ВЕСТНИК НОВЫХ МЕДИЦИНСКИХ ТЕХНОЛОГИЙ – 2015 – N 2
Электронный журнал

УДК: 663.1:004.056 DOI: 10.12737/ 11910

ДЕТАЛЬНЫЙ АЛГОРИТМ МНОЖЕСТВА РЕАЛИЗАЦИЙ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МЕДИЦИНСКОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ

В.П. ГУЛОВ[*], В.А. ХВОСТОВ[**], П.Е. ЧЕСНОКОВ[*]

[*]*ГБОУ ВПО ВГМА им. Бурденко Н.Н. Минздрава России, ул. Студенческая, д.10, г. Воронеж, Россия, 394000*
[**]*Федеральное автономное учреждение «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю», ул. 9 Января, д. 280а, г. Воронеж, Россия, 394026*

Аннотация. Приведен детальный алгоритм реализации угроз информационной безопасности к информационным ресурсам медицинских информационных систем, используемых при обработке персональных данных. Предложенный алгоритм разработан применительно к задачам обоснования требований к информационной безопасности содержит вербальное и статистическое описание основных этапов реализации угроз. В основу алгоритма положены результаты статистической обработки экспериментальных записей цифрового потока для типовых условий с использованием специализированных программных средств анализа. Предложен перечень зарегистрированных признаков для распознавания угроз информационной безопасности в цифровом потоке. Методика экспериментального анализа статистических характеристик реализаций угроз информационной безопасности состоит из следующих этапов: запись цифрового потока в сегменте локальной вычислительной сети, реализующей информационной безопасности, за представительный период времени, распознавание типов реализаций угроз информационной безопасности по признакам IP пакетов. Детальный алгоритм предназначен для разработки прогнозной «картины состояний природы», являющейся исходными данными процедуры нормирования требований к информационной безопасности методами принятия решений. Для формализации многофакторного характера реализаций угроз информационной безопасности предложен метод построения формальных моделей с использованием логических деревьев атак с присвоением дугам дерева числовых коэффициентов, имеющих временной смысл.

Ключевые слова: информационная безопасность, модель защиты, критерий эффективности.

A DETAILED ALGORITHM OF A PLURALITY OF IMPLEMENTATIONS OF INFORMATION SECURITY THREATS IN THE MEDICAL INFORMATION SYSTEM

V.P. GULOV[*], V.A. KHVOSTOV[**], P.E. CHESNOKOV[*]

[*]*Medical University VGMA them. NN Burdenko Russian Ministry of Health, st. Student, 10, Voronezh, Russia, 394000*
[**]*Federal Autonomous Institution "State Research and Testing Institute for technical protection of information from the Federal Service for Technical and Export Control," st. January 9, etc. 280a, Voronezh, Russia, 394026*

Abstract. The article presents a detailed algorithm for implementing information security threats to information resources health information systems used in the processing of personal data. The proposed algorithm is developed in relation to the problems of justification of requirements to information security, contains verbal and statistical description of the basic stages of realization of threats. The algorithm is based on the results of statistical processing of experimental records the digital stream to the standard conditions using specialized software analysis tools. The authors offer a list of registered signs for recognition of threats to information security in the digital stream. The technique of the experimental analysis of statistical characteristics of realizations of information safety threats consists of following stages: recording the digital data stream segment local area network that implements information security representative for a period of time, recognition of the types of implementations of information security threats on the grounds of IP packets. The detailed algorithm is designed to develop a predictive "picture of state of nature, which is source data of the normalization procedure of requirements for information security methods of decision making. To formalize multivariate nature of the implementations of information security threats, the authors propose a method of constructing formal models using logical attack trees with the assignment of the arcs of the tree of the numerical coefficients that have a temporal meaning.

Key words: information safety, protection model, criterion of efficiency.

Библиографическая ссылка:
Гулов В.П., Хвостов В.А., Чесноков П.Е. Детальный алгоритм множества реализаций угроз информационной безопасности в медицинской информационной системе // Вестник новых медицинских технологий. Электронное издание. 2015. №2. Публикация 1-4. URL: http://www.medtsu.tula.ru/VNMT/Bulletin/E2015-2/5191.pdf (дата обращения: 30.06.2015). DOI: 10.12737/ 11910

Развитие здравоохранения России направлено также и на повышение эффективности посредством широкого внедрения информационных технологий. При этом реализуются проекты по внедрению в поликлиниках и больницах электронных медицинских карт пациентов, предоставлению услуг «электронной регистратуры», созданию территориальных медицинских регистров и *автоматизированных систем* (АС) в здравоохранении (*медицинских информационных систем* (МИС). Эта качественно новая технологическая среда информационного взаимодействия в современной медицине создает также и множество новых проблем, связанных с обеспечением конфиденциальности медицинской информации и сохранением врачебной тайны и других *персональных данных* (ПДн) при их использовании. Гарантия защиты ПДн в учреждениях здравоохранения России также закреплена законодательно Федеральными законами.

Обоснование требований к системам обеспечения *информационной безопасности* (ИБ), реализующим защиту ПДн, является одним из ключевых этапов, выполняемых при разработке МИС. Работа по обоснованию требований к ИБ регламентируется большим количеством нормативных документов. В частности руководящими документами *Федеральной службы технического и экспортного контроля* (ФСТЭК) России, стандартами [1], ведомственными приказами и инструкциями. Методологической основой обоснования требований к ИБ в России являются нормативные документы ФСТЭК России. При этом используется классификационный подход, заключающийся в сопоставлении функций защиты реализуемых в *системе защиты информации* (СЗИ) с перечнем функций защиты обязательных к реализации для определенного класса защищенности или профиля защиты. При использовании классификационного подхода обоснования требований полнота непротиворечивость модели защиты обеспечивается использованием периметрового подхода. Подробное изложение периметровой модели при обосновании требований к СЗИ приведено в [2-5].

Как показано в [3], классификационные методы обоснования требований к СЗИ обладают рядом недостатков. В частности классификационные методы не позволяют применять методы технического синтеза в области ИБ при проектировании АС, широко используемые при их проектировании по другим аспектам. В этой связи перспективным видится переход от классификационных подходов к подходам, основанным на оценке эффективности СЗИ, нормировании требований [3]. При этом традиционная периметровая модель защиты, основанная на вербальном умозрительном описании реализации угроз ИБ, не удовлетворяет требованиям метода нормирования.

Периметровая модель привязывается к уязвимостям объекта защиты – МИС. При этом не рассматриваются конкретные реализации угроз ИБ (последовательность реализации различных этапов, вероятностные и временные характеристики, возможные варианты и их цели, механизм возникновения ущербов).

Таким образом, исходя из потребности научных основ технического синтеза при проектировании подсистем обеспечения безопасности МИС, **целью статьи** является разработка детального типового алгоритма реализации угроз *несанкционированного доступа* (НСД) в терминах конкретных способов реализаций угроз ИБ и программных средств для их осуществления. Детальный алгоритм разрабатывается в интересах формирования «картины состояний природы» при решении задачи нормирования требований к ИБ методами принятия решений.

Последовательность реализации угроз ИБ можно составить, используя разработанную конфликтно-динамическую модель [4] и специальную литературу [3]. Алгоритм реализации угроз ИБ условно можно разделить на три этапа.

1. Сбор информации о топологии и принципах функционирования АС. Он включает такие действия, как определение сетевой топологии, типа и версии *операционной системы* (ОС) разведываемого объекта, а также доступных сетевых и иных сервисов.

2. Непосредственное проникновение в автоматизированную систему. Проникновение подразумевает под собой преодоление средств защиты периметра и может реализовываться различными путями. Например, использованием уязвимости сервиса компьютера, реализующего защиту (запуск эксплойта). Такое содержание может задействовать так называемые «туннели» в средствах защиты информации, через которые затем возможно проникновение в МИС. К этому шагу можно отнести подбор пароля администратора или иного пользователя.

3. Установление контроля над автоматизированной системой. Установление контроля подразумевает получение прав администратора (*root*) и использование утилиту скрытого управления (*backdoor, rootcit*). При этом одним из основныхтребований к данному виду программ является скрытность ее использования в МИС. Таким образом, важнейшим компонентом любого *руткита* являются программы, скрывающие присутствие постороннего кода (например, кода *backdoor*-программы), данных (файлов, каталогов, ключей реестра) и процессов.

Конкретные способы реализаций всех трех этапов с их полным описанием содержатся в базе данных компьютерных атак, ведущейся *DARPA (DARPA Intrusion Detection Attacks Database)* доступные в интернет по адресу *www.II.mit.edu.*

Детальный типовой алгоритм реализации НСД с использованием рассмотренных способов и содержательная часть этапов 1,2,3 типового алгоритма реализации НСД представлены в табл. 1.

Библиографическая ссылка:
Гулов В.П., Хвостов В.А., Чесноков П.Е. Детальный алгоритм множества реализаций угроз информационной безопасности в медицинской информационной системе // Вестник новых медицинских технологий. Электронное издание. 2015. №2. Публикация 1-4. URL: http://www.medtsu.tula.ru/VNMT/Bulletin/E2015-2/5191.pdf (дата обращения: 30.06.2015). DOI: 10.12737/ 11910

Таблица 1

Детальное описание реализаций угроз НСД

Наименование атаки	Используемый сервис (протокол)	Уязвимая операционная система	Механизм реализации	Среднее время реализации	Цель реализации	Краткое описание
Сбор информации о топологии и принципах функционирования автоматизированной системы (*Probes*)						
Ipsweep	*ISMP*	Все	Неправомерное использование	Короткое. Полное сканирование TCP/IP портов одной компьютерной системы единицы минут. Идентификация сетевых маршрутов и открытых для использования сетевых служб до нескольких секунд.	Поиск функционирующих СВТ	Идентификация объекта НСД и исследование его технического облика и характеристик отдельных компонентов – данных непосредственно о самих компьютерах, модулях, их составляющих и иной аппаратуре, используемой в компьютерной системе, конфигурации программно-аппаратного обеспечения и средств защиты.
Mscan	множество	Все	Неправомерное использование		Поиск известных уязвимостей	
Nmap	множество	Все	Неправомерное использование		Обнаружение открытых портов *TCP/IP*	
Saint	множество	Все	Неправомерное использование		Поиск известных уязвимостей	
Satan	множество	Все	Неправомерное использование		Поиск известных уязвимостей	
Непосредственное проникновение в автоматизированную систему (*RemotetoLocalUserAttacks*)						
Dictionary	*telnet, rlogin, pop, imap, ftp*	Все	Неправомерное использование	Среднее. Время подбора пароля от нескольких секунд до нескольких лет (в зависимости от предусмотренных мер защиты и производительности компьютерной системы или сети используемой для подбора пароля)	Получение доступа с правами пользователя	Вскрытие парольных систем защиты данных методами простого перебора и перебора по заданному словарю.
Ftpwrite	*ftp*	Все	Ошибки конфигурации и настройки	Короткое	Получение доступа с правами пользователя	Получение доступа к компьютерной системе с правами пользователя с помощью с использованием анонимной программы передачи файлов *misconfiguration*
Guest	*telnet, rlogin*	Все	Ошибки конфигурации и настройки		Получение доступа с правами пользователя	Вариант атаки подбора по словарю. На плохо сконфигурированных системах учетная запись гостя достигается без пароля по умолчанию. Это одна из первых и простейших уязвимостей используемая при атаке.
Imap	*imap*	*Linux*	Ошибки при разработке программ		Получение доступа с правами администратора (*root*)	Организация канала доступа к информационным ресурсам с использованием атаки на переполнение буфера.
Named	*dns*	*Linux*	Ошибки при разработке программ		Получение доступа с правами администратора (*root*)	Получение доступа с правами администратора посредством подделывания ответов на *DNS* запрос.

Библиографическая ссылка:
Гулов В.П., Хвостов В.А., Чесноков П.Е. Детальный алгоритм множества реализаций угроз информационной безопасности в медицинской информационной системе // Вестник новых медицинских технологий. Электронное издание. 2015. №2. Публикация 1-4. URL: http://www.medtsu.tula.ru/VNMT/Bulletin/E2015-2/5191.pdf (дата обращения: 30.06.2015). DOI: 10.12737/ 11910

Продолжение таблицы 1

Наименование атаки	Используемый сервис (протокол)	Уязвимая операционная система	Механизм реализации	Среднее время реализации	Цель реализации	Краткое описание
Phf	*http*	Все	Ошибки при разработке программ	Короткое	Запуск команд от имени пользователя *http*	Организация канала доступа к информационным ресурсам с использованием атаки основанной на применении *CGI* скрипта, выполняемого с более высоким уровнем привилегий на сервере.
Sendmail	*smtp*	Linux	Ошибки при разработке программ	Большое	Запуск команд от имени администратора	Организация канала доступа к информационным ресурсам с использованием атаки на переполнение буфера почтового сервера
Xlock	*X*	Все	Ошибки конфигурации и настройки	Среднее	Обход парольной защиты	В нападении *Xlock* удаленный атакующий получает локальный доступ, используя открытый авторизованным локальным пользователем *X* терминал.
Xsnoop	*X*	Все	Ошибки конфигурации и настройки	Короткое	Удаленное слежение за командной строкой	Атака посредством наблюдения нажатия клавиши, обработанные незащищенным *X* сервером, чтобы попытаться получить информацию, которая может использоваться для получения локального доступа.
Установление контроля над автоматизированной системой (*UsertoRootAttacks*)						
Eject	Любая сессия пользователя	*Solaris*	Переполнение буфера	Среднее	Получение доступа с правами администратора (*root*)	1. Организация канала доступа к информационным ресурсам. 2. Программное копирование данных из электронных носителей. 3. Использование информации, которая осталась на носителях после ее обработки ("сборка мусора"). 4. Перехват защищаемых данных. 5. Вскрытие пароля. 6. Модификация алгоритма функционирования средств защиты информации.
Ffbconfig	Любая сессия пользователя	Все	Переполнение буфера	Среднее	Получение доступа с правами администратора (*root*)	
Fdformat	Любая сессия пользователя	Все	Переполнение буфера	Среднее	Получение доступа с правами администратора (*root*)	
Perl	Любая сессия пользователя	Все	Ошибки конфигурации и настройки	Короткое	Получение доступа с правами администратора (*root*)	
Ps	Любая сессия пользователя	*Solaris*	Ошибки конфигурации и настройки	Короткое	Получение доступа с правами администратора (*root*)	
Xterm	Любая сессия пользователя	*Linux*	Переполнение буфера	Короткое	Получение доступа с правами администратора (*root*)	

Методический подход к формализации конфликтно динамических процессов, происходящих при НСД, позволяющих в дальнейшем решать задачу нормирования требований к ИБ, предложен в [4].

Для формализации используется с использованием математического аппарата марковских процессов. При этом детальный типовой алгоритм реализации НСД формализуется графом, отображающим динамику выполнения всех этапов НСД всеми способами. В [3] получено аналитическое выражение для вероятности выполнения НСД для стационарного случая.

Библиографическая ссылка:
Гулов В.П., Хвостов В.А., Чесноков П.Е. Детальный алгоритм множества реализаций угроз информационной безопасности в медицинской информационной системе // Вестник новых медицинских технологий. Электронное издание. 2015. №2. Публикация 1-4. URL: http://www.medtsu.tula.ru/VNMT/Bulletin/E2015-2/5191.pdf (дата обращения: 30.06.2015). DOI: 10.12737/ 11910

Результирующее выражение марковской модели предназначено для оценки целевой функции ИБ – вероятности реализации различных вариантов угроз и механизмов защиты в виде:

$$P_{нсд} = \prod_{i=1}^{3}(1-1/(1+\sum_{j=1}^{n,k,m}\frac{\lambda_i^j}{\mu_i^j}(1+\beta_i^j\frac{\mu_i^j}{\nu_i^j}))) \quad (1)$$

Где i – этап реализации угрозы ИБ; j – способ i-го этапа реализации имеет экспоненциальное распределение с параметром λ_i^j; β_i^j – доля не обнаруживаемых СЗИ типовых угроз ИБ для j-го способа i-го этапа реализации; ν_i^j – параметр экспоненциального времени реализации действий по НСД j-го способа i-го этапа реализации угрозы;

μ_i^j – параметр экспоненциального времени нейтрализации обнаруженных действий j-го способа i-го этапа реализации угрозы;

n, k, m – количество способов реализации угроз НСД первого, второго и третьего этапов.

Значения параметра λ_i^j определяются на основе статистической обработки цифрового потока в сети.Методика экспериментального анализа статистических характеристик реализаций угроз ИБ состоит в следующем [3].

1. Запись цифрового потока в *локальной вычислительной сети* (ЛВС) за представительный период времени с использованием *tcpdump*. Анализатор пакетов *tcpdump* является широко используемым средством, позволяющим исследовать трафик, передающийся в локальной сети. Вывод информации обо всех заголовках *IP* пакета и объеме его полезной информации выполняется в специальный *log* файл. Пример записанного цифрового потока представлен на рис. 1.

2. Распознавание типов реализаций угроз ИБ по признакам *IP* пакетов. При этом можно использовать имеющиеся СОВ. В частности бесплатный фильтр для обработки данных *Snort (http://snort.source-fire.com/)*. К системе Snort существует много дополнительных утилит, расширяющих ее функциональность. В частности *Snort_stat* – скрипт для статистического анализа журнала регистрации *Snort*. Пример перечня признаков, содержащихся в IP пакете, используемых для распознавания НСД представлен в табл. 2.

Примерный состав стенда для статистической обработки цифрового потока представлен на рис. 2.

Результаты статистической обработки экспериментальных записей цифрового потока для типовых условий с использованием рассмотренной методики доступны в интернет по адресу *www.II.mit.edu*.

Для оценки параметров $\square$ можно воспользоваться методикой формализации угроз ИБ, разработанной в [4]. В качестве основополагающей конструкции здесь выступает иерархическое дерево $G = (L, E)$, где $L= \{l_i\}$ – множество вершин дерева, $E=\{e_s\}$, $E \in \{L^2\}$ – множество дуг дерева. Каждая вершина дерева G ассоциируется с определенным действием нарушителя, при этом корень дерева обозначаетконечную цель информационной атаки, реализация которой может нанести значительный ущерб МИС.

Таким образом, на графе G имеется возможность составить множество возможных путей $Gp = \{gp_r\}$, где каждый путь gp_r представляет собой последовательность дуг $(e_1, e_2, ...e_n)$ вида $e_i = (l_i, l_j)$, $l_i, l_j \in L$, при этом конечная вершина дуги l_i. одновременно является начальной вершиной дуги l_{i+1}.

Таблица 2

Перечень некоторых зарегистрированных признаков для распознавания угроз ИБ в цифровом потоке

№ п.п.	Название признака	Тип шкалы	Описание
1	*duration*	*continuous*	Длительность соединения
2	*protocol_type*	*discrete*	Тип протокола
3	*service*	*discrete*	Сетевой сервис
4	*flag*	*discrete*	Флаг отсутствия ошибки при соединении
5	*src_bytes*	*continuous*	Число байт, переданных от источника к получателю
6	*dst_bytes*	*continuous*	Число байт, переданных от получателя к источнику
7	*land*	*discrete*	1 – если у соединения совпадает получатель и источник (*host/port*); 0 – в противном случае
8	*wrong_fragment*	*continuous*	Число поврежденных фрагментов
9	*urgent*	*continuous*	Число важных (urgent) пакетов
10	*hot*	*continuous*	Число hot индикаторов
11	*num_failed_logins*	*continuous*	Число ошибок при вводе пароля

Библиографическая ссылка:
Гулов В.П., Хвостов В.А., Чесноков П.Е. Детальный алгоритм множества реализаций угроз информационной безопасности в медицинской информационной системе // Вестник новых медицинских технологий. Электронное издание. 2015. №2. Публикация 1-4. URL: http://www.medtsu.tula.ru/VNMT/Bulletin/E2015-2/5191.pdf (дата обращения: 30.06.2015). DOI: 10.12737/ 11910

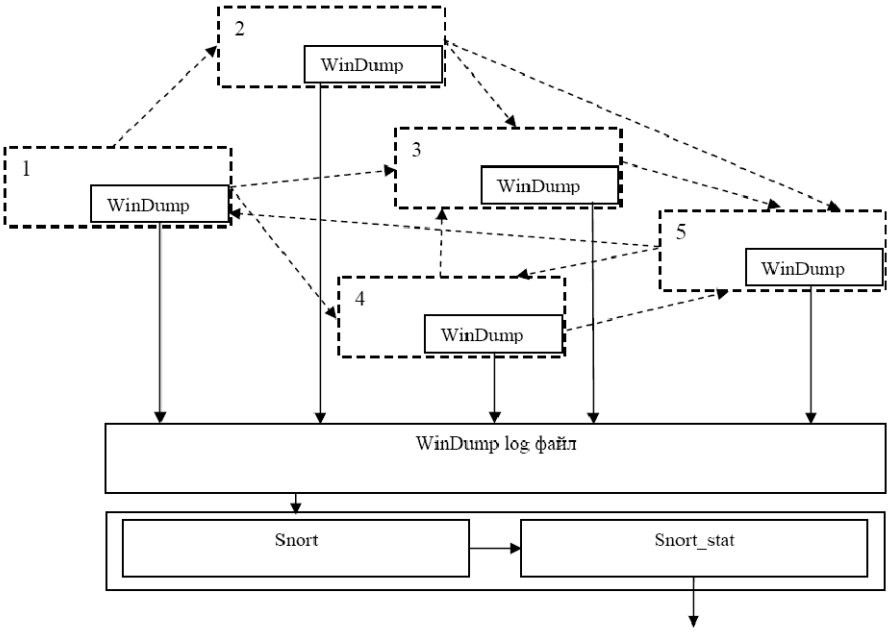

Рис. 1. Структурная схема стенда сбора и анализа статистических характеристик реализаций угроз ИБ АС, соответствующая структуре типовой АС

В качестве начальной вершины пути могут выступать листья дерева *G,* а в качестве конечной вершины – корень дерева *G.*

С семантической точки зрения каждая вершина дерева может трактоваться двумя способами:

– вершина дерева обозначает совокупность действий нарушителя, причем все они выполняются для достижения конечной цели атаки (такие вершины именуются вершинами, построенными на основе логической связки «И»);

– вершина дерева обозначает совокупность действий нарушителя, причем выполнения любого из них достаточно для достижения конечной цели атаки (такие вершины называются вершинами, построенными на основе логической связки «ИЛИ»).

Деревья атак могут изображаться как в графическом, так и в текстовом виде. Корень этого дерева – вершина $l_0 \in L-$ обозначает действие нарушителя. Для выполнения этого действия злоумышленник первоначально должен осуществить все операции, которые обозначаются элементами $\{l_i \in L\}_{i[1,n]}$. При этом последовательность действий, выполняемых нарушителем, определяется индексами вершин $\{l_i \in L\}_{i[1,n]}$, т.е. первым выполняется действие, ассоциированное с вершиной $l_1 \in L$, а последним – $l_n \in L$. С каждой дугой дерева сопоставляется параметр, имеющий смысл времени реализации НСД, соотнесенного с дугой. Тогда формальная модель угрозы ИБ будет иметь следующий вид:

$$\begin{aligned} G &= (L, E, \overline{T}_G); \\ L &= \{l_0, l_1, l_2, ...l_n\}; \\ E &= \{(l_0, l_1, t_{01})(l_0, l_2, t_{02}), ...(l_i, l_j, t_{ij})\}; \end{aligned} \quad (2)$$

где t_{ij} – время реализации, соответствующее дуге дерева атаки ij.

$\overline{T}_G$ – среднее время реализации всего дерева атаки.

Построение деревьев атак и оценку параметров v_i^j можно осуществить на основе анализа материалов [4], содержащих детальное описание способов реализации НСД. Пример дерева атаки представлен на рис. 3.

Библиографическая ссылка:
Гулов В.П., Хвостов В.А., Чесноков П.Е. Детальный алгоритм множества реализаций угроз информационной безопасности в медицинской информационной системе // Вестник новых медицинских технологий. Электронное издание. 2015. №2. Публикация 1-4. URL: http://www.medtsu.tula.ru/VNMT/Bulletin/E2015-2/5191.pdf (дата обращения: 30.06.2015). DOI: 10.12737/ 11910

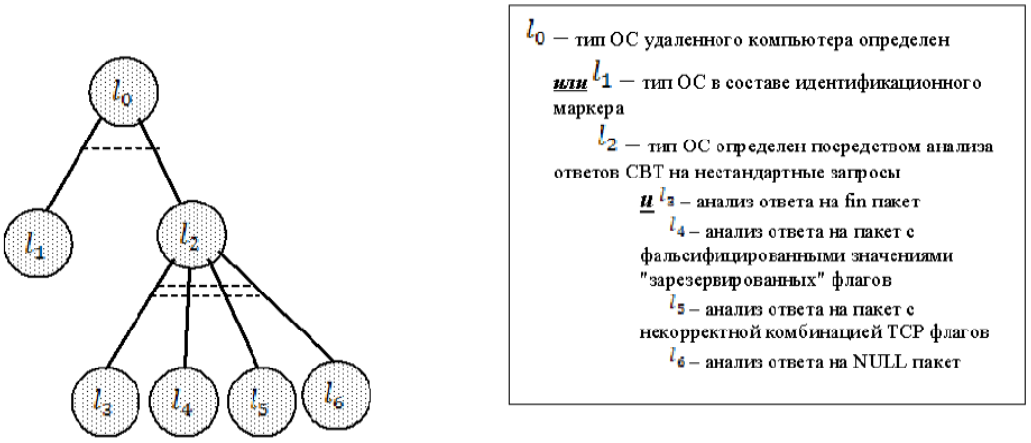

Рис. 2. Пример дерева атаки определения типа операционной системы

Таким образом, детальный алгоритм реализации угроз НСД к информационным ресурсам МИС, разработанный применительно к задаче нормирования требований к ИБ, представляет собой совокупность логических деревьев атак с оценками параметра v_i^j и характеризуемых статистическими характеристиками их реализации λ_i^j.

Литература

1. ГОСТ Р ИСО/МЭК 15408-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. М.: ИПК Издательство стандартов, 2002.

2. Макаров О.Ю., Хвостов В.А., Хвостова Н.В.Методика нормирования требований к информационной безопасности автоматизированных систем // Вестник Воронежского государственного технического университета. 2010. Т.6, №11. С. 47–51.

3. Методы и средства повышения защищенности автоматизированных систем: монография / Хвостов В.А. [и др.]; под общ.ред. д-ра техн. наук, проф. С.В. Скрыля и д-ра техн. наук, проф. Е.А. Рогозина Воронеж: Воронежский институт МВД России, 2013. 108 с.

4. Кисляк А.А., Макаров О.Ю., Рогозин Е.А., Хвостов В.А. Методика оценки вероятности несанкционированного доступа в автоматизированные системы, использующие протокол TCP/IP // Информация и безопасность. 2009. Т. 12, №2. С. 285–288.

5. Кисляк А.А., Макаров О.Ю., Рогозин Е.А., Хвостов В.А. Об одном способе формализации понятия стойкости функции безопасности ГОСТ ИСО/МЭК 15408 // Вестник Воронежского государственного технического университета. 2009. Т.5, №2 С. 94–98.

References

1. GOST R ISO/MEK 15408-2002. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Kriterii otsenki bezopasnosti informatsionnykh tekhnologiy. Moscow: IPK Izdatel'stvo standartov; 2002. Russian.

2. Makarov OYu, Khvostov VA, Khvostova NV. Metodika normirovaniya trebovaniy k informatsi-onnoy bezopasnosti avtomatizirovannykh sistem. Vestnik Voronezhskogo gosudarstvennogo tekhnichesko-go universiteta. 2010;6(11):47-51. Russian.

3. Khvostov VA, et al. Metody i sredstva povysheniya zashchishchennosti avtomatizirovannykh sistem: monografiya; pod obshch.red. d-ra tekhn. nauk, prof. S.V. Skrylya i d-ra tekhn. nauk, prof. E.A. Rogozina Voronezh: Voronezhskiy institut MVD Rossii; 2013. Russian.

Библиографическая ссылка:
Гулов В.П., Хвостов В.А., Чесноков П.Е. Детальный алгоритм множества реализаций угроз информационной безопасности в медицинской информационной системе // Вестник новых медицинских технологий. Электронное издание. 2015. №2. Публикация 1-4. URL: http://www.medtsu.tula.ru/VNMT/Bulletin/E2015-2/5191.pdf (дата обращения: 30.06.2015). DOI: 10.12737/ 11910

4. Kislyak AA, Makarov OYu, Rogozin EA, Khvostov VA. Metodika otsenki veroyatnosti nesanktsionirovannogo dostupa v avtomatizirovannye sistemy, ispol'zuyushchie protokol TCP/IP. Informatsiya i bezopasnost'. 2009;12(2):285-8. Russian.

5. Kislyak AA, Makarov OYu, Rogozin EA, Khvostov VA. Ob odnom sposobe formalizatsii ponyatiya stoykosti funktsii bezopasnosti GOST ISO/MEK 15408. Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta. 2009;5(2):94-8. Russian.

Библиографическая ссылка:
Гулов В.П., Хвостов В.А., Чесноков П.Е. Детальный алгоритм множества реализаций угроз информационной безопасности в медицинской информационной системе // Вестник новых медицинских технологий. Электронное издание. 2015. №2. Публикация 1-4. URL: http://www.medtsu.tula.ru/VNMT/Bulletin/E2015-2/5191.pdf (дата обращения: 30.06.2015). DOI: 10.12737/ 11910