УДК 004.056

ОПТИМИЗАЦИЯ ПОИСКА УЯЗВИМОСТЕЙ В СИСТЕМЕ ЗАЩИТЫ РЕСУРСОВ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ СЕТИ УНИВЕРСИТЕТА

[1]Надеждин Е.Н., [2]Новикова Т.Л.

[1]Тульский государственный педагогический университет имени Л.Н. Толстого, Тула, e-mail: en-hope@yandex.ru;

[2]Шуйский филиал Ивановского государственного университета, Шуя, e-mail: tshershakova@mail.ru

Статья посвящена проблеме поиска и нейтрализации уязвимостей в программном обеспечении корпоративной информационной сети образовательной организации в процессе внутреннего аудита информационной безопасности. Основное внимание уделено двум задачам, занимающим особое место в деятельности аудитора: задаче автоматической классификации выявленных уязвимостей и задаче определения наилучшего плана их нейтрализации путём выбора наилучших способов защиты информации. Предложена модель задачи автоматической классификации уязвимостей и способ её реализации на основе решения оптимизационной задачи дискретного программирования. Обоснована модель задачи выбора предпочтительного плана распределения механизмов защиты между выявленными уязвимостями, которая сведена к формулировке обобщённой задачи о назначениях. Рассмотрен пример решения комбинаторной задачи о назначениях с нелинейной целевой функцией и дополнительными функциональными ограничениями, учитывающими корреляцию отдельных уязвимостей и допустимость применения для их нейтрализации интегрированных механизмов защиты информации.

Ключевые слова: информационная сеть образовательной организации, поиск уязвимостей в программном обеспечении, автоматическая классификация уязвимостей, план нейтрализации уязвимостей, механизм защиты информации, комбинаторная задача оптимизации

OPTIMIZE THE SEARCH FOR VULNERABILITIES IN THE SECURITY SYSTEM RESOURCE INFORMATION-COMPUTER NETWORK OF THE UNIVERSITY

[1]Nadezhdin E.N., [2]Novikova T.L.

[1]Tula State Pedagogical University named after L.N. Tolstoy, Tula, e-mail: en-hope@yandex.ru;

[2]Shuya branch of Ivanovo State University, Shuya, e-mail: tshershakova@mail.ru

The article is devoted to the problem of finding and eliminating vulnerabilities in the software of the corporate information network of educational organizations in the internal audit process of information security. The focus is on two tasks that occupy a special place in the analytical work of the auditor: automatic classification of the detected vulnerabilities and determine the best plan to neutralize them by selecting mechanisms of information protection. The proposed model the problem of automatic classification of the detected vulnerabilities and its implementation method based on the solution of the optimization problem of discrete programming. Justified model of the problem of selecting a preferred plan of distribution of protection mechanisms between identified vulnerabilities, which is reduced to the formulation of the generalized problem of appointments. Consider an example of solving combinatorial problems assignment with a nonlinear objective function and additional functional limitations, taking into account the correlation of individual vulnerabilities and the admissibility of the application for their neutralization integrated mechanisms of information protection.

Keywords: the information network of an educational organization, the search for vulnerabilities in the software, automatic classification of security vulnerabilities, plan for resolution, the mechanism of protection of the information, a combinatorial optimization problem

В деятельности современной образовательной организации (ОО) особое место отводится аудиту информационной безопасности (АИБ), целью которого является получение объективных качественных и количественных оценок текущего состояния информационной безопасности (ИБ) в соответствии с установленными требованиями и показателями [8, 10]. Основное содержание деятельности аудитора ИБ связано с решением комплекса нетривиальных информационно-аналитических задач. К таким задачам относят [1, с. 18]: анализ информационных рисков, обусловленных возможностью осуществления угроз безопасности в отношении ресурсов корпоративной информационно-вычислительной сети (КИС); оценка текущего уровня защищенности ресурсов КИС; локализация «слабых звеньев» и выделение уязвимостей в системе защиты информации; оценка соответствия системы защиты информации (СЗИ) существующим стандартам; выработка рекомендаций по внедрению новых и повышению эффективности используемых механизмов безопасности КИС.

Проблема обеспечения безопасности образовательных организаций ОО нашла отражение в исследованиях известных отечественных учёных В.А. Галатенко,

А.А. Грушо, П.Д. Зегжды, А.А. Малюка, В.А. Сердюка, П.Б. Хорева и др., в которых с различных позиций рассматриваются теоретические и прикладные аспекты анализа угроз и оценки рисков информационной безопасности. Однако, несмотря на возросший поток публикаций, вопросы рационального поиска, локализации и устранения уязвимостей в программно-аппаратных средствах КИС ОО по-прежнему остаются открытыми и ждут своего конструктивного решения [6, 9]. В современных условиях не менее актуальными являются задачи рациональной организации, повышения качества и сокращения сроков проведения внутреннего АИБ ОО [8, 10]. Как показала практика, в условиях ограниченности привлекаемых ресурсов результаты внутреннего АИБ существенно зависят от сложности объекта автоматизации, квалификации экспертов-аудиторов и характеристик используемых ими прикладных методик и инструментальных средств. На фоне интенсивного развития технологий вскрытия СЗИ и интеллектуализации средств осуществления кибернетических атак на объекты информационной инфраструктуры ОО особую остроту приобрела задача превентивной разработки методик автоматизированного анализа защищённости ресурсов КИС и адаптации механизмов их защиты [2, 6].

Целью статьи является обоснование оптимизационного подхода к задачам поиска, локализации и нейтрализации уязвимостей в программном обеспечении КИС, выявленных в процессе реализации программы внутреннего АИБ ОО.

Под уязвимостью обычно понимают «брешь в средствах защиты, вызванную ошибками или конфликтами в процедурах (проекте, реализации, внутреннем контроле системы), которая может быть использована для несанкционированного проникновения в систему или для нарушения штатного режима функционирования программного обеспечения» [1, с. 263].

Появление уязвимостей в программном обеспечении (ПО) узлов КИС обусловлено преимущественно тремя факторами [5]. Во-первых, это ошибки недостаточно опытных разработчиков авторских приложений, например студентов или молодых преподавателей, дополняющих стандартные программные средства собственными расширениями. Во-вторых, это могут быть несертифицированные (нелегитимные) программные средства, которые размещаются пользователями в узлах сети для решения прикладных задач в нарушение требований корпоративной политики безопасности. В-третьих, источником уязвимостей в ПО могут служить целенаправленные действия внутренних нарушителей – инсайдеров, которые несанкционированно, исходя из корыстных побуждений, устанавливают в системе недоверенные программные продукты и/или осуществляют их некорректную настройку.

Самостоятельный поиск сетевым администратором уязвимостей в КИС, как правило, связан с большими затратами времени и вычислительных ресурсов. Поэтому на практике всё чаще прибегают к использованию сканеров безопасности (СКБ) – специальных программных автоматизированных средств, предназначенных для поиска, локализации и анализа уязвимостей локальных сетей. В настоящее время в корпоративных информационных сетях для выявления уязвимостей применяются сканеры безопасности разных типов [11]: *XSpider (компания Positive Technologies), Nessus (компания Tenable Network Security), ISS Internet Scanner (компания Internet Security Systems (IBM)), Shadow Security Scanner (компания SafetyLab) и др.* В СКБ последнего поколения, например, типа *Shadow Security Scanner,* гибко используются пассивный и активный режимы сканирования уязвимостей с элементами адаптивной настройки. Функционал СКБ последнего поколения охватывает следующие задачи: установление наличия уязвимости; локализация и анализ уязвимостей; обновление баз данных уязвимостей и баз данных способов их устранения; автоматическая генерация и интерпретация отчётов; формирование и выдача рекомендаций; настройка параметров режима сканирования сети; документирование и визуализация результатов анализа.

К дополнительным функциям СКБ можно отнести: формирование набора собственных правил сканирования на основе существующих или вновь создаваемых правил; возможность составления вероятных сценариев компьютерных атак; допустимость внешнего управления режимом работы через доступное администратору специальное программное обеспечение; изменение или расширение своей функциональности на основе авторских приложений; возможность осуществления собственных проверок на уязвимость с помощью специального менеджера; сигнализация администратору о несанкционированной прикладной (или сетевой) деятельности внутреннего нарушителя. Анализ указанных выше функций показывает, что СКБ сегодня обладает признаками интеллектуальной информационной системы. Это обстоятельство определяет технологическую базу и предпосылки для существенного повышения интенсив-

ности аналитической деятельности аудитора ИБ в вопросах оценки уровня защищённости ресурсов КИС.

В последующем для большей определённости задачи исследования ограничимся рассмотрением информационно-вычислительных аспектов проблемы поиска и нейтрализации уязвимостей в программном обеспечении узлов КИС.

Первая задача состоит в автоматической классификации уязвимостей, выявленных в процессе мониторинга и зондирования программного обеспечения узлов КИС. Такая процедура призвана выделить основные группы уязвимостей, родственные по совокупности признаков, и осуществить их ранжирование. *Вторая задача* заключается в разработке рекомендаций по нейтрализации выявленных уязвимостей. Далее эту задачу будем интерпретировать как задачу выбора наилучшего плана нейтрализации уязвимостей на основе выбора и активизации механизмов защиты информации (МЗИ) из некоторого конечного множества механизмов защиты, имеющихся в распоряжении администратора сетевой безопасности. Рассмотрим более подробно модели этих задач.

Как показали исследования, задача автоматической классификации уязвимостей в ряде случаев может быть представлена как задача кластеризации информационных объектов по нескольким признакам и может быть решена на основе известных методов кластерного анализа [13]. Однако данный подход требует привлечения экспертов высокой квалификации и его полная автоматизация в силу необходимости учёта ряда субъективных факторов затруднительна. Поэтому в качестве альтернативы кластерному анализу рассмотрим оптимизационный подход, который опирается на базовые положения и рекомендации теории математического программирования [3, 4, 12].

Как известно, в общем случае задача классификации заключается в разбиении некоторого числа n объектов на ω классов так, чтобы минимизировать некоторый критерий взаимной несогласованности их свойств.

Предположим, что заданы P объектов и для каждой пары объектов i и j известно некоторое число $\lambda_{i,j} \geq 0$ (если эти объекты рассматриваются как элементы евклидова пространства), или, в общем случае, индекс несогласованности, Примем далее $\lambda_{i,i} \geq 0$. Задача состоит в разбиении множества P этих объектов на ω классов и в выборе в каждом классе специального опорного объекта, называемого представителем этого класса, таким образом, чтобы сумма расстояний от конкретных объектов до их представителей в классах была минимальна.

Обозначим через $J = (1,2,...,j,...,n)$ множество уязвимостей, а через $I = (1,2,...,i,..,m)$ – множество классов. Введём в рассмотрение переменную $x_{i,j} = \{0,1\}$, которая обладает следующим свойством:

$$x_{i,j} = \begin{cases} 1, & \text{если объект } j \text{ относится к классу } i; \\ 0, & \text{в противном случае.} \end{cases}$$

Модель задачи автоматической классификации представим в следующем виде:

$$\sum_{i \in I} \sum_{j \in J} \lambda_{i,j} \cdot x_{i,j} \rightarrow \min, \qquad (1)$$

$$x_{i,j} \leq y_i \quad \forall i \in I, \quad \forall j \in J, \qquad (2)$$

$$\sum_{i \in I} x_{i,j} = 1 \quad \forall j \in J, \qquad (3)$$

$$\sum_{i \in I} y_i = \omega, \qquad (4)$$

где $y_i = \{0;1\}\ \forall i \in I$ и $y_j\ \{0;1\}\ \forall j \in J$.

Ограничение (2) выражает тот факт, что объект j может быть связан с представителем i только в том случае, когда представитель класса i выбран ($y_i = 1$). Ограничения (2) в сочетании с требованием бинарности переменных $x_{i,j}$ воспроизводят тот факт, что каждый объект (в нашем случае – уязвимость) должен быть связан с одним и только одним представителем, т.е. принадлежать одному классу. Соотношение (4) определяет число классов.

Решение сформулированной комбинаторной задачи (1)–(4) может быть получено на основе известных методов целочисленного программирования, например на основе метода ветвей и границ и его модификаций [3, 12].

Стремление реализовать в современной СЗИ ОО принцип «разумной достаточности» при учёте полученных с помощью СКБ формализованных данных о защищённости ресурсов КИС продвигает на уровень практической реализации задачу автоматического выбора рационального способа нейтрализации уязвимостей ПО. Этот вопрос может быть сведён к постановке и решению задачи о назначении, хорошо известной в теории математического программирования [4].

Процедуру обоснования плана нейтрализации выявленных уязвимостей ПО КИС на основе применения имеющихся в распоряжении администратора ИБ механизмов защиты информации представим как комбинаторную задачу оптимизации.

Рассмотрим классическую формулировку задачи о назначении [4, с. 473].

Задача о назначениях – это распределительная задача, в которой для выполне-

ния каждой работы требуется один и только один ресурс, и каждый ресурс может быть использован на одной и только одной работе. Иными словами, в классическом варианте принимается, что ресурсы неделимы между работами, а работы неделимы между ресурсами.

Пусть заданы: m – количество имеющихся ресурсов; n – количество работ; A_i, $i = 1,\ldots,m$ – единичное количество ресурса, A_i, $i = 1,\ldots,m$; $b_j = 1$ – единичное количество работы, B_j, $j = 1,\ldots,n$; $r_{i,j}$ – характеристика качества (положительный эффект), обусловленный выполнением работы B_j с помощью ресурса A_i.

Искомые параметры:

$x_{i,j}$ – индикатор назначения ресурса A_i на работу B_j

$$x_{i,j} = \begin{cases} 0, \text{ если ресурс } i \text{ не назначен на работу } j, \\ 1, \text{ если ресурс } i \text{ назначен на работу } j. \end{cases}$$

Математическая модель ***задачи о назначениях*** имеет вид

$$f(X) = \sum_{i=1}^{m}\sum_{j=1}^{n}(r_{i,j} \cdot x_{i,j}) \to \max, \qquad (5)$$

$$\begin{cases} \sum_{i=1}^{m} x_{i,j} = 1,\ j = 1,...,n, \\ \sum_{j=1}^{n} x_{i,j} = 1,\ i = 1,...,m, \\ x_{i,j} = \{0,1\},\ i = 1,...,m,\ j = 1,...,n. \end{cases} \qquad (6)$$

В нашем случае модель задачи о назначении будет иметь следующие особенности:

1. Требуется в результате решения задачи предложить такой план $X^* = (x_1^*, x_2^*, ..., x_n^*)$ защиты программного обеспечения, который позволит нейтрализовать выявленные ранее уязвимости и добиться минимального среднего ущерба при осуществлении атак злоумышленника с наименьшими затратами вычислительных (или материальных) ресурсов.

Отдельные МЗИ могут быть использованы для интегрированной защиты ресурсов, что проявляется в возможности одновременной нейтрализации нескольких коррелированных уязвимостей в программном обеспечении. При этом принимаем условие, что $m \le N$ и допустима нейтрализация одновременно двух разных уязвимостей с помощью одного механизма защиты. В формальном плане учёт этого обстоятельства требует ослабления ограничений, в частности вместо второго соотношения в выражении (6) предлагается записать неравенство

$$1 \le \sum_{j=1}^{n} x_{i,j} \le 2,\ i = 1,...,m.$$

2. Реализация плана защиты ресурсов заключается в активизации m ($m \le N$) имеющихся механизмов защиты.

3. Оценка реализуемого МЗИ характеризуется затратами ресурсов, выраженными в стоимостном эквиваленте, и средним предотвращённым ущербом, обусловленным успешной нейтрализацией вероятной атаки злоумышленника на ПО КИС.

С учётом указанных замечаний определим обобщённый показатель оптимальности комплекса мер защиты следующим образом:

$$F(X) = \frac{F_1(X)}{F_2(X)}, \qquad (7)$$

где $F_1(X)$ – величина совокупного предотвращённого ущерба в стоимостном эквиваленте;

$F_2(X)$ – величина совокупных затрат на реализацию активированного механизма защиты программного обеспечения, реализующего оптимальный план нейтрализации уязвимостей в стоимостном эквиваленте. Выражение (7) представляет собой показатель, сформированный в соответствии с обобщённым критерием «эффективность/стоимость».

Рассмотрим пример решения задачи выбора плана нейтрализации уязвимостей.

Пусть по итогам первого этапа АИБ в программном обеспечении узлов КИС выявлено $n = 8$ уязвимостей. В распоряжении администратора безопасности имеется несколько способов A_i, $i = 1,\ldots,m$, ($m = 5$) нейтрализации уязвимостей B_i, $i = 1,\ldots,n$ ($n = 8$). Каждый из способов даёт определённый конечный эффект в конкретных условиях реализации существующих угроз и регламента работы программного обеспечения. Для оценки эффективности комплекса мер защиты вводится матрица частных показателей

$$R = \{r_{i,j}\},\ i = 1,...,m,\ j = 1,...,n;$$

$$(0 \le r_{i,j} \le 1),$$

в которой элемент $r_{i,j}$ характеризует относительную эффективность защиты программных компонентов при нейтрализации уязвимости B_j на основе механизма защиты A_i.

В целях упрощения численного решения задачи оптимизацию будем осуществлять по критерию максимума предотвращённого ущерба, определяемого функционалом

$$F_1(X) = \sum_{i=1}^{m}\sum_{j=1}^{n}(r_{i,j}\cdot x_{i,j}) + \sum_{i=1}^{n}\sum_{\substack{j,k=1\\ j\neq k}}^{n}(d_{j,k}\cdot \nu_{j,k}\cdot x_{i,j}\cdot x_{i,k}) \rightarrow \max, \quad (8)$$

где

$$d_{j,k} = \begin{cases} 0, \text{ если } B_j \text{ и } B_k - \text{независимы}; \\ 1, \text{ если } B_j \text{ и } B_k - \text{зависимы}. \end{cases}$$

Здесь $\nu_{j,k} \in V$ – элемент, отражающий частный положительный эффект, который связан с одновременной нейтрализацией уязвимостей B_j и B_k.

Для учёта факта конечности ресурсов, привлекаемых для защиты программного обеспечения, систему ограничений (6) задачи дополним неравенством, учитывающим ограничение на допустимые совокупные затраты $C_Д$ при реализации механизмов защиты:

$$F_2(X) = \sum_{i=1}^{m}\left[\sum_{j=1}^{n}(c_{i,j}\cdot x_{i,j}) - \sum_{\substack{j,k=1\\ j\neq k}}^{n}(d_{j,k}\cdot c_{i,j}\cdot x_{i,j}\cdot x_{i,k})\right] \leq C_Д. \quad (9)$$

Численное решение задачи оптимизации плана защиты ПО в булевых переменных получено на основе авторского приложения, реализующего известный метод вектора спада [12].

Таблица 1

Матрица частных показателей эффективности МЗИ

i \ *J*	1	2	3	4	5	6	7	8
1	0,1	0,22	0,25	0,20	0,15	0,15	0,30	0,10
2	0,04	0,10	0,13	0,10	0,40	0,40	0,10	0,10
3	0,3	0,20	0,35	0,30	0,20	0,10	0,20	0,12
4	0,15	0,22	0,13	0,11	0,14	0,10	0,13	0,10
5	0,23	0,40	0,40	0,30	0,20	0,10	0,30	0,20

Таблица 2

Опорный план защиты X_0^* ($F_1(X_0^*) = 0,96$)

i \ *j*	1	2	3	4	5	6	7	8
1	0	1	0	0	1	0	0	0
2	1	0	0	1	0	0	1	0
3	0	0	0	0	0	0	0	1
4	0	0	1	0	0	0	0	0
5	0	0	0	0	0	1	0	0

Таблица 3

Оптимальный план защиты X^* ($F_1(X^*) = 1,60$)

i \ *j*	1	2	3	4	5	6	7	8
1	0	0	0	0	0	0	1	0
2	0	0	0	0	1	1	0	0
3	1	0	0	1	0	0	0	0
4	0	0	0	0	0	0	0	1
5	0	1	1	0	0	0	0	0

В соответствии с табл. 3, в которой представлены результаты решения комбинаторной задачи, оптимальный план защиты ПО состоит в реализации следующей схемы компенсации уязвимостей $B_j, j = 1,\ldots,8$:

$$A_1 \to B_7;\ A_2 \to (B_5,\ B_6);\ A_3 \to (B_1;\ B_4);$$
$$A_4 \to B_8;\ A_5 \to (B_2;\ B_3).$$

По данным вычислительного эксперимента, достигаемый при реализации полученного плана защиты эффект увеличился в 1,67 раза по сравнению с опорным вариантом защиты (см. табл. 2) и достиг величины 1,6 у. е.

Заключение

В статье показано, что обоснованный учет существующих информационных угроз, обнаружение и классификация уязвимостей и выполненный на этой основе анализ рисков закладывают основу для определения рационального плана адекватных мер защиты, обеспечивающих требуемый уровень защищённости программного обеспечения.

Для сокращения объёма аналитических расчётов при обосновании плана нейтрализации уязвимостей представляется целесообразным осуществить кластеризацию массива выявленных уязвимостей в ПО узлов КИС на основе постановки и целочисленного решения комбинаторной оптимизационной задачи классификации. Выделение комплекса возможных способов нейтрализации вероятных угроз с учётом особенностей выявленных уязвимостей формирует базис для формальной постановки задачи выбора интегрированных механизмов защиты ресурсов, которая представляет собой специальный вид задачи о назначении. Для поиска оптимального плана могут быть использованы апробированные на практике численные методы дискретного программирования в булевых переменных.

Для практического использования предложенного оптимизационного подхода требуется корректное обоснование показателей, характеризующих основные виды уязвимостей, и данных, определяющих частные показатели эффективности МЗИ. Эти вопросы требуют дополнительного изучения с учётом накопленного опыта успешного отражения информационных атак на ПО КИС.

Список литературы

1. Аверченков В.И. Аудит информационной безопасности: учеб. пособие для вузов [электронный ресурс]. – 2-е изд., стереотип. – М.: ФЛИНТА, 2011. – 269 с.

2. Ахметов Ю.М. Принципы разработки эффективного инструмента аудита безопасности информационных систем // Информационное противодействие угрозам терроризма. Научно-практический журнал. – 2010. – № 14. – С. 21–26.

3. Леонтьев В.А. Реализация математических моделей на ЭВМ (статистические и оптимизационные проблемы). – М.: Энергия, 1981. – 176 с.

4. Мину М. Математическое программирование. Теория и алгоритмы: Пер. с фр. и предисловие А.И. Штерна. – М.: Наука. Гл. ред. Физ.-мат. лит., 1990. – 488 с.

5. Миронов С.В., Куликов Г.В. Технологии контроля безопасности автоматизированных систем на основе структурного и поведенческого тестирования программного обеспечения // Кибернетика и программирование. – 2015. – № 5. – С. 158–172.

6. Надеждин Е.Н. Проблемные вопросы управления рисками информационной безопасности в сфере образования // Научный поиск. – 2012. – № 2.6. – С. 50–57.

7. Надеждин Е.Н., Новикова Т.Л. Информационно-аналитическая поддержка деятельности аудитора информационной безопасности // Фундаментальные исследования. – 2016. – № 10–1. – С. 67–72.

8. Надеждин Е.Н., Шептуховский В.А. Методика оценивания рисков информационной безопасности в вычислительных сетях образовательных учреждений // Педагогическая информатика. – 2012. – № 4. – С. 84–92.

9. Новикова Т.Л. Внутренний аудит информационной безопасности как инструмент управления информационными рисками образовательной организации // Шуйская сессия студентов, аспирантов, молодых учёных «Университет новой школе»: материалы IX Международной научной конференции (Шуя, 2–3 июня 2016 г.) / отв. ред. А.А. Червова. – Шуя: Изд-во Шуйского филиала ИвГУ, 2016. – С. 105–106.

10. Рожкова Е.О., Ильин И.В., Галушкин С.Я. Обзор и сравнение сканеров уязвимостей // Научное сообщество студентов XXI столетия. Технические науки: Сб. ст. по мат. XXX Междунар. студ. науч.-практ. конф. № 3(29). – 2015. – С. 77-87.

11. Сергиенко И.В. Математические модели и методы решения задач дискретной оптимизации. – 2-е изд., доп. и перераб. – Киев: Наук. думка, 1988. – 472 с.

12. Смирнова Е.Е. Методика экстрагирования математических понятий с признаками междисциплинарности на основе кластерного анализа // Информатизация образования и науки. – 2015. – № 2(26). – С. 133–145.