УДК 004.056.53

А.В. Нестеренко, И.Е. Нетесин

ГРАФОВАЯ МОДЕЛЬ КИБЕРБЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Ключевые слова: кибербезопасность, информационные ресурсы, угрозы, риски, онтологии, графовая модель.

Введение

В настоящее время существенно возросла актуальность обеспечения кибербезопасности информационных ресурсов, особенно государственных, в связи с обострением использования кибернетической компоненты в составе гибридных форм вмешательства в жизнедеятельность стран, распространением хакерских атак. Подобные действия могут нанести значительный ущерб органам государственного управления, которые являются владельцами или распорядителями информации и поддерживающей ее инфраструктуры, а также различным юридическим и физическим лицам — пользователям этой информации и государству в целом [1].

Увеличение количества автоматизированных систем, обеспечивающих хранение и обработку государственных информационных ресурсов, наличие в них различных уязвимостей и недостатков защиты влияет на рост количества и разнообразия угроз с одновременным ростом потерь от реализации этих угроз. Осведомленность владельца ресурса о возможных угрозах конкретной системе и связанных рисках создает условия для своевременного применения соответствующих контрмер и уменьшения рисков. В этом вопросе важное значение приобретает создание адекватной модели, которая отражала бы взаимосвязь угроз, значения (ценности) ресурсов, ожидаемых рисков и механизмов защиты [2–4].

Проведенный анализ выявляет существующую проблематику, связанную с тем, что построение подобной модели безопасности информационных ресурсов, которые поддерживаются органами управления, в частности в государственной сфере, сдерживается рядом факторов, среди которых недостаточность детального определения классификации угроз государственным информационным ресурсам [5], онтологических описаний операционно-процессных свойств ресурсов [6] и др.

В данном аспекте недостаток исследований взаимосвязи составляющих среды безопасности государственных информационных ресурсов, исследований на соответствие сложившимся условиям и возможность адаптации к происходящим изменениям, выступают той проблемой, которая требует рассмотрения.

Проблемы построения моделей безопасности среды информационных ресурсов, определение воздействий различного типа угроз и нарушителей и обеспечение защищенности ресурсов освещены в работах отечественных авторов В.Л. Бурячка, В.С. Василенко, В.В. Домарева, А. Б. Качинского, А.Я. Матова, А.Н. Новикова,

В.А. Устименко, В.А. Хорошко, А.К. Юдина и др. Среди зарубежных авторов выделяют Edward G. Amoroso, Siri Bromander, Bruce Schneier, Adam Shostack и др. В то же время дефицит учета в существующих моделях факторов, касающихся отношений понятий и объектов в сфере кибербезопасности, остается недостаточно изученной проблемой в определении приоритетов обеспечения безопасности.

До сих пор остаются нерешенными вопросы теоретического изучения и раскрытия подходов к описанию взаимосвязи угроз и различных свойств информационных объектов (ресурсов) для выбора средств защиты, необходимых для решения задач обеспечения безопасности. Перспективным считается представление моделей в виде графов [7–9], но и этот подход требует дальнейшего развития.

Цель данной статьи — изучение и исследование существующих подходов в процессе решения экспертами практических задач по обеспечению кибербезопасности, а также описание модели безопасности систем ведения информационных ресурсов на основе онтологий и графового представления.

Построение информационной модели предметной области

При определении понятий и объектов, относящихся к какой-либо области, а также отношений между ними, что является основой онтологического подхода, необходим учет формально-методологических требований, критериев и оценок. Основные из них [10]:

1) построение информационной и функциональной модели предметной области;

2) необходимость структурирования терминов, используемых для представления понятий и объектов;

3) правила формирования достоверных высказываний, утверждений и выводов, описывающих термины и понятия предметной области;

4) поддержка таксономий тематических онтологий предметной области.

Основным понятием информационной и кибербезопасности является угроза (Threat), которая может вызвать нештатные ситуации в системе. Также к комплексу понятий необходимо отнести и такие, как нарушитель (Violator), владелец ресурса (Proprietor of resource), уязвимость (Vulnerability), средства защиты (Facilities of defence), риски (Risks).

Используя международный стандарт ISO/IEC 15408 «Общие критерии оценки безопасности информационных технологий», можно показать специфику процессов, происходящих в условиях наличия угроз в среде информационных ресурсов. Эту специфику представим в виде графа процессов (обозначим G_P) (рис. 1). Вершинами графа являются основные понятия среды, а дугами — отношение между ними. Имена вершин обозначены первыми буквами соответствующих англоязычных названий.

Тогда граф G_P описывает такие процессы. Владелец ресурса (PR) оценивает (1) имеющиеся у него информационные ресурсы (IR) для определения их свойств (открытости, конфиденциальности и ценности для организации, учреждения). Нарушитель (V_i) создает (2) угрозу (T), которая порождает (3) риск (R) потери (4) ресурсом (IR) собственных свойств. В то же время угроза получает (5) выражение в виде атаки (A), которая, используя (6) уязвимости (V_u) системы, достигает негативных последствий активности. Между атаками нарушитель постоянно осуществляет поиск (8) новых уязвимостей в системе, которые могут появляться (9) в течение жизненного цикла ресурса.

Владелец ресурса, зная (10) о наличии риска потери ресурсом своих свойств, создает (11) средства защиты (FD), которые способны уменьшить (12) риски. Но средства защиты также могут иметь недостатки, поэтому нарушитель находит их и использует (13) для доступа (14) к ресурсу. В этих обстоятельствах владелец вынужден осуществлять постоянный мониторинг (15) уязвимостей систе-

мы для их своевременного выявления и тем самым уменьшения (16) рисков. В то же время необходимо принятие мер по оценке (17) состояния средств защиты для выявления и устранения недостатков защиты.

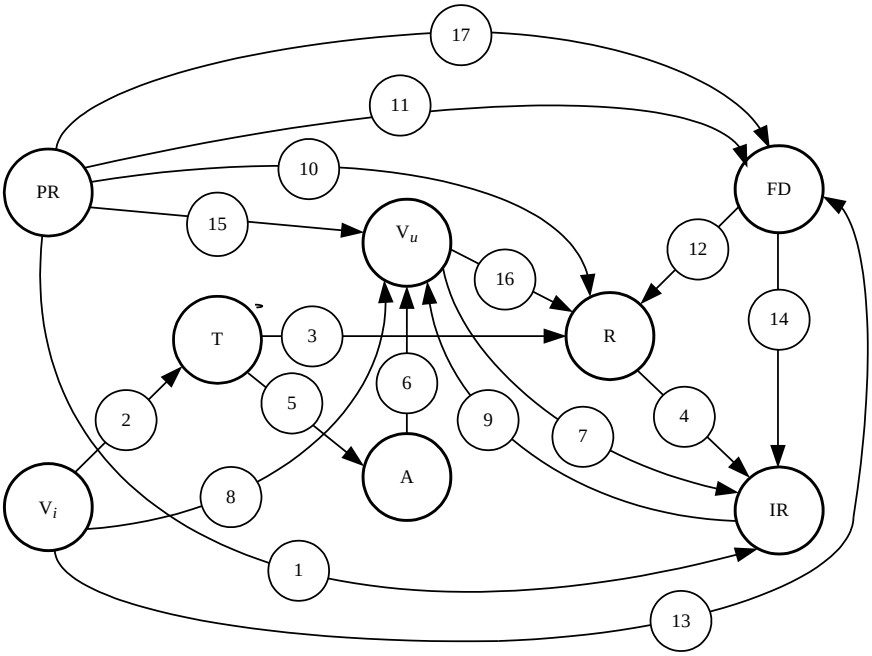

Рис. 1

Совокупности средств защиты, функционирующих совместно для выполнения определенной задачи предотвращения опасности (криптографические протоколы, средства защиты операционных систем и т.д.), соответствует термин механизм защиты.

Из рис. 1 видно, что на графе G_P вершины V_u и R относятся к наиболее нагруженным, что свидетельствует о значительной важности выявления уязвимостей в системе и их корреляций с уровнем рисков потери свойств ресурса. Из этого вытекает, что наличие уязвимостей вызывает и появление угроз (были бы уязвимости, а нарушитель всегда найдется). Иными словами, наличие уязвимостей создает окно опасности, которым могут воспользоваться нарушители для создания нештатной ситуации.

Для описания сферы кибербезопасности автоматизированной системы (АС) необходимо определить свойства защищенности ресурсов, которые с наибольшей вероятностью нарушаются вследствие воздействия угроз, т.е. осуществить идентификацию угроз в виде их перечня с указанием соответствия свойствам информационных ресурсов, на нарушение которых они направлены (нарушение конфиденциальности, целостности, доступности и пр.). Подобное описание целесообразно формировать на основе онтологий. В центре любой онтологии находится определенная классификация, которая описывает понятия предметной области [11].

В качестве примера для дальнейших исследований возьмем АС, которая поддерживает некоторый реестр государственной информации как справочно-поисковой системы массового обслуживания с открытой информацией, доступ к которой обеспечивается с официального сайта органа управления. По своему назначению и архитектурной реализации такую АС можно отнести к распреде-

ленным многомашинным многопользовательским комплексам, которые обрабатывают информацию разной степени ограничения доступа. Существенной особенностью этого класса систем является необходимость передачи информации через незащищенную среду (обычно Интернет).

Прежде всего рассмотрим общий случай классификации угроз и нештатных ситуаций, которые могут возникнуть относительно выбранной АС. Для анализа угроз ресурсам АС необходимо определение возможных каналов и видов угроз, которые могут быть реализованы в отношении системы или информации, а также анализ основных источников их происхождения.

Примером обобщенной классификации, описывающей существующие угрозы информационной безопасности, по которой каждая из угроз подпадает только под один классификационный признак, и которая вследствие этого наиболее применима для анализа рисков в реальных АС, является классификация Digital Security Classification of Threats, созданная специалистами компании Digital Security. Используя эту классификацию, онтологию угроз АС можно представить онтографом, приведеным на рис. 2.

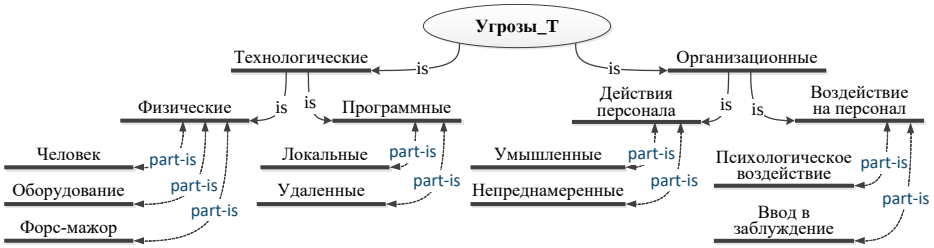

Рис. 2

Аналогичный подход применим и для классификационного описания ресурсов АС (рис. 3). Согласно принятой в теории защиты информации терминологии защищаемые ресурсы принято называть объектами защиты, или просто объектами.

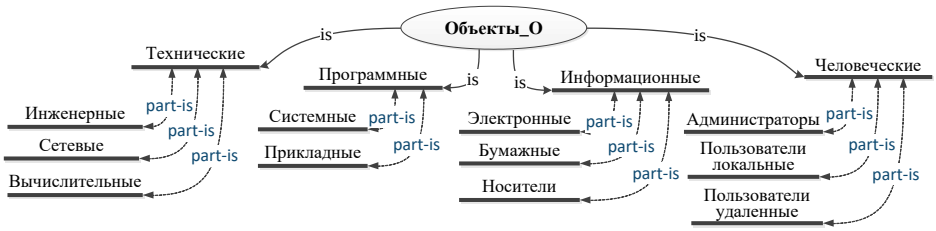

Рис. 3

Описание характеристик возможных угроз для выбранной АС приведено в табл. 1. Данное описание сформировано исходя из того, что для реализации угроз нарушитель может действовать дистанционно (через средства связи, утечки информации, средства специального воздействия техническим каналам) или непосредственно (в том числе и путем физического воздействия) на элементы системы. С использованием подобного подхода сформировано и описание ресурсов АС, представленное в табл. 2, где приведены оценки уровня ущерба.

В этих таблицах для упрощения дальнейшего изложения обозначения угроз и объектов даны в сокращенном упорядоченном виде.

Обычно оценка угрозы базируется, прежде всего, на вероятности ее возникновения. В отличие от такого подхода оценки угроз, приведенные далее в табл. 1, базируются на методологии нормативных документов и опыте мониторинга осуществления угроз в системах ведения государственных информационных ресурсов,

которые представлены в виде качественных оценок с использованием лингвистической переменной, принимающей значения: незначительная, низкая, высокая, очень высокая.

Таблица 1

Обозначение угрозы	Характеристика угроз (в соответствии с рис. 2)	Оценка возможности осуществления
Технологические / физические / человек		
T01	Нарушение физической целостности автоматизированной системы (АС) или ее отдельных компонентов, действия, приводящие к отказу АС или отдельных ее элементов из-за разрушения вычислительных ресурсов (в том числе процессоров и носителей данных), периферийного оборудования, в том числе телекоммуникационного	Незначительная
T02	Нарушение режимов функционирования (вывода из строя) систем жизнеобеспечения АС (инженерных коммуникаций)	Низкая
T03	Повреждения носителей информации	Высокая
Технологические / физические / оборудование		
T04	Перехват передаваемых данных, изменение (модификация) информации сообщений с использованием специального оборудования	Незначительная
T05	Прерывания передачи потока данных	Незначительная
T06	Нарушение режимов функционирования АС путем применения электромагнитного излучения	Низкая
Технологические / физические / форс-мажор		
T07	Изменение условий физической среды вследствие стихийного бедствия (землетрясение, наводнение, пожар, аварии водопровода)	Незначительная
T08	Сбои и отказы в работе технических средств АС вследствие аварийного отключения питания	Низкая
T09	Влияние природных и технических электромагнитных помех (грозовые разряды, искрение в электросетях во время электросварки и т.д.)	Низкая
Технологические / программные (локальные и удаленные)		
T10	Модификация программного обеспечения (локальная)	Низкая
T11	Модификация программного обеспечения (удаленная)	Низкая
T12	Внедрение и использование компьютерных вирусов (локальное)	Высокая
T13	Внедрение и использование компьютерных вирусов (удаленное)	Высокая
T14	Доступ к данным с нарушением установленных правил разграничения доступа в целях ознакомления, модификации, копирования, уничтожения данных и т.п. (локальный)	Низкая
T15	То же (удаленный)	Низкая
T16	Получение защищенных данных с помощью специально организованной серии санкционированных запросов (локальное)	Низкая
T17	То же (удаленное)	Низкая
T18	Несанкционированное изменение полномочия других пользователей (локальное)	Низкая
T19	То же (удаленное)	Низкая
T20	Выдача собственных несанкционированных запросов под запросы операционной системы	Низкая
T21	Неправомерное изменение режимов работы АС (ее отдельных компонентов, оборудования, программных средств и т.п.), инициирование технологических или тестирующих процессов, которые способны привести к необратимым изменениям в системе (локальное)	Низкая
T22	То же (удаленное)	Низкая

Продолжение таблицы 1

Организационные / действие персонала / умышленные		
T23	Получение атрибутов доступа с последующим их использованием для маскировки под зарегистрированного пользователя	Низкая
T24	Несанкционированное копирование носителей информации	Очень высокая
T25	Кражи носителей информации, производственных отходов (распечаток, записей и т.д.)	Высокая
T26	Фальсификация фактов формирования и выдачи данных	Низкая
T27	Подтверждение получения от некоторого пользователя данных, сформированных самим нарушителем	Низкая
T28	Подтверждение передачи какому-нибудь пользователю данных, которые не передавались	Низкая
T29	Фальсификация фактов получения данных	Низкая
T30	Внедрение и использование запрещенного политикой безопасности программного обеспечения (ПО) или несанкционированное использование ПО, с помощью которого можно получить доступ к критической информации	Высокая
T31	Раскрытие содержания данных в каналах связи	Высокая
Организационные / действие персонала / непреднамеренные		
T32	Ошибки при вводе данных в систему, выдачи данных по неверным адресам внутренних и внешних абонентов и т.д.	Высокая
T33	Невыполнение организационных мероприятий относительно порядка и правил эксплуатации или использования ресурсов АС, предусмотренных политикой безопасности, должностными или иными, в том числе технологическими, инструкциями	Низкая
T34	Некомпетентное применение средств защиты	Низкая
T35	Неумышленное заражение ПО компьютерными вирусами	Низкая
Организационные / воздействие на персонал / психологическое воздействие		
T36	Использование персонала АС (шантаж, подкуп) с корыстной целью	Незначительная
Организационные / воздействие на персонал / ввод в заблуждение		
T37	Закладка ложных решений при проектировании, разработке и модификации компонентов АС (технических средств, технологии обработки информации, ПО, средств защиты, структур данных и т.д.)	Низкая

Для обобщения и упрощения модели оценки ущерба ресурсов, приведенные в табл. 2, осуществлены также по качественной шкале (низкая, средняя, высокая, недопустимо высокая).

Обычно оценка уровня ущерба, нанесенного ресурсу вследствие реализации угрозы, рассматривается как ожидаемые убытки в стоимостном выражении, что достаточно сложно. В предлагаемой модели уровень ущерба оценивается на основе относительной ценности ресурсов, определяемой экспертным путем в рамках одной системы. Чем выше ценность ресурса относительно других ресурсов, тем больше ущерб от реализации угрозы. При этом для упрощения модели принимается, что любая угроза, направленная на ресурс, наносит ему одинаковый ущерб.

Приведенный подход выбора качественных шкал связан с широко известным положением теории систем: чем выше степень неопределенности объекта, который моделируется, тем проще должна быть его модель, кроме того, чем сложнее модель, тем сложнее обеспечить ее входными данными [12]. Таким образом, при отсутствии точных входных данных упрощенные или, как их еще называют, «грубые» модели оказываются более действенными.

Таблица 2

Обозначения объекта	Объекты (в соответствии с рис. 3)	Оценка уровня ущерба
Технические инженерные		
О01	Инженерные коммуникации электропитания	Недопустимо высокий
О02	Инженерные коммуникации охлаждения	Недопустимо высокий
О03	Инженерные коммуникации водоснабжения	Средний
Обозначения объекта	Объекты (в соответствии с рис. 3)	Оценка уровня ущерба
Технические вычислительные		
О04	Серверы	Недопустимо высокий
О05	Персональные компьютеры	Высокий
О06	Периферийное оборудование	Средний
Технические сетевые		
О07	Сетевое оборудование локальных сетей (кабельная сеть, коммутаторы и др.)	Высокий
О08	Сетевое оборудование наружных сетей (кабельные линии, маршрутизаторы и др.)	Высокий
Программные системные		
О09	Операционные системы, системы управления базами данных (СУБД)	Высокий
О10	ПО комплекса средств защиты	Недопустимо высокий
Программные приложения		
О11	Клиентское ПО	Низкий
Информационные электронные		
О12	Базы данных (БД), файлы	Недопустимо высокий
Информационные бумажные		
О13	Техническая и эксплуатационная документация	Низкий
О14	Документация по информационной безопасности	Средний
Информационные носители		
О15	Сменные носители с архивной информацией	Высокий
Человеческие		
О16 О17	Пользователи локальные, удаленные	Высокий
О18	Администраторы	Недопустимо высокий

Модель взаимодействия угроз, ресурсов и механизмов защиты

Представим модель отношений множества угроз T и множества объектов O двудольным графом $G = (V(T, O),\ T(T, O))$ (рис. 4), в котором множества вершин его долей $T \cup O = V(T, O)$, $T = \{T01, T02, ..., T37\}$, $O = \{O01, O02, ..., O18\}$, $T \cap O = \varnothing$ и множество ребер $E(T, O)$, в котором ребро $(T_p, O_q) \in E(T, O)$, если есть угроза T_p объекту O_q. Направленность угрозы T_p к конкретному объекту O_q определяется на основе описаний табл. 1 и 2.

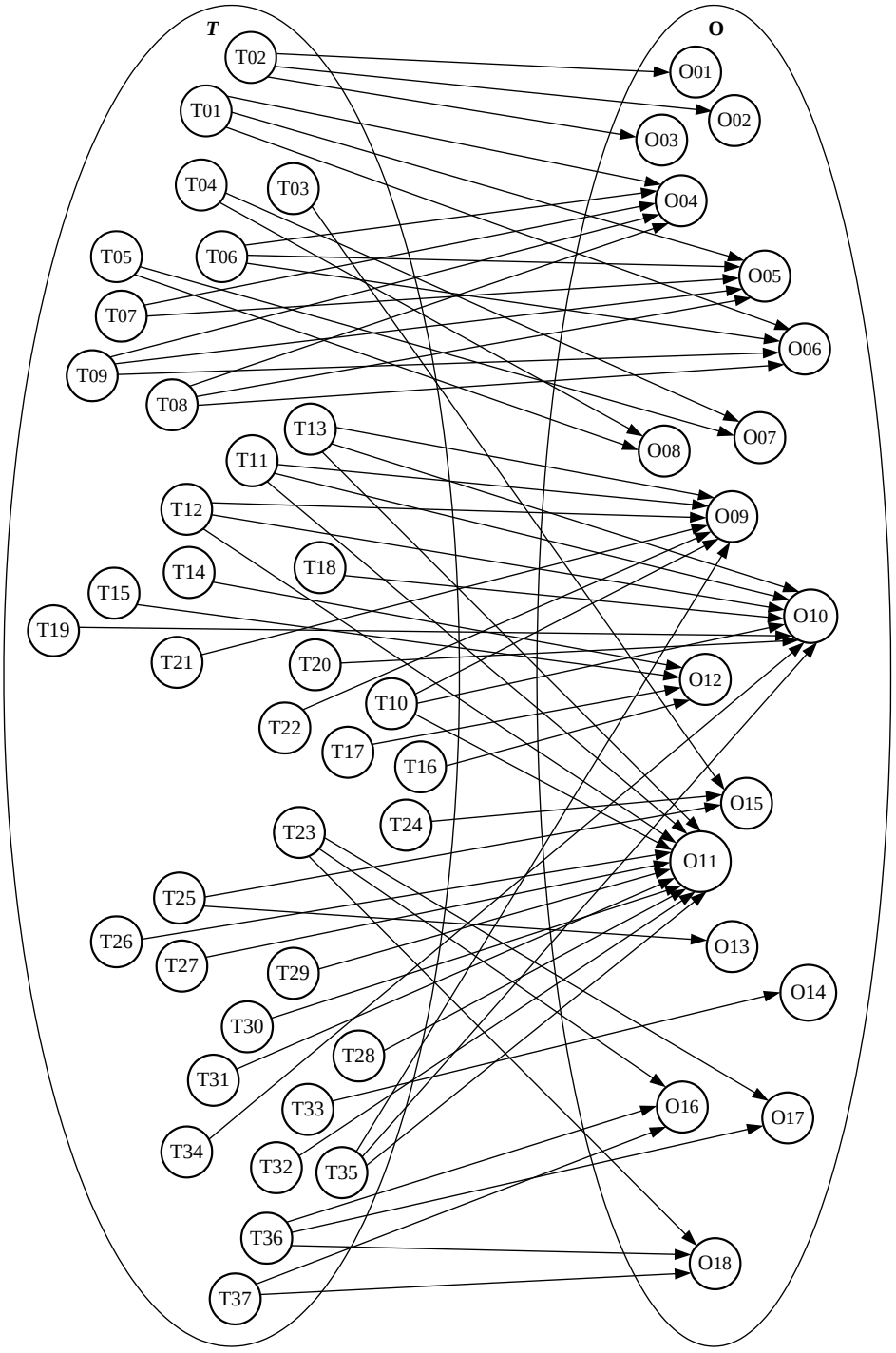

Рис. 4

В общем случае из модели угроз вытекает необходимость защиты всех свойств информации от воздействия угроз, и прежде всего, от воздействия угроз, следствием реализации которых может быть недопустимо высокий или высокий уровень вреда, поскольку такие угрозы имеют комплексный характер, т.е. одновременное воздействие на несколько свойств защищенности. Такие угрозы принято называть наиболее существенными (более опасными).

Выявление наиболее существенных угроз и высокого уровня ущерба, нанесенного ресурсу, является основой для определения в дальнейшем нужных средств защиты, а следовательно, определение состава необходимых контрмер для обеспечения допустимой защищенности, необходимых для защиты средств, подсистем, механизмов и функций защиты, т.е. позволяет строить соответствующие модели систем защиты.

В соответствии с известной моделью безопасности с полным перекрытием [13], которая строится, исходя из положения, что система безопасности должна иметь, по крайней мере, одно средство для обеспечения безопасности на каждом возможном пути действия угрозы на объект, в данной модели появляется третий набор, описывающий механизмы защиты $M = \{M_r\},\ r-1, ..., |M|,$ где $|M|$ — количество механизмов.

В идеальном случае каждый механизм M_r должен устранять одно или несколько ребер (T_p, O_q). На практике M_r выполняет функцию «барьера», обеспечивая некоторую степень сопротивления попыткам реализации угрозы. Включение в модель множества M превращает граф G_{TO} в трехдольный граф $G_{TMO} = (V(T, M, O),\ E(T, M),\ E(M, O))$.

Применим онтологический подход для описания механизмов защиты АС (рис. 5). Представим описание механизмов защиты, предлагаемых для выбранной системы, с учетом оценки эффективности применения механизма в системе (табл. 3). Эта оценка может базироваться и на стоимости создания комплекса средств защиты (КСЗ) как совокупности программно-аппаратных средств, обеспечивающих реализацию механизмов защиты, локализованных в системе в виде одного или нескольких аппаратных и/или программных компонентов.

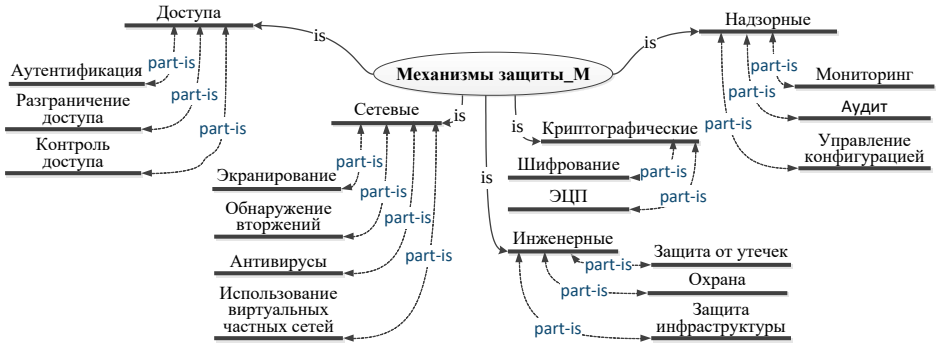

Рис. 5

Для определения приоритетности построения средств защиты объектов системы предлагается осуществить разбиение специальным образом всех объектов системы (первоначального графа) на подсистемы (подграфы) и определить относительные риски этих подсистем в пределах общей системы, чтобы решить, каким подсистемам надо уделить первоочередное внимание для повышения их уровня защищенности.

Для осуществления процесса разбиения найдем на графе G_{TO} его компоненты связности, т.е. такие его подграфы $G_i = (V_i, O_i)$, что $\cup G_i = G_{TO}$, но $V_i \cap V_j = \varnothing$ и $E_i \cap V_j = \varnothing$, $i, j = 1, 2, ..., i \neq j$, в то время как в любом G_i любые вершины u и v соединены простой цепью. Стрелочки на ребрах графа G_{TO} указывают лишь на то, что опасность исходит со стороны угроз к объектам и выполняют чисто иллюстративную функцию. Поэтому можно рассматривать граф G_{TO} как неориентированный.

Таблица 3

Имя узла графа	Механизмы	Оценка эффективности
Доступа		
M01	Аутентификация	средняя
M02	Разграничение доступа	средняя
M03	Контроль доступа	высокая
Сетевые		
M04	Экранирование	значительная
M05	Обнаружения вторжений	значительная
M06	Антивирусы	высокая
M07	Использование виртуальных частных сетей	средняя
Криптографические		
M08	Шифрование	высокая
M09	Применение электронной цифровой подписи (ЭЦП)	средняя
Надзорные		
M10	Мониторинг	средняя
M11	Аудит	высокая
M12	Управление конфигурацией	значительная
Инженерные		
M13	Защита от утечек	средняя
M14	Охрана	высокая
M15	Защита инфраструктуры	значительная

Для нахождения компонент связности возможно применение известных методов. Большинство алгоритмов на графах использует их представления с помощью матрицы смежности или списков смежных вершин. Матрица смежности D графа с n вершинами является матрицей порядка $n \times n$, в которой ее элемент $x_{ij} = 1$, если вершина u_i соединена ребром с вершиной vj, иначе $x_{ij} = 0$. При задании графа списком смежных вершин для каждой вершины задается список вершин, соединенных с ней ребрами.

В случае представления графа с помощью списков смежных вершин для поиска компонент связности обычно применяют методы, основанные на алгоритмах поиска в глубину и поиска в ширину, исследующих граф методом обхода всех вершины и ребер, используя механизмы рекурсии, покраски вершин или ребер, понятия предков и потомков, меток времени и т.д. [14, 15].

Количество операций для поиска в глубину или в ширину, а также для поиска компонент связности, которые основаны на этих алгоритмах, пропорционально количеству вершин и ребер, вместе взятых, поэтому составляет O (V + + E), где константа, скрытая в обозначении O (O большое), не превышает

нескольких десятков [12, 13]. $|V|$ и $|E|$ — количество соответственно вершин и ребер во множествах V и E.

Приведем стандартное описание G_{TO} с помощью списков смежных вершин:

T01: O04, O05, O06;
T02: O01, O02, O03;
T03: O15;
...
T37: O16, O18;
O1: T02;
…
O10: T13, T11, T12, T10, T18, T19, T20;
…
O18: T23, T36, T37.

В случае задания графа матрицей смежности D можно применить алгоритмы, которые превращают ее в блочно-диагональную матрицу B вида

$$\begin{pmatrix} B_{11} & & 0 \\ & \ddots & \\ 0 & & B_{ii} \end{pmatrix},$$

где B_{ii} — матрица смежности, соответствующая отдельным компонентам связности исходного графа.

Это достигается, например, умножением матрицы D на некоторую матрицу перестановки P и ее обратную матрицу P^{-1}, т.е. $B = P^{-1}DP$ [16]. Другой способ получения из матрицы смежности блочно-диагональной матрицы B — применение алгоритма, который использует вектор указателей, содержащий последовательность перестановок строк и столбцов матрицы D [17].

Количество операций в алгоритмах, которые используют матричное представление, составляет $O(V)^2$. Переход от одного представления к другому может быть выполнен также за $O(V)^2$. операций [13].

Применяя один из приведенных алгоритмов, получаем искомые компоненты связности $G_i = (V_i, E_i)$ графа G_{TO} (рис. 6).

Теперь, рассматривая приведенные подграфы G_i, определение необходимых механизмов защиты из набора M очевидно значительно упрощается. Но остается проблема оценки эффективности реализации выбранных механизмов защиты и приоритетности их реализации для определенных объектов. Для этого традиционно известным является установление, прежде всего, оценок рисков поражения ресурсов, которые следуют из оценок возможности осуществления угроз и уровня вреда (ущерба) от поражения. Ниже в качестве оценок предлагается использовать экспертные оценки, приведенные в табл. 1 и 2. Для этого качественные оценки возможности осуществления угроз представим в количественном (бальном) измерении по такой условной схеме: незначительная возможность — 1, низкая — 3, высокая — 7, очень высокая — 9 баллов.

Аналогично для предварительных оценок ущерба будем использовать также шкалу по схеме: низкий ущерб — 20, средний — 50, высокий — 70, недопустимо высокий — 90 баллов.

Данные оценки носят относительный характер, поэтому и оценки рисков поражения объектов также будут относительными между объектами конкретной системы.

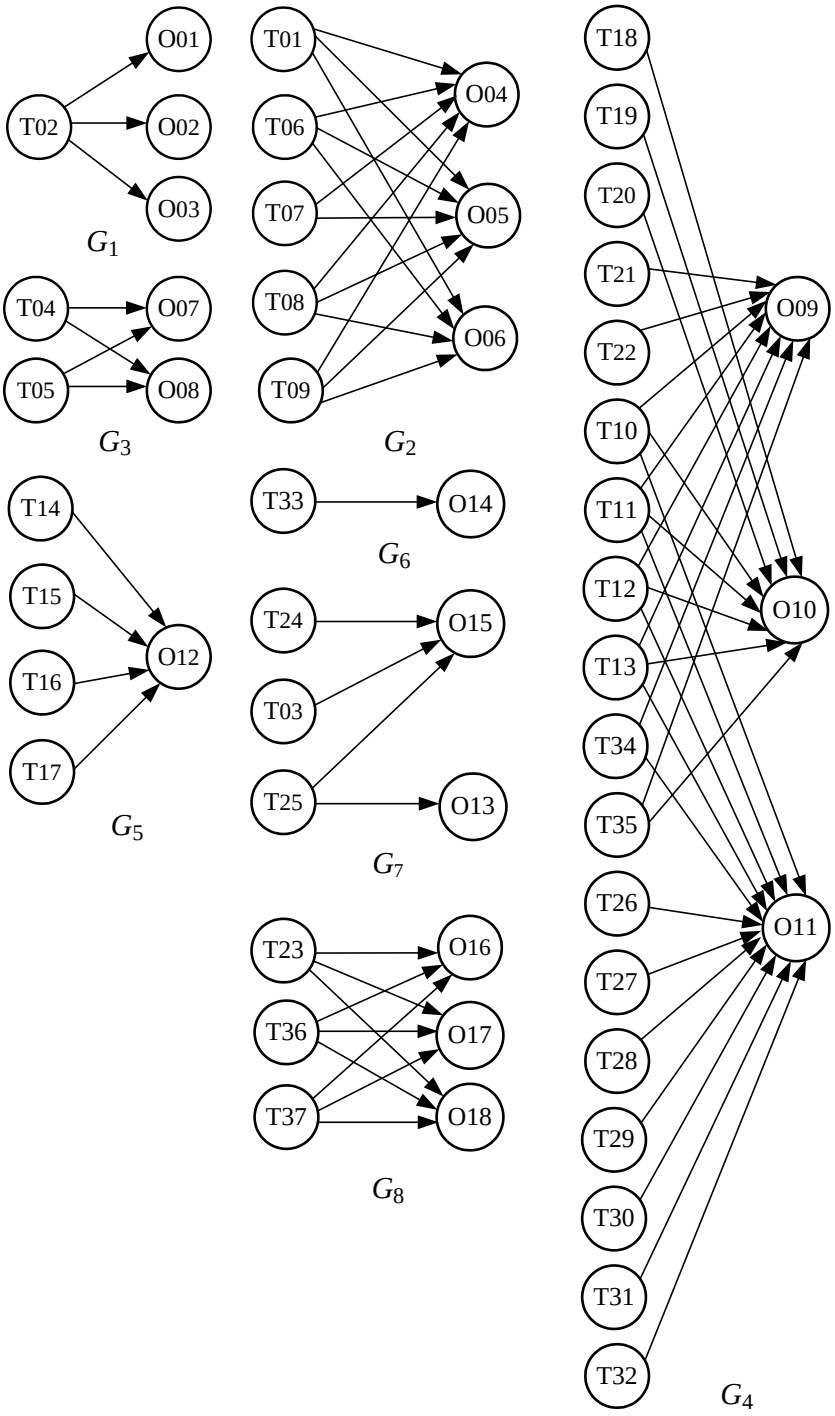

Рис. 6

Отметим, еще раз, что выбор и соотнесение измерительных шкал, вообще говоря, — прерогатива экспертов, поэтому в дальнейшем это нивелируется нормированием.

Для решения вышеобозначенной проблемы предлагается алгоритм, который в конечном итоге приводит к получению оценок рисков объектов, входящих в подграфы и защищенных выбранными механизмами (рис. 7). Необходимо отметить,

что данный алгоритм, как и весь подход в целом, рассматривает случай, когда система допускает разбиение объектов минимум на две подсистемы.

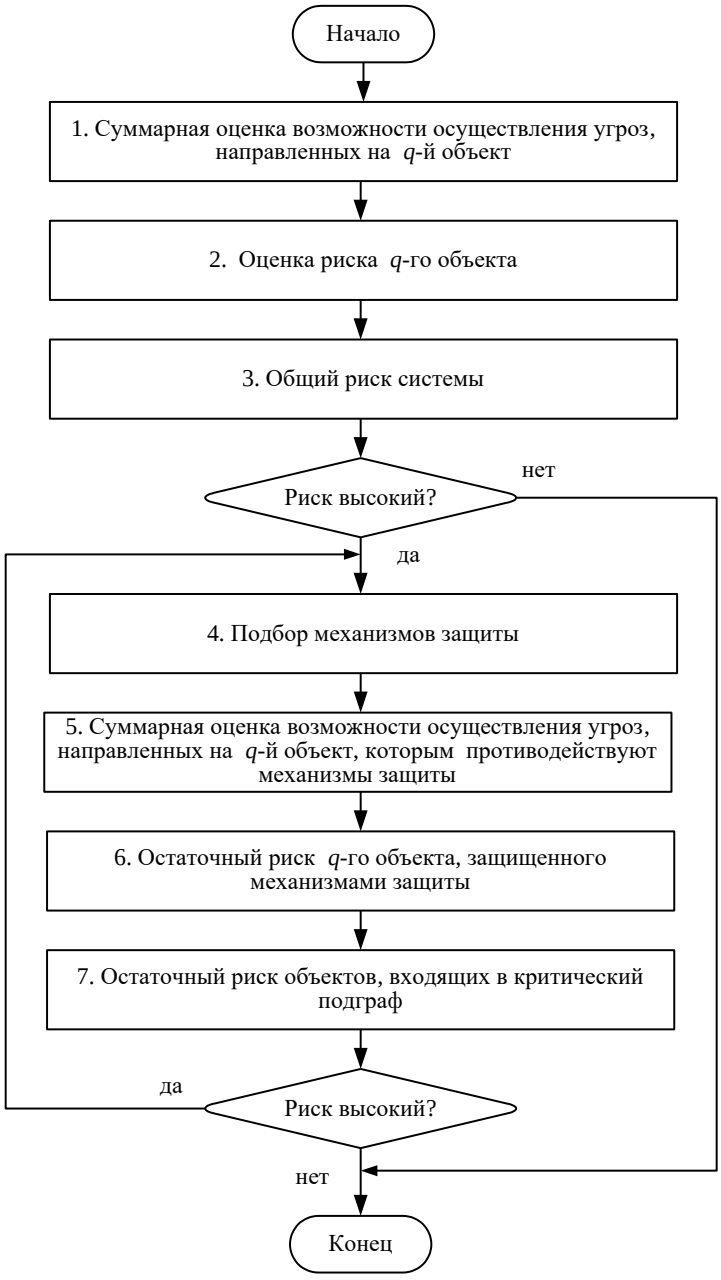

Рис.7

Рассмотрим подробнее шаги алгоритма.

1. В условиях, когда каждый ресурс (объект) может подпадать под действие нескольких угроз, определим суммарную оценку C_q возможности осуществления угроз, направленных на q-й объект:

$$C_q = \sum_p A_p, \tag{1}$$

для $\{\forall p \mid \exists (T_p, O_q)\}$, где A_p — оценка возможности осуществления p-й угрозы (согласно табл. 1).

Проведем нормирование величин C_q для получения их относительных величин $\tilde{C}_q$ в интервале (0, 1) :

$$\tilde{C}_q = \frac{C_q}{\sum_{k=1}^{|O|} C_k}, \tag{2}$$

где $|O|$ — количество объектов в системе.

2. По аналогии с одним из наиболее распространенных подходов к количественному определению риска как произведения размера потерь на вероятность наступления рискового события, в данном случае относительную оценку S_q риска q-го ресурса, можно рассчитывать по следующему выражению:

$$S_q = L_q \tilde{C}_q, \tag{3}$$

где L_q — оценка уровня ущерба, наносимого q-му ресурсу (согласно табл. 2).

При совместной реализации угроз уровень общего ущерба не всегда может быть равен сумме ущербов, так как они могут быть коррелированны. Поэтому, в отличие от вероятностного подхода, в предлагаемом подходе оценивается риск поражения от осуществления всех угроз в зависимости от бальных оценок возможностей их осуществления, что в целом не должно существенно повлиять на общую оценку рисков, исходя из приведенного выше допущения о целесообразности использования грубых моделей в случае отсутствия достаточной информации о взаимосвязи угроз и ресурсов.

Результаты расчетов по оценке рисков, которые используют количественные балльные оценки и проведены по формулам (1)–(3), могут быть представлены в виде таблиц или диаграмм. Из данных диаграммы, приведенной на рис. 8, следует, что к объектам, которые имеют высокий риск поражения, относятся (первая тройка): О10 — 13,64, О09 — 8,79, О11 — 5,11. Приведенные ресурсы входят в подграф G_4, который имеет из всех подграфов наивысшую оценку риска 27,53 — как сумму рисков, входящих в него объектов (рис. 9).

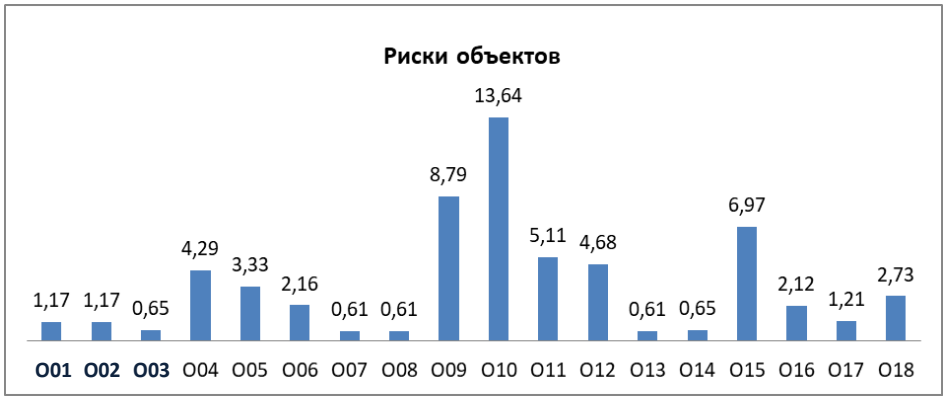

Рис. 8

3. Общий риск системы вычисляется как сумма всех S_q и равен 60,48. Таким образом, оценка общего риска системы находится в интервале между 50 и 70 и определяет риск, в сравнении с оценками ущерба, как близкий к высокому, что свидетельствует о необходимости применения (усиления) средств защиты, в первую очередь, объектов с высокими рисками.

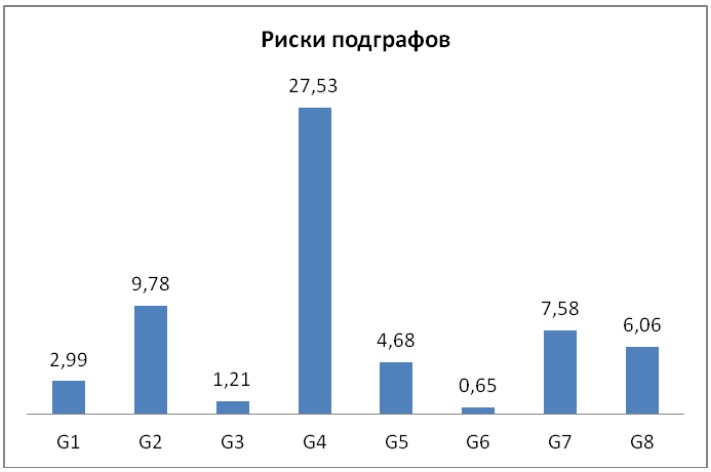

Рис. 9

4. Для оценки защиты этих объектов выбранными механизмами защиты построим для критического подграфа G_4 трехдольный граф (рис. 10). Выбор механизмов осуществляется экспертами исходя из сущности угроз (табл. 1) и соответствующей функциональности механизмов защиты (табл. 3). Например, для вирусной угрозы выбирается механизм антивирусной защиты, для несанкционированного доступа — механизм аутентификации и т.д.

Качественные оценки эффективности механизмов защиты представим в количественном измерении в процентах, а именно: средняя — 50 %, высокая — 70 %, значительная — 90 %.

5. Исходя из того, что каждый механизм защиты может противодействовать нескольким угрозам, определим суммарную оценку $C_q^{(r)}$ возможности осуществления угроз, направленных на q-й объект, которым противодействует r-й механизм:

$$C_q^{(r)} = \sum_p A_p \qquad (4)$$

для $\{\forall p \,|\, \exists(T_p, M_r)\ \&\ (M_r, O_q)\}$.

Проведем нормирование величин $C_q^{(r)}$:

$$\overline{\overline{C_q^{(r)}}} = \frac{C_q^{(r)}}{\sum\limits_{k=1}^{|O|}\sum\limits_{j=1}^{|M|} C_k^{(j)}}. \qquad (5)$$

6. Тогда остаточный относительный риск $\overline{\overline{S_q}}$ объекта q, защищенного механизмами M_r, рассчитывается по формуле

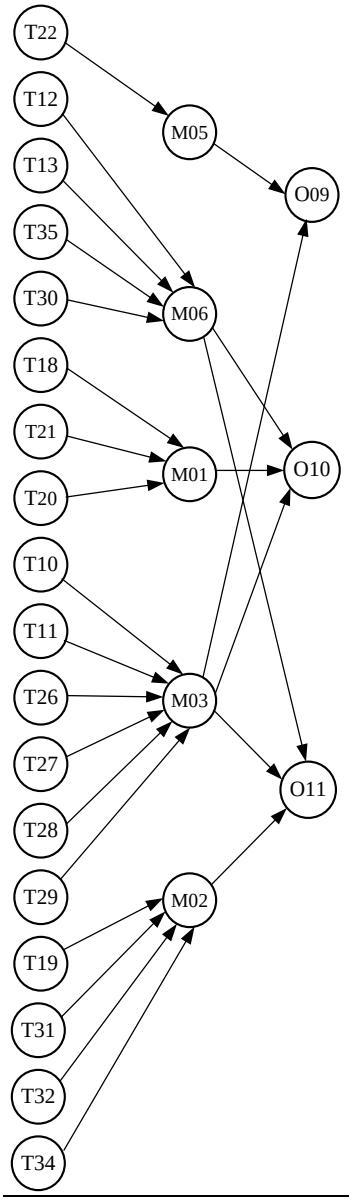

Рис. 10

$$\overline{\overline{S_q}} = L_q \sum_r \overline{\overline{C_q^{(r)}}} \left(1 - F_r / 100\right) \quad (6)$$

для $\{\forall r \mid \exists (M_r, O_q)\}$, где F_r — эффективность r-го механизма (по табл. 3).

7. Остаточный риск объектов, входящих в подграф G_i, равняется:

$$\overline{\overline{S}}(G_i) = \sum_q \overline{\overline{S_q}} \quad (7)$$

для $\{\forall q \mid O_q \in G_i\}$.

В результате проведенных расчетов по формулам (4)–(7) остаточные риски объектов, входящих в подграф G_4 и защищенных выбранными механизмами, оцениваются: для O09 — 3,09, для O10 — 4,44, для O11 — 2,83, а суммарный остаточный риск этих объектов оценивается величиной 9,36, что значительно меньше (на 18,17) оценки, полученной ранее для этих же, но незащищенных, объектов (27,53).

Результаты расчетов дают основание оценить уровень защищенности этих ресурсов выбранными механизмами как достаточно высокий. Реализация механизмов защиты даже для одного критического подграфа позволяет снизить общий риск системы с 60,48 до 42,31, что в сравнении с уровнем ущерба ниже среднего.

Следует подчеркнуть, что данный метод не предполагает сравнение общих рисков разных систем, а именно, направлен на сравнение рисков подсистем отдельной системы в целях определения приоритетности их защиты механизмами. При этом существенно не количество механизмов, обеспечивающих защиту, а их функциональность, т.е. возможность противостоять выявленным угрозам.

В то же время при проектировании комплекса средств защиты АС полученные результаты дают основание для принятия решения о возможном выборе альтернативных механизмов, например более дешевых, если есть ограничения по бюджету, либо об интеграции разрозненных механизмов защиты (как в приведенном примере — M01, M02, M03, M05, M06) в комплексный барьер, сочетающий функционал указанных механизмов.

Заключение

Предложенная модель кибербезопасности автоматизированных систем ведения информационных ресурсов (объектов) на основе графов для представления взаимодействия различного типа угроз и ресурсов и проведенные на ее основе расчеты свидетельствуют о простоте и удобстве ее применения, предоставляя эффективный инструмент экспертам и разработчикам средств защиты. Показано, что применение элементов онтологических описаний повышает уровень конкретизации модели и дает более четкое представление о состоянии среды безопасности автоматизированной системы.

Основная идея предлагаемого подхода — разбиение исходной системы, представленной графом отношений угроз и объектов, на подсистемы (подграфы — компоненты связности), и определение относительных рисков этих подсистем в пределах общей системы для того, чтобы выяснить, каким подсистемам надо уделить первоочередное внимание для повышения их уровня защищенности. Для этого предложен алгоритм, по которому рассчитываются относительные риски подсистем, исходя из которых экспертным путем выбираются механизмы защиты.

Применение предложенного подхода к оценке безопасности систем ведения информационных ресурсов способствует определению приоритетов выбора механизмов защиты, что важно при построении комплекса средств защиты автоматизированной системы.

Учитывая, что статья не охватывает ряд важных аспектов затронутой проблемы, направлениями дальнейших исследований должно быть рассмотрение вопросов, связанных со случаями влияния поражения некоторого ресурса на работоспособность других ресурсов, а также с оценкой сравнительной стоимости механизмов защиты по отношению к уровням рисков, особенно когда конкретный механизм обеспечивает защиту нескольких видов ресурсов.

О.В. Нестеренко, І.Є. Нетесін

ГРАФОВА МОДЕЛЬ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ РЕСУРСІВ

В умовах наростаючої активності кібератак на автоматизовані інформаційні системи усе більшої актуальності набуває задача визначення пріоритетності побудови засобів захисту. Запропоновано модель для розв'язання цієї задачі, що ґрунтується на онтологічному описі і графовому поданні середовища безпеки системи. Побудовано онтології загроз, ресурсів (об'єктів) та механізмів захисту. В основу запропонованого підходу покладено побудову і розбиття графа відношень загроз і об'єктів системи на підграфи (підсистеми) як компоненти зв'язності вихідного графа з подальшим знаходженням відносних ризиків ураження цих підсистем в межах загальної системи з метою з'ясування, яким підсистемам треба приділити першочергову увагу для підвищення їх рівня захищеності. Оцінки ризиків ураження ресурсів визначаються, виходячи з оцінок можливості здійснення загроз і оцінок рівня шкоди (збитків) від ураження. Для цього пропонується використовувати бальні експертні оцінки. Розроблено алгоритм, за яким розраховуються відносні ризики підсистем. Дано аналітичні вирази і на прикладі проведено розрахунки ризиків ураження об'єктів для системи без урахування розбиття на підсистеми і з урахуванням розбиття, що дозволяє визначати критичні для захисту підсистеми. Показано, що застосування моделі дає більш чітке уявлення про взаємодію загроз і ресурсів системи, допомагає знаходити найбільш значні уразливості системи і шукати шляхи поліпшення її захищеності в процесі вирішення практичних завдань із забезпечення кібербезпеки. Проведені розрахунки підтверджують коректність і адекватність запропонованої моделі, її простоту і зручність застосування, надаючи ефективний інструмент експертам і розробникам комплексів засобів захисту автоматизованих інформаційних систем.

Ключеві слова: кібербезпека, інформаційні ресурси, загрози, ризик, онтології, графова модель.

A.V. Nesterenko, I.E. Netesin

CYBER SECURITY GRAPH MODEL OF INFORMATION RESOURCES

With the growing activity of cyberattacks on automated information systems, the task of determining the priority of building protective equipment is becoming increasingly relevant. The model for solving this problem, based on the ontological description and graph representation of the system security environment, is proposed. The ontologies of threats, resources (objects) and protection mechanisms are developed. The proposed approach is based on construction and partitioning of the graph of the relations of threats and system objects into subgraphs (subsystems) as connected components of the original graph with subsequent finding the relative risks of the damage of

these subsystems within the overall system in order to find out the subsystems should be given priority to increase their security level. The risks assessments of resources damage is determined on the basis of expert threat scores and expert scores of the level of harm (loss) from damage. The algorithm has been developed by which the relative risks of subsystems are calculated. Analytical expressions are given and the example is used to calculate the risks of damage of the objects for the system without the partition into subsystems and taking into account the partition, to detect critical subsystems for protection. Application of the model gives the clearer picture of the interaction of threats and system resources, helps to find the most significant vulnerabilities of the system and to look for ways to improve its security in the process of solving practical tasks to ensure cybersecurity. The performed calculations confirm the correctness and adequacy of the proposed model, its simplicity and ease of use, providing an effective tool for experts and developers of security systems for automated information systems.

Keywords: cyber security, information resources, threat, risk, ontology, graph model.

1. Нестеренко О.В. Безпека інформаційного простору державної влади. Технологічні основи. Киев : Наук. думка, 2009. 352 с.
2. Шевченко В.Л., Нестеренко О.В., Нетесін І.Є., Шевченко А.В. Прогностичне моделювання комп'ютерних вірусних епідемій. Київ : *УкрНЦ РІТ*. 2019. 152 с.
3. Качинський А. Б. Безпека, загрози і ризик: наукові концепції та математичні методи. Київ : Інститут проблем національної безпеки; Національна академія служби безпеки України, 2004. 472 с.
4. Нетесин И.Е. Модели безопасности и зашиты в распределенных компьютерных средах. *Проблемы программирования*. 2000. № 3–4. С. 148–158.
5. Юдін О.К., Бучик С.С. Державні інформаційні ресурси. Методологія побудови класифікатора загроз. Київ : НАУ. 2015. 214 с.
6. Стрижак О.Є. Онтологічні інформаційно-аналітичні системи. *Радіоелектронні і комп'ютерні системи*. 2014. № 3 (67). С. 71–76.
7. Качинський А.Б., Ткач В.М., Поденко А.А. Ієрархія факторів типових сценаріїв реалізації DDos-атак. *Математичне моделювання в економіці.* 2017. № 1–2. С. 17–30, 2018. № 1. С. 31–48.
8. Хнигічева А.М., Новіков О.М., Тимошенко А.О. Моделювання безпеки складних інформаційно-комунікаційних систем із використанням логіко-ймовірнісного методу. *Наукові вісті Національного технічного університету України «Київський політехнічний інститут»*, 2010. Вип.6. С. 70–77.
9. Пустовіт О.С., Устименко В.О. Про застосування алгебраїчної комбінаторики до проблем кодування та криптографії. *Математичне моделювання в економіці*. 2017. № 1–2. С. 31–46.
10. Палагин А.В., Петренко Н.Г. К вопросу системно-онтологической интеграции знаний предметной области. *Математические машины и системы*. 2007. № 3, 4. С. 63–75.
11. Nesterenko O., Trofymchuk O. Patterns in forming the ontology-based environment of information-analytical activity in administrative management. *Eastern-European Journal of Enterprise Technologies*. 2019. **101**, N 5/2. P. 33–42. DOI**:** 10.15587/1729-4061.2019.180107.
12. Пригожин И. Стенгерс И. Порядок из хаоса: Новый диалог человека с природой. М. : Прогресс. 1986. 432 с.
13. Хоффман Л. Дж. Современные методы защиты информации. М. : Сов. радио. 1980. 264 с.
14. Кормен Т., Лейзерсон Ч. , Ривест Р., Штайн К. Алгоритмы. Построение и анализ. М. : Санкт-Петербург; Киев: Издательский дом «Вильямс». 2013. 1296 с.
15. Рейнгольд Э., Нивергельт Ю., Део Н. Комбинаторные алгоритмы. Теория и практика. М. : Мир. 1980. 478 с.
16. Харари Ф. Теория графов. М. : Мир. 1973. 302 с.
17. Берзтисс А.Т. Структуры данных. М. : Статистика. 1974. 408 с.

Получено 12.02.2020
После доработки 20.03.2020