Гулов Владимир Павлович
д-р биол. наук, профессор
ФГБОУ ВО «Воронежский государственный
медицинский университет им. Н.Н. Бурденко»
Минздрава России
г. Воронеж, Воронежская область
Скрыпников Алексей Васильевич
д-р техн. наук, профессор, заведующий кафедрой
ФГБОУ ВО «Воронежский государственный
университет инженерных технологий»
г. Воронеж, Воронежская область
Хвостов Виктор Анатольевич
канд. техн. наук, преподаватель
ФГБОУ ВО «Воронежский государственный
университет инженерных технологий»
г. Воронеж, Воронежская область
Пелешенко Елена Ивановна
канд. техн. наук, начальник отдела защиты ОИС
ФГБОУ ВО «Воронежский государственный
медицинский университет им. Н.Н. Бурденко»
Минздрава России
г. Воронеж, Воронежская область

МОДЕЛИ И АЛГОРИТМЫ ПРОГНОЗА ВОЗМОЖНОСТЕЙ РЕАЛИЗАЦИИ УГРОЗ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ ТЕХНОЛОГИЧЕСКИХ МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ

Аннотация: *статья посвящена разработке и внедрению модели прогноза угроз информационной безопасности информационных систем, используемых в медицинском исследовании. Разработан алгоритм количественной оценки типичных угроз несанкционированного доступа к системам обработки медицинской информации.*

Ключевые слова: *обеспечение безопасности, несанкционированный доступ, медицинские информационные системы.*

В настоящее время развитие средств вычислительной техники привело к появлению технологических медицинских информационных систем (МИС). Особенностью этих систем является работа непосредственно в процессе оказания медицинской помощи, приближением непосредственно к пациенту и зависимости как качества предоставления медицинской услуги, а зачастую и жизни пациента, от надежности их функционирования. Примером технологических МИС напрямую определяющих жизнь пациента являются роботы, используемые в телехирургии, автоматические системы дозирования лекарственных препаратов в реанимационных отделениях и т. п.

В связи с этим актуализировалась задача обеспечения информационной безопасности (ИБ) именно технологических МИС. При этом необходимо отметить отсутствие к настоящему времени нормативной и методической основы для решения задач обеспечения ИБ информационных систем данного класса.

При построении методического обеспечения для обоснования требований к информационным системам является содержательный анализ угроз ИБ для них. Однако в известной литературе не содержится данных ни о модели угроз ИБ ни об их вероятностно временных характеристиках. В этой связи построение прогнозных моделей реализации угроз ИБ технологических МИС становится особенно актуальным.

Последовательность реализации угрозы ИБ можно представить, используя конфликтно-динамическую модель [1; 4]. При реализации угрозы можно выделить три этапа:

1. *Сбор информации* о топологии и принципах функционирования автоматизированной системы. 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 основных требований 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) [2].

Методический подход к формализации конфликтно динамических процессов, происходящих при НСД, позволяющих в дальнейшем решать задачу прогноза разработан в [3].

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.

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

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

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.

Для оценки параметров ν_i^j 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 обозначает конечную 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}.

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»).

Построение деревьев атак и оценку параметров v_i^j можно осуществить на основе анализа материалов [2], содержащих детальное описание способов реализации НСД.

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.

Список литературы

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

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

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

4. Прогностическая модель реализации угроз информационной безопасности технологическим медицинским информационным системам / В.П. Гулов,

В.А. Хвостов // Прикладные информационные системы медицины. – 2015. – Т. 18. – №2. – С. 3–10.