УДК 004.94:004.056

А.Б. Степанян, В.А. Дмитриев, В.К. Фисенко
Объединенный институт проблем информатики НАН Беларуси, Беларусь
Беларусь, 220012, г. Минск, ул. Сурганова, 6

Классификация угроз информационной безопасности автоматизированной системы

A.B. Stepanyan, U.A. Dzmitryieu, U.K. Fisenka
United Institute of Informatics Problems NAS of Belarus, Belarus
Belarus, 220012, c. Minsk, Surganov str., 6

Classification of Information Security Threats of Automated System

А.Б. Степанян, В.А. Дмитрієв, В.К. Фисенко
Об'єднаний інститут проблем інформатики НАН Білорусі, Білорусь
Білорусь, 220012, м. Мінськ, вул. Сурганова, 6

Класифікація загроз інформаційної безпеки автоматизованої системи

В статье рассматривается проблема классификации угроз информационной безопасности и даны основные определения, на основе которых предлагается алгоритм нахождения класса объектов.
Ключевые слова: классификация угроз информационной системы, автоматизированная информационно-поисковая система, релевантные объекты, алгоритм сужения-расширения, итерационный поиск.

The problem of classification of information security threats is considered, and the main definitions are given on the basis of which the algorithm for finding the class of objects is offered.
Key words: classification of information security threats, automated information-search system, relevant objects, restriction-expansion algorithm, iterative search.

Розглядається проблема класифікації загроз інформційної безпеки і подані основні визначення, за якими пропонується алгоритм знаходження класу об'єктів.
Ключові слова: класифікація загроз інформаційної системи, автоматизована інформаційно-пошукова система, релевантні об'єкти, алгоритм звуження-розширення, ітераційний пошук.

Проблема классификация угрозы информационной безопасности

Классификация угроз информационной безопасности особенно важна при оценке защищенности информационных систем в реальных условиях эксплуатации [1].

Угрозами информационной безопасности называются потенциальные источники нежелательных событий, которые могут нанести ущерб ресурсам информационной системы. Все угрозы безопасности направлены против программных и технических средств информационной системы. В конечном итоге, эти угрозы оказывают влияние на безопасность информационных ресурсов и приводят к нарушению основных свойств хранимой и обрабатываемой информации.

Построение надежной защиты автоматизированной системы невозможно без предварительного анализа возможных угроз безопасности системы. Этот анализ дол-жен включать в себя:

– выявление характера хранящейся в системе информации, выделение наиболее опасных угроз (несанкционированное чтение, несанкционированное изменение и т.д.);

– оценку затрат времени и средств на вскрытие системы, допустимых для злоумышленников;

– оценку ценности информации, хранящейся в системе;

– построение модели злоумышленника (другими словами, определение того, от кого нужно защищаться – от постороннего лица, пользователя системы, администратора и т.д.);

– оценку допустимых затрат времени, средств и ресурсов системы на организацию ее защиты.

В ходе анализа этих угроз необходимо убедиться, что все возможные источники угроз идентифицированы, идентифицированы и сопоставлены с источниками угроз все возможные уязвимости, присущие объекту защиты, всем идентифицированным источникам и уязвимостям сопоставлены угрозы безопасности информации [2].

Исходя их данного принципа, моделирование и классификацию источников угроз и их проявлений, целесообразно проводить на основе анализа взаимодействия логической цепочки: источник угрозы – уязвимость – угроза – последствия.

Под этими терминами будем понимать:

– источник угрозы – это потенциальные антропогенные, техногенные или стихийные носители угроз безопасности;

– угроза (Threat) – это возможная опасность (потенциальная или реально существующая) совершения какого-либо деяния (действия или бездействия), направленная против объекта защиты (информационных ресурсов), наносящая ущерб собственнику, владельцу или пользователю, проявляющаяся в опасности искажения и потери информации;

– уязвимость (Vulnerability) – это присущие объекту информатизации причины, приводящие к нарушению безопасности информации на конкретном объекте и обусловленные недостатками процесса функционирования объекта информатизации, свойствами архитектуры автоматизированной системы, протоколами обмена и интерфейсами, применяемые программным обеспечением и аппаратной платформой, условиями эксплуатации;

– последствия – это возможные последствия реализации угрозы (возможные действия) при взаимодействии источника угрозы через имеющиеся уязвимости.

Классификация угроз может быть проведена по множеству признаков. Наиболее распространённые из них приведены в [3].

По природе возникновения принято выделять естественные и искусственные угрозы. Естественными принято называть угрозы, возникшие в результате воз-действия на автоматизированные системы объективных физических процессов или стихийных природных явлений, не зависящих от человека. В свою очередь, искусственные угрозы вызваны действием человеческого фактора.

Примерами естественных угроз могут служить пожары, наводнения, цунами, землетрясения и т.д. Неприятная особенность таких угроз – чрезвычайная трудность или даже невозможность их прогнозирования. По степени преднамеренности выделяют случайные и преднамеренные угрозы. Случайные угрозы бывают обусловлены халатностью или непреднамеренными ошибками персонала. Преднамеренные угрозы обычно возникают в результате деятельности злоумышленника.

В качестве примеров случайных угроз можно привести непреднамеренный ввод ошибочных данных.

Пример преднамеренной угрозы − проникновение злоумышленника на охра-няемую территорию с нарушением установленных правил физического доступа.

В зависимости от источника угрозы принято выделять:

– угрозы, источником которых является природная среда. Примеры таких угроз – пожары, наводнения и другие стихийные бедствия;

– угрозы, источником которых является человек. Примером такой угрозы может служить внедрение агентов в ряды персонала автоматизированных систем со стороны конкурирующей организации;

– угрозы, источником которых являются санкционированные программно-аппаратные средства. Пример такой угрозы – некомпетентное использование системных утилит;

– угрозы, источником которых являются несанкционированные программно-аппаратные средства. К таким угрозам можно отнести, например, внедрение в систему вредоносного программного средства, например, троянской программы.

По положению источника угрозы выделяют:

– угрозы, источник которых расположен вне контролируемой зоны. Примеры таких угроз – перехват побочных электромагнитных излучений (ПЭМИН) или перехват данных, передаваемых по каналам связи; дистанционная фото- и видеосъёмка; перехват акустической информации с использованием направленных микрофонов;

– угрозы, источник которых расположен в пределах контролируемой зоны. Примерами подобных угроз могут служить применение подслушивающих устройств или хищение носителей, содержащих конфиденциальную информацию.

По степени воздействия на автоматизированные системы выделяют пассивные и активные угрозы. Пассивные угрозы при реализации не осуществляют никаких изменений в составе и структуре автоматизированных систем.

Реализация активных угроз, напротив, нарушает структуру автоматизированной системы. Примером пассивной угрозы может служить несанкционированное копирование файлов с данными.

По способу доступа к ресурсам автоматизированных систем выделяют:

– угрозы, использующие стандартный доступ. Пример такой угрозы – несанкционированное получение пароля путём подкупа, шантажа, угроз или физического насилия по отношению к законному обладателю;

– угрозы, использующие нестандартный путь доступа. Пример такой угрозы – использование не декларированных возможностей средств защиты.

Критерии классификации угроз можно продолжать, однако на практике чаще всего используется следующая основная классификация угроз, основывающаяся на трёх базовых свойствах защищаемой информации:

– угрозы нарушения конфиденциальности информации, в результате реализации которых информация становится доступной субъекту, не располагающему пол-номочиями для ознакомления с ней;

– угрозы нарушения целостности информации, к которым относится любое злонамеренное искажение информации, обрабатываемой с использованием автоматизированных систем;

– угрозы нарушения доступности информации, возникающие в тех случаях, когда доступ к некоторому ресурсу автоматизированной системы для легальных пользователей блокируется.

Выделяют два основных метода перечисления угроз:

1) построение произвольных списков угроз;

2) построение деревьев угроз.

В первом методе, возможные угрозы выявляются экспертным путём и фиксируются случайным и неструктурированным образом. Для данного подхода характерны неполнота и противоречивость получаемых результатов.

Во втором методе, угрозы описываются в виде одного или нескольких дере-вьев. Детализация угроз осуществляется сверху вниз, и в конечном итоге каждый лист дерева дает описание конкретной угрозы.

Между поддеревьями в случае необходимости могут быть организованы логические связи. Можно в качестве примера привести дерево угрозы блокирования доступа к сетевому приложению.

Обычно, блокирование доступа к приложению может произойти либо в результате реализации DoS-атаки на сетевой интерфейс, либо в результате завершения работы компьютера. В свою очередь, завершение работы компьютера может произойти либо вследствие несанкционированного физического доступа злоумышленника к компьютеру, либо в результате использования злоумышленником уязвимости, реализующей атаку на переполнение буфера.

Отметим, что реальные угрозы информационной безопасности далеко не всегда можно строго отнести к какой-то одной из перечисленных категорий или классу. Так, например, угроза хищения носителей информации может быть при определённых условиях отнесена ко всем трём категориям.

Заметим, что перечисление угроз, характерных для той или иной автоматизированной системы, является важным этапом анализа уязвимостей автоматизированных систем, проводимого, например, в рамках аудита информационной безопасности, и создаёт базу для последующего проведения анализа рисков.

В данной статье угрозу автоматизированной системы будем считать как объект некоторого класса угроз.

Так как и классы угроз, и объекты из класса характеризуются обобщенными признаками в виде дескрипторных векторов, следовательно, процесс поиска класса объектов можно считать как автоматизированный процесс поиска класса объектов с помощью автоматизированной информационной поисковой системы (АИПС).

При этом начальный вектор реакции (класс объектов) получается путем предварительного поиска, т.е. предварительного сравнения класса (поискового образа запроса) со всеми объектами (поисковыми образами объектов) из заданного множества объектов.

Основные определения

Пусть объект характеризуется набором обобщенных признаков $T^{(1)}, T^{(2)}, \ldots T^{(M)}$. В качестве обобщенных признаков могут служить: признаки по природе возникновения угроз; в зависимости от источника угроз; по положению источника угроз; по степени воздействия угроз; по способу доступа и т.д. [4]. Допустимое универсальное множество значений обобщенных признаков $T^{(l)}$, l = (1,N), обозначим, через - $T^{(l)}$.

Обозначим через $T^{(k)}$ множество дескрипторов, которые входят в лексическую базу АИПС

$$T^{(k)} = \left\{t_j^{(k)}\right\}, \text{ j= (1,n).}$$

Определение 1. Упорядоченный набор $T_i^{(k)} = \left\{t_{i1}^{(k)}, t_{i2}^{(k)}, \dots t_{in}^{(k)}\right\}$, где i = (1,M) и $t_{ij}^{(k)}$, принимающий значения из интервала $[0,1]$, назовем дескрипторным вектором.

Определение 2. Неотрицательная вещественная функция A = A(X,Y) называется мерой сходства (близости) векторов X и Y, если:

1) $0 \le A(X,Y) < 1$, если $X \ne Y$;
2) $A(X,Y) = 1$, если $X = Y$;
3) $A(X,Y) = A(Y,X)$.

На основании меры близости можно получить матрицу близости множества объектов, которая также обозначается через A.

В качестве меры близости для дескрипторного вектора можно использовать косинусную меру, которая имеет следующий вид:

$$A\left(T_p^{(k)}, T_q^{(k)}\right) = \frac{\sum_{j=1}^{n} t_{pj}^{(k)} \times t_{qj}^{(k)}}{\sqrt{\sum_{j=1}^{n} (t_{pj}^{(k)})^2} \times \sqrt{\sum_{j=1}^{n} (t_{qj}^{(k)})^2}}, \qquad p,q = \overline{(1, M)}.$$

Определение 3. Y= AX назовем средой первого порядка (СПП) вектора X, где A – матрица близости.

Определение 4. n-мерное векторное пространство U назовем поисковым пространством, если для каждой пары векторов **a,b** $\in U$ задан способ определения значения меры близости.

При информационном поиске на массиве из **n** объектов АИПС порождает некоторый вектор (вектор реакции АИПС) X $\in$ U. Компоненты вектора реакции X показывают степень близости поисковых образов объектов поисковым образам запроса и вычисляются с помощью критерия смыслового соответствия, используемого данной АИПС.

Пусть $\overset{f_1}{\rightarrow}$ оператор ортогональной проекции U на U_1 ($U_1 \subset U$).

Определение 5. Вектор $X \in U$ назовем устойчивым относительно ортогональ-ной проекции f_1 и линейного оператора A, если

$$X \overset{f_1}{\rightarrow} \overline{X} \overset{A}{\rightarrow} Y \overset{f_1}{\rightarrow} \lambda \overline{X},$$

где $\overset{f_1}{\rightarrow}$ – ортогональная проекция U на U_1, а $\overset{A}{\rightarrow}$ – линейное преобразование в пространстве U, λ – положительное вещественное число.

Заметим, что при этом вектор X не меняет свое направление относительно подпространства U_1. Вектор X обладает свойством квазиустойчивости, определяет квазисобственный вектор и может, в частном случае, являться собственном вектором матрицы A.

Пусть U_1 и U_2 – подпространства из U, соответствующие подмножествам D_1 и $D_2 = D \backslash D_1$, $D_1 \ne \varnothing$, $D_2 \ne \varnothing$.

Множество индексов i обозначим через I_1, если $d_i \in D_1$, а I_2 множество индексов i, если $d_i \in D_2$.

Определение 6. Для вектора $X \in U$ подпространство $U_1 \subset U$ назовем доминирующим над подпространством $U_2 \subset U$, если $\min_{i \in I_1}\{x_i\} \ge \max_{i \in I_2}\{x_i\}$.

Подпространство U_1 назовем полным доминирующим, если

1) $x_i = 0$ при $i \in I_1$,

2) $x_i \geq 0$ при $i \in I_2$.

Определение 7. Вектор $\hat{X} \in U$ $(\hat{X} > 0)$ назовем ядром относительно линейного оператора A, если

1) для $\hat{X}$ существует такое подпространство U_1, которое является полным доминирующим;

2) СПП вектора $\hat{X}$ является устойчивым относительно ортогональной проекции $\xrightarrow{F_1}$ и линейного оператора A;

3) U_1 является доминирующим подпространством для вектора $Y = A\hat{X}$.

Ядро определяет некоторое подмножество элементов $D_1 \subset D$, соответствующее подпространству U_1. Из условия (3) определения (6) следует, что элементы подмножества D_1 имеют сравнительно большие значения меры близости между собой, а с элементами из $D \backslash D_1$ – сравнительно малые значения меры близости. Это означает, что объекты, соответствующие элементам подмножества D_1, имеют единую семантическую основу. Следовательно, ядро определяет некоторое подмножество объектов, которые можно рассмотреть как хорошую выдачу на некоторый запрос. Таким образом, задача информационного поиска сводится к нахождению ядра соответствующего подмножества D_1. Для повышения показателя полноты вместо ядра можно использовать СПП ядра. В этом случае целесообразно найти такое СПП ядра, которое имеет максимальное значение меры близости F к СПП первоначального вектора реакции АИПС [5]:

$$F(Y,Z) = \max_{Z,W} F, \quad (1)$$

где Y – СПП первоначального вектора реакции;

Z – СПП некоторого ядра из множества W СПП ядер.

В качестве F используется косинусная мера безопасности.

Задача поиска семантических однородных объектов сводится к задаче разбиения объектов релевантных и нерелевантных. Из этого следует, что применением правил кластер-анализа в поиске релевантных объектов можно получить более высокие показатели функциональной эффективности АИПС.

В анализе функциональной эффективности можно принять следующие правила кластер-анализа.

1) Однозначность результата поиска.

2) Независимость результата поиска от порядка объектов в поисковом массиве.

3) Устойчивость результата поиска.

4) Независимость результата поиска от масштаба измерения.

5) Объекты, имеющие большое сходство с релевантными объектами, должны включатся в выдачу.

6) Процедура коррекции поискового предписания при организации автоматической обратной должна быть совершенной.

Последнее правило используется при многоэтапном поиске. При этом процедуру назовем совершенной, если многократное повторение данной процедуры не ухудшает показателей поиска, а в противном случае, процедуру назовем несовершенной.

Алгоритм – СР

В данном разделе приводится итерационной алгоритм нахождения квазиоптимального вектора реакции – СР алгоритм. При этом на каждом шаге порождается вектор

реакции АИПС, на основе вектора реакции предыдущего шага. Начальный вектор реакции получается путем предварительного поиска. Процесс порождения вектора тоже является итерационным процессом, в течение которого выделяется подмножество (процесс сужения) однородных релевантных объектов D_R. На основе этого подмножества получается новый вектор реакции, который определяет расширенное подмножество документов, семантически близких с элементами D_R (процесс расширения). Последовательное применение процедур сужения-расширения имеет цель – итерационным образом из выдачи исключить нерелевантные объекты и включить в выдачу релевантные объекты.

Пусть дано множество объектов D и первоначальный вектор реакции АИПС X_1.

Рассмотрим последовательность подмножества объектов:

$D_1, D_2, \ldots, D_i, \ldots, D_{n-1}$, где в подмножество D_i выключены i объектов, которым соответствует первые i-максимальные компоненты вектора X_1. Этой последовательности соответствует последовательность подпространств $U_1, U_2, \ldots, U_i, \ldots, U_{n-1}$, определяемая подмножествами D_i. Обозначим через $\xrightarrow{f_2^{(i)}}$ ортогональную проекцию U на U_i. Тогда имеем

$$X_1 \xrightarrow{f_2^{(1)}} \widetilde{X_1}(1),$$
$$X_1 \xrightarrow{f_2^{(2)}} \widetilde{X_1}(2),$$
$$\ldots\ldots\ldots$$
$$X_1 \xrightarrow{f_2^{(i)}} \widetilde{X_1}(i),$$
$$\ldots\ldots\ldots$$
$$X_1 \xrightarrow{f_2^{(n-1)}} \widetilde{X_1}(n-1),$$

где $\widetilde{X_1}(i)$ – проекция вектора X_1 на подпространство U_i, $i = \overline{1, n-1}$.

Векторы $\widetilde{X_1}(i)$ удовлетворяют первому и третьему условиям ядра, которые и используются в дальнейших процедурах решения оптимизационной задачи (1).

Из векторов $\widetilde{X_1}(i)$ выбирается вектор $\widetilde{X_1}(K_1^*)$, удовлетворяющий условию

$$F = \max_i F(X_1, A\,\widetilde{X_1}(i)). \qquad (2)$$

Вектор $\widetilde{X_1}(K_1^*)$ используется для получения нового вектора реакции

$$X_2 = A\,\widetilde{X_1}(K_1^*).$$

Обозначим через H_1 множество операторов $\xrightarrow{f_2^{(1)}}, \xrightarrow{f_2^{(2)}}, \ldots \xrightarrow{f_2^{(n-1)}}$.

Тогда выражение (2) можно записать в следующем виде:

$$F = \max_{f_2^{(i)} \in H_1} F(X_1, Af_1^{(i)} X_1).$$

Для данной L-й итерации получим следующее выражение

$$F_L = \max_{f_L^{(i)} \in H_L} F(X_L, Af_L^{(i)} X_L) \qquad (3)$$

Пусть $\xrightarrow{f_1^*}, \xrightarrow{f_2^*}, \ldots \xrightarrow{f_{L-1}^*}$ максимизирует функции $F_1, F_2, \ldots, F_{L-1}$, соответственно. Тогда вектор реакции X_L L-о шага определяется следующим образом:

$$X_L = Af_{L-1}^* X_{L-1}.$$

Таким образом,

$$F_L = \max_{f_L^{(i)} \in H_L} F(Af_{L-1}^* X_{L-1}, Af_L^{(i)} Af_{L-1}^* X_{L-1}).$$

Легко заметить, что

$$X_L = Af^*_{L-1} \times Af^*_{L-2} \times \ldots \times Af^*_1 X_1.$$

Обозначим через $A^o_{L-1} = Af^*_{L-1} \times Af^*_{L-2} \times \ldots \times Af^*_1$.

Тогда $F_L = \max_{f_L^{(i)} \in H_L} F(A^o_L X_1, Af_L^{(i)} A^o_{L-1} X_1)$.

Экспериментальное исследование данного итерационного процесса показало, что F_L быстро сходится к единице при небольших значениях L ($L \leq 20$).

Легко заметить, что с помощью оптимального оператора ортогональной проекции f_L^*, из вектора X_L получается ядро $\widehat{X_L}$.

Эффективность применения данного итерационного метода зависит от истинности отражения близости объектов матрицей А. Следовательно, при определении матрицы А необходимо учесть всю информацию из объекта, который может увеличить функциональную эффективность АИПС.

Для этой цели можно использовать несколько матриц близости. Например, если взять две матрицы близости для разных признаков $A^{(1)}$ и $A^{(2)}$, тогда можно получить СПП вектора X_0 с использованием разных признаков:

$$X_1^{(1)} = A^{(1)} X_0,$$
$$X_1^{(2)} = A^{(2)} X_0.$$

Выпуклая линейная комбинация векторов $X_1^{(1)}$ и $X_1^{(2)}$ может рассматриваться как обобщенный результат:

$$X_1 = \omega_1 X_1^{(1)} + \omega_2 X_1^{(2)},$$

где $\omega_1 + \omega_2 = 1$, $\omega_1, \omega_2 \geq 0$.

Следовательно, $X_1 = \omega_1 A^{(1)} X_0 + (1 - \omega_1) A^{(2)} X_0 = [\omega_1 A^{(1)} + (1 - \omega_1) A^{(2)}] X_0$.

Обозначим через $A = \omega_1 A^{(1)} + (1 - \omega_1) A^{(2)}$, тогда $X_1 = AX_0$.

Значение коэффициента ω_1 будет влиять на показатели функциональной эффективности АИПС. Его оптимальное значение может быть выбрано экспериментальным путем.

Литература

1. Максимович Е.П. Методологические основы поддержки принятия решения при анализе информационной безопасности в процессе эксплуатации информационных систем / Е.П. Максимович, А.Б. Степанян, В.К. Фисенко // Искусственный интеллект. – 2012. – № 3. − С. 458-469.
2. Классификация угроз информационной безопасности [Электронный ресурс]. – Режим доступа : http://it-ideas74.ru/articles/25-security-inform.html.
3. Вихорев С.В. Классификация угроз информационной безопасности / С.В. Вихорев [Электронный ресурс]. – Режим доступа : http://www.cnews.ru/ reviews/free/oldcom/ security/elvis_class.shtml.
4. Степанян А.Б., Карапетян А.Г., Аветисян Д.О. Прикладные аспекты использования искусственного интеллекта, порожденного в процессе динамического взаимодействия поисковых стратегий / А.Б. Степанян, А.Г. Карапетян, Д.О. Аветисян // В сб. тезисы докладов Всесоюзного семинара «Интеллектуальные банки данных», Цахкадзор, Армянская ССР, 1980. – С. 16-17.
5. Степанян А.Б. Функциональная эффективность АИПС и автоматическое индекси-рование документов / А.Б. Степанян, А.Г. Карапетян // В сб. тезисы докладов Всесоюзной научной конференции «Научные основы создания АСНТИ в высшей школе», Киев, 1986. − С. 78-80.

Literatura

1. Maksimovich E.P., Stepanyan A.B., Fisenko V.K. Methodological foundations to support decision-making in the analysis of information security during the information system operation. – Artificial intelligence, № 3. − 2012. − S. 458-469.

2. Classification of information security threats // http://it-ideas74.ru/articles/25-security-inform.html.
3. Vihorev S.V. Classification of information security threats // http://www.cnews.ru/ reviews/free/ oldcom/ security/elvis_class.shtml.
4. Stepanyan A.B., Karapetyan A.G., Avetisyan D.O Applied aspects of the use of artificial intelligence descendant in the process of searching strategies dynamic co-operation. Vsesojuznyj seminar «Intellektual'nye banki dannyh» (Cahkadzor,1980). − S. 16-17.
5. Stepanyan A.B., Karapetyan A.G. Functional efficiency of AIPS and automatic indexing of documents. Vsesojuznaja nauchnaja konferencyja «Nauchnye osnovy sozdanija ASNTI v vyshej shkole» (Kiev,1986). − S. 78-80.

RESUME

A.B. Stepanyan, U.A. Dzmitryieu, U.K. Fisenka

Classification of Information Security Threats of Automated System

In the article, the problem of classification of information security threats is considered, and the main definitions are given on the basis of which the algorithm for finding the class of objects is offered.

The proximity measure of two vectors in n-dimensional space on the basis of which it is possible to receive a proximity matrix of a set of objects is defined.

The algorithm of classification of information security threats is considered as a process of search of the relevant uniform objects having a uniform semantic basis. The iterative algorithm of finding of a quasioptimum vector reaction of AIPS is given, where the consecutive application of restriction-extension procedures has the purpose to exclude the irrelevant objects from delivery in an iterative way and to include in delivery the relevant objects.

The offered method of search of relevant uniform objects is reduced to finding a kernel, which is stable with respect to the orthogonal projection $\overrightarrow{A_1}$ and the linear operator A.

Статья поступила в редакцию 05.04.2013.