1}} \times P_{сзи_{k_2}} \times \ldots \times P_{сзи_{k_n}} \times \left(1 - P_{обх_1}\right) \times \left(1 - P_{обх_2}\right) \times \ldots \times \left(1 - P_{обх_j}\right)$$

В работе [28] приводится вероятностная модель оценки уязвимости информации. В данной модели выделяется пять зон, в которых возможны несанкционированные действия:

Конец ознакомительного фрагмента.

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, купив полную легальную версию на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.