Бондарчук Максим Сергеевич

РАЗРАБОТКА МАТЕМАТИЧЕСКОЙ МОДЕЛИ ЗАЩИЩЕННОЙ КОМПЬЮТЕРНОЙ СЕТИ НА ОСНОВАНИИ ТРЕБОВАНИЙ СТАНДАРТОВ БЕЗОПАСНОСТИ

Адрес статьи: www.gramota.net/materials/1/2012/4/7.html

Источник

Альманах современной науки и образования

Тамбов: Грамота, 2012. № 4 (59). С. 33-37. ISSN 1993-5552.

Адрес журнала: www.gramota.net/editions/1.html

Содержание данного номера журнала: www.gramota.net/materials/1/2012/4/

декоративной живописи находятся в диалектической взаимосвязи, но изобразительность подчинена выразительностью, так как в декоративно-прикладном искусстве выразительность является наиболее важным моментом художественного образного отражения. Декоративность в работах трактуется так же как прием художественно-образного мышления, характерной чертой которого является создание особой композиционной модели. Здесь декоративность служит как прием для выявления согласованности произведения, соразмерности и упорядоченности всех его деталей и форм, применяется не только в декоративно-прикладном искусстве, но и в других искусствах.

Таким образом, декоративность является не только специфической особенностью декоративно-прикладного искусства, неразрывно связанной с «выразительностью», но и служит приемом художественно-образного мышления, в том числе и в живописи. Трактовка декоративности как специфической особенности декоративно-прикладного искусства и приема художественно-образного мышления во всех пространственно-временных искусствах является основополагающей теоретической предпосылкой преподавания курса «Декоративная живопись» при обучении студентов: дизайнеров, декораторов, прикладников [1, с. 47].

При выполнении натурных постановок на курсе «Декоративная живопись» студенты учатся перевоплощать реальные формы и предметы объективной действительности в условные плоскостные, орнаментальные изображения, что сопутствует организации работы по спецкурсу «Процесс создания декоративного произведения» при создании творческих композиций. Условность как способ образного решения задач декоративной живописи заключается в выявлении орнаментально-ритмической основы натурной постановки, в плоскостно-декоративной трактовке цвета средствами «ограниченной палитры», в частном подходе от натурного цвета в целях поиска гармоничного колористического строя живописного произведения, применение метода творческой интерпретации натуры для реализации творческого замысла. Членение плоскости работы на различные по размеру, по пластическим очертаниям части определяется характером натурных постановок - силуэтом предметов, характером орнамента тканей (например, в натюрморте), костюмов в портретных зарисовках и фигурах людей. В данном случае натурную постановку, живую модель нельзя пассивно копировать, а стараться разглядеть в объекте и понять роль пластических поворотов и контрастов, суметь их выявить и усилить.

Курс «Декоративная живопись» помогает студентам развивать творческие способности, воображение на спецкурсе «Процесс создания декоративного произведения» при составлении декоративных композиций в жанрах: портрет, пейзаж, натюрморт. Это способствует развитию в овладении навыков преображения реальных объектов в условные, стилизованные формы. В умении работать с многоцветной палитрой, выявлять нужное колористическое решение для творческой идеи при составлении сложных декоративных сюжетных композиций.

Список литературы

1. **Ермолаева Л. П.** Основы дизайнерского искусства. М.: Архитектура-С, 2009. С. 152.
2. **Логвиненко Г. М.** Декоративная композиция. М.: Владос, 2006. С. 144.

УДК 004.056

Технические науки

Максим Сергеевич Бондарчук
Академия ФСО России, г. Орел

РАЗРАБОТКА МАТЕМАТИЧЕСКОЙ МОДЕЛИ ЗАЩИЩЕННОЙ КОМПЬЮТЕРНОЙ СЕТИ НА ОСНОВАНИИ ТРЕБОВАНИЙ СТАНДАРТОВ БЕЗОПАСНОСТИ©

В статье рассматривается научный подход к проблеме проектирования защищённых компьютерных сетей в соответствии с требованиями ГОСТов. В результате анализа угроз безопасности, целей безопасности, функциональных требований безопасности разработана математическая модель, характеризующая защищенность объекта оценки на основании систематизированного подхода к теоретическим основам проектирования защищенных компьютерных сетей.

Проблема компьютерной безопасности, возникшая при появлении и распространении информационных технологий, на сегодняшний день остро стоит перед разработчиками и пользователями. Для согласования всех взглядов на проблему создания защищенных компьютерных сетей разрабатываются соответствующие стандарты безопасности.

К документам, стандартизирующим требования и критерии безопасности, относятся: «Оранжевая книга», «Европейские критерии», «Федеральные критерии», «Общие критерии» и другие. Данные документы отличаются требованиями к проектируемым системам, рассматриваемыми угрозами, подходами к проблеме обеспечения безопасности информации.

В Российской Федерации существенная роль в области обеспечения информационной безопасности наряду с руководящими документами Гостехкомиссии отводится также стандарту ГОСТ Р ИСО/МЭК 15408.

ГОСТ Р ИСО/МЭК 15408-2008 подготовлен Центром безопасности информации, Центром «Атомзащитаинформ», ЦНИИАТОМИНФОРМ, ВНИИстандарт при участии экспертов Международной рабочей группы по «Общим критериям» на основе международного стандарта ISO/IEC 15408. Стандарт содержит три части и утвержден Приказами Федерального агентства по техническому регулированию и метрологии от 18.12.2008 г. № 519-ст, 520-ст, 521-ст, введён в действие 1 октября 2009 года.

Предоставляемые документами требования к функциям безопасности продуктов или систем информационных технологий позволяют обеспечить потребителям необходимый уровень защиты. Для обеспечения конфиденциальности, целостности, доступности информации стандарты предлагают соответствующие механизмы, что позволяет говорить о качественно новом подходе к проблеме безопасности информационных технологий. Учитывая общие черты и различия существующих документов необходимо разработать наиболее полный алгоритм оценки безопасности проектируемой системы. Сложность и многообразие подходов, отсутствие систематизации основных направлений анализа и синтеза компьютерных сетей создают значительные трудности для специалистов проектировщиков, использующих теоретические подходы для решения практических задач. В то же время достаточная завершенность математических результатов и потребности разработчиков обусловили необходимость и своевременность систематизированного изложения теоретических основ проектирования защищенных компьютерных сетей.

Предметной областью исследований являются защищённые компьютерные сети.

Цель исследований заключается в разработке научного подхода к проблеме проектирования защищённых компьютерных сетей в соответствии с требованиями ГОСТов.

В качестве объекта оценки (ОО) рассматривается компьютерная сеть. Чтобы обеспечить ее защищенность, необходимо выполнение функциональных требований безопасности в соответствии с требованиями руководящих документов. В результате проведенного анализа ОО, его среды и условий функционирования формируется перечень угроз безопасности. Ниже представлен перечень угроз безопасности, которые способны повлиять на безопасную эксплуатацию ОО.

Пусть U - множество угроз для данного ОО. Выделено двенадцать элементов данного множества.

U_1 - подмена адреса подуровня управления доступом;

U_2 - подмена адреса источника передаваемой ОО информации с целью выдачи себя за администратора;

U_3 - чтение, изменение (модификация), уничтожение значений параметров конфигурации ОО;

U_4 - обход механизмов защиты информации с целью получения доступа к ОО, осуществления несанкционированного доступа;

U_5 - потеря данных или переполнение журнала аудита ОО посредством создания определенного числа регистрируемых ОО событий с целью сокрытия предпринятых действий;

U_6 - воздействие на механизмы аудита ОО с целью вызова сбоя или отказа в работе данного механизма ОО;

U_7 - осуществление несанкционированного доступа к программной и/или информационной части ОО с целью осуществления несанкционированного доступа к информации, передаваемой внутри конкретной локальной вычислительной сети;

U_8 - воздействие на механизм идентификации и аутентификации ОО с целью получения доступа к ОО, присвоения полномочий администратора;

U_9 - ошибки администратора при настройке параметров конфигурации ОО, нарушение администратором технологии эксплуатации ОО;

U_{10} - сбой и/или отказ отдельного компонента, механизма ОО или всего ОО в процессе его функционирования;

U_{11} - осуществление физического доступа к ОО с последующим целенаправленным нанесением повреждений или уничтожением ОО;

U_{12} - перехват и повторная передача ОО данных идентификации и аутентификации с целью выдачи себя за администратора.

На основании угроз безопасности формируются цели безопасности.

Каждая угроза U_i определяется как зависимость вида:

$U_i((f_T(U_i)),(f_F(f_T(U_i))))$, где $f_T(U_i)=T_i$ - множество целей безопасности соответствующих i-ой угрозе, $f_F(f_T(U_i))=F_i$ - множество функциональных требований безопасности в случае i-ой угрозы, f_T - логическая функция анализа - подбор целей безопасности в соответствии с угрозами, f_F - логическая функция анализа - подбор функциональных требований в соответствии с определенными целями безопасности.

Таким образом, для каждой угрозы U_i формируется множество целей безопасности T, для каждой цели безопасности T_i - множество функциональных требований безопасности F.

При рассмотрении целей безопасности можно сделать вывод об их соответствии сервисам безопасности, то есть каждая цель соответствует определенному сервису безопасности. В работах В. Б. Бетелина и В. А. Галатенко были выделены следующие базовые сервисы безопасности [1]: идентификация и аутентификация, управление доступом, протоколирование и аудит, шифрование, контроль целостности, экранирование, анализ защищенности, обеспечение отказоустойчивости, обеспечение безопасного восстановления, туннелирование, управление.

Существующие цели безопасности для данного ОО: T_1 - идентификация; T_2 - обслуживание; T_3 - сигнализация; T_4 - аудит; T_5 - обслуживание, резервирование; T_6 - конфиденциальность; T_7 - фильтрация кадров; T_8 - защита от повторной передачи; T_9 - восстановление; T_{10} - контроль; T_{11} - тестирование.

Множество угроз представлено матрицей-строкой $U=(U_1,\ldots,U_n)$, при n = (1, …, m), где m - количество угроз для данного ОО.

Множество функциональных требований F выбирается в соответствии с ОО из полного каталога функциональных требований ГОСТ Р ИСО/МЭК 15408.

В каталоге требований в соответствии с ГОСТ Р ИСО/МЭК 15408 все требования разделены на 11 классов, в соответствии с этим образуются множества:

$((F_{1\,1},\ldots,F_{1\,j}),\ldots,(F_{11\,1},\ldots,F_{11\,g}))$, j и g - количество функциональных требований в том или ином классе. Для каждого класса существует определенный набор функциональных требований.

Основываясь на зависимости целей безопасности от угроз безопасности, а функциональных требований безопасности от целей безопасности, для каждой угрозы U_i формируются множества функциональных требований из разных классов (F_{kj}), где k - определенный класс требований, j - определенное требование в классе k.

Множества функциональных требований в пределах класса для каждой цели безопасности Ti далее представлены в виде матриц-строк.

$F = (F_1,\ldots,F_j)$; j - число требований в определенном классе.

Существующие классы функциональных требований (в соответствии с ГОСТ Р ИСО/МЭК 15408) представлены в Таблице 1 [4]:

Таблица 1. *Классы функциональных требований безопасности*

№ п/п	Класс функциональных требований	Описание класса функциональных требований
1	FAU	Аудит безопасности
2	FCO	Связь
3	FCS	Криптографическая поддержка
4	FDP	Защита данных пользователя
5	FIA	Идентификация и аутентификация
6	FMT	Управление безопасностью
7	FPR	Приватность
8	FPT	Защита комплекса средств обеспечения безопасности ОО
9	FRU	Использование ресурсов
10	FTA	Доступ к ОО
11	FTP	Доверенный маршрут/канал

Функциональные требования, существующие для каждой из одиннадцати целей безопасности, будут представлены в виде элементов матрицы-строки, равных 1, а остальные требования из данного класса равны 0. Рассматриваются 11 целей безопасности, соответствующих сервисам безопасности, и 11 классов безопасности. В пределах каждого класса выполняется логическое сложение матриц для исключения повторения функциональных требований:

Класс FAU (6 требований):

(0 0 0 0 0 0) ∨ (1 1 1 1 1 0) ∨ (1 1 1 0 0 0) ∨ (1 1 1 1 1 0) ∨ (0 1 0 0 0 0) ∨ (0 0 0 0 0 0) ∨ (0 0 0 0 0 0) ∨ (0 0 0 0 0 0) ∨ (0 0 0 0 0 0) ∨ (0 0 0 1 0 0) ∨ (0 0 0 0 0 0) = (1 1 1 1 1 0)

Класс FCO (2 требования):

(0 0) ∨ (0 0) ∨ (0 0) ∨ (0 0) ∨ (0 0) ∨ (0 0) ∨ (0 0) ∨(0 0) ∨ (0 0) ∨ (0 0) = (0 0)

Класс FCS (2 требования):

(0 0) ∨ (0 0) ∨ (0 0) ∨ (0 0) ∨ (0 0) ∨ (1 1) ∨ (0 0) ∨ (0 0) ∨ (0 0) ∨ (0 0) ∨ (0 0) = (1 1)

Класс FDP (13 требований):

(1 1 0 0 1 1 0 0 0 0 0 0 0) ∨ (1 1 0 0 1 1 0 0 0 0 0 0 0) ∨ (0 0 0 0 0 0 0 0 0 0 0 0 0 0) ∨ (0 0 0 0 0 0 0 0 0 0 0 0 0 0) ∨ (0 0 0 0 0 0 0 0 0 0 0 0 0 0) ∨ (1 1 0 0 0 0 0 0 1 0 0 0 0) ∨ (0 0 0 1 1 1 1 0 0 0 0 0 0) ∨ (0 0 0 0 0 0 0 0 0 0 0 0 0) ∨ (0 0 0 0 0 0 0 0 0 0 0 0 0 0) ∨ (1 1 0 0 0 0 0 0 0 0 0 0 0) ∨ (0 0 0 0 0 0 0 0 0 0 0 0 0) = (1 1 0 1 1 1 1 0 0 0 0 0 0)

Класс FIA (6 требований):

(0 1 0 1 1 1) ∨ (0 0 0 1 1 0) ∨ (0 0 0 0 0 0) ∨ (1 0 0 1 1 1) ∨ (0 0 0 0 0 0) ∨ (0 0 0 0 0 0) ∨ (0 1 0 1 1 0) ∨ (0 0 0 1 1 0) ∨ (0 0 0 0 0 0) ∨ (0 0 0 1 1 0) ∨ (0 0 0 0 0 0) = (1 1 0 1 1 1)

Класс FMT (6 требований):

(1 1 1 0 0 1) ∨ (1 1 1 0 0 1) ∨ (0 0 0 0 0 0) ∨ (1 1 1 0 0 0) ∨ (0 0 0 0 0 0) ∨ (0 0 0 0 0 0) ∨ (1 1 0 0 0 0) ∨ (0 0 0 0 0 0) ∨ (0 0 0 0 0 0) ∨ (1 1 1 0 0 0) ∨ (0 0 0 0 0 0) = (1 1 1 0 0 1)

Класс FPR (4 требования):

(0 0 0 0) ∨ (0 0 0 1) ∨ (0 0 0 0) ∨ (0 0 0 0) ∨ (0 0 0 0) ∨ (0 0 0 0) ∨ (0 0 0 0) ∨ (0 0 0 0) ∨ (0 0 0 0) ∨ (0 0 0 0) ∨ (0 0 0 0) = (0 0 0 1)

Класс FPT (16 требований):

(0 0 0 0 0 0 0 0 1 1 0 0 0 0 1 0) ∨ (1 0 0 0 0 0 0 1 0 0 0 0 0 0 0 1) ∨ (0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0) ∨ (0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 0 0) ∨ (0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0) ∨ (0 0 0 0 0 0 0 0 0 1 0 0 0 0 0) ∨ (0 0 0 0 0 0 0 0 0 1 1 0 0 1 0 0) ∨ (0 0 0 0 0 0 0 0 1 0 0 0 1 0 0 0) ∨ (0 1 0 0 0 0 0 1 0 1 0 0 0 0 0 0) ∨ (1 0 0 0 0 0 0 0 0 1 1 0 0 0 0 1) ∨ (1 1 0 0 0 0 0 1 1 0 1 0 0 0 0 1) = (1 1 0 0 0 0 0 1 1 1 1 0 1 1 1 1)

Класс FRU (3 требования):

(0 0 0) ∨ (0 0 0) ∨ (1 0 0)∨(0 0 0) ∨ (1 0 0) ∨ (0 0 0) ∨ (0 0 0) ∨ (0 0 0) ∨ (1 0 0) ∨ (0 0 0) ∨ (0 0 0) = (1 0 0)

Класс FTA (6 требований):

(0 0 0 0 0 0) ∨ (0 0 0 0 0 0) ∨ (0 0 0 0 0 0) ∨ (0 0 0 0 0 0) ∨ (0 0 0 0 0 0) ∨ (0 0 1 0 0 1) ∨ (0 0 0 0 0 0) ∨ (0 0 0 0 0 0) ∨ (0 0 0 0 0 0) ∨ (0 0 1 0 0 1) ∨ (0 0 0 0 0 0) = (0 0 1 0 0 1)

Класс FTP (2 требования):

(0 1) ∨ (0 1) ∨ (0 0) ∨ (0 0) ∨ (0 0) ∨ (0 1) ∨ (0 0) ∨ (0 0) ∨ (0 0) ∨ (0 0) ∨ (0 0) = (0 1)

Таким образом, в результате логического сложения матриц определяется набор функциональных требований безопасности, актуальных для исследуемого ОО [3].

В Таблице 2 представлено количество требований от каждого класса:

Таблица 2. *Распределение функциональных требований безопасности*

Класс требований	Матрицы требований	Количество актуальных требований, A	Общее количество требований, N
FAU	(1 1 1 1 1 0)	5	6
FCO	(0 0)	0	2
FCS	(1 1)	2	2
FDP	(1 1 0 1 1 1 1 0 0 0 0 0 0)	6	13
FIA	(1 1 0 1 1 1)	6	6
FMT	(1 1 1 0 0 1)	4	6
FPR	(0 0 0 1)	1	4
FPT	(1 1 0 0 0 0 0 1 1 1 1 0 1 1 1 1)	10	16
FRU	(1 0 0)	1	3
FTA	(0 0 1 0 0 1)	2	6
FTP	(0 1)	1	2

Пусть N_m - общее количество требований в классе m при m = (1, …, 11).

A_m - число актуальных требований из класса m при m = (1, …, 11).

Тогда отношение количества актуальных требований каждого класса к общему количеству требований:

$$\alpha_{\min m} = \frac{A_m}{N_m} \quad (1)$$

$\alpha_{min\ m}$ - показатель минимально допустимой входимости требований в класс. Тогда показатели минимально допустимой входимости для каждого класса функциональных требований безопасности:

$\alpha_{min\ 1} = 5/6 = 0{,}83$

$\alpha_{min\ 2} = 0/2 = 0$

$\alpha_{min\ 3} = 2/2 = 1$

$\alpha_{min\ 4} = 6/13 = 0{,}46$

$\alpha_{min\ 5} = 6/6 = 1$

$\alpha_{min\ 6} = 4/6 = 0{,}67$

$\alpha_{min\ 7} = 1/4 = 0{,}25$

$\alpha_{min\ 8} = 10/16 = 0{,}625$

$\alpha_{min\ 9} = 1/3 = 0{,}33$

$\alpha_{min\ 10} = 2/6 = 0{,}33$

$\alpha_{min\ 11} = 1/2 = 0{,}5$

Найдем сумму $S_{\alpha\ min}$ всех $\alpha_{min\ m}$:

$$S_{\alpha \min} = \Sigma \alpha_{\min m} \quad (2)$$

при m = (1, …, 11).

$S_{\alpha\ min} = 5{,}995$

$$\alpha_{max\ m} = 1 \quad (3)$$

$\alpha_{max\ m}$ - показатель максимально допустимой входимости требований в класс m при m = (1, …, 11).

В результате получаем целевую функцию, характеризующую защищенность ОО и представляющую собой математическую модель защищенной компьютерной сети:

$$\sum \frac{f_m(T_m)}{N_m} = 5{,}995 \quad (4)$$

при m = (1,…,11),

где $f_m(T_m)$ - логическая функция анализа, на основании которой осуществляется подбор функциональных требований безопасности [2].

Выражение (4) описывает защищенную компьютерную сеть в целом. Выражение (5) используется для организации защиты отдельных структурных элементов компьютерной сети:

$$0{,}166 * f_1(T_1) + 0{,}5 * f_2(T_2) + 0{,}5 * f_3(T_3) + 0{,}077 * f_4(T_4) + 0{,}166 * f_5(T_5) + 0{,}166 * f_6(T_6) + 0{,}25 * f_7(T_7) + 0{,}625 * f_8(T_8) + 0{,}33 * f_9(T_9) + 0{,}166 * f_{10}(T_{10}) + 0{,}5 * f_{11}(T_{11}) = 5{,}995 \quad (5)$$

При этом необходимо выполнения условия:

$$5{,}995 \le \sum \frac{f_m(T_m)}{N_m} \le 1 \quad (6)$$

при m = (1, …, 11).

В исследовании рассмотрена математическая модель синтеза защищённых компьютерных сетей в соответствии с руководящими документами в области информационной безопасности.

Разработанная модель основана на логическом анализе структуры защищенной сети, направлена на систематизирование и оптимизацию требований стандартов безопасности и представляет собой универсальную модель синтеза защищенной компьютерной сети.

Список литературы

1. **Бетелин В. Б., Галатенко В. А.** Профили защиты на основе «Общих критериев». М.: Jet Info, 2003. 32 с.
2. **Биячуев Т. А.** Безопасность корпоративных сетей. СПб.: СПбГУ ИТМО, 2004. 161 с.
3. **Вишневский В. М.** Теоретические основы проектирования компьютерных сетей. М.: Техносфера, 2003. 512 с.
4. **ГОСТ Р ИСО/МЭК 15408-2-2008.** Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. М.: Стандартинформ, 2009. 167 с.

УДК 811.112.2
Филологические науки

Павел Анатольевич Бородин
Московский государственный педагогический университет

К ВОПРОСУ ОБ ОСНОВНЫХ ЦЕННОСТЯХ В КУЛЬТУРЕ ОБЩЕНИЯ©

Сейчас никого уже не надо убеждать в том, насколько важно межкультурное общение в самых разных областях: бытовой, экономической, научной и др. Однако оно часто бывает затруднено или даже вообще прерывается потому, что представитель одной культуры ведет себя, по мнению представителя другой культуры, *неприемлемо*. На эту тему написано много практически-ориентированной литературы. Во многих таких «сборниках полезных советов» даются рекомендации, как следует вести или не следует себя с представителем иной культуры, как можно поступать с ним, а как нельзя. Например: «На встречу с немцем нельзя опаздывать», «Китайцы избегают числа четыре», «В гостях у русского не следует отказываться от спиртного» и т.п.

Однако почти никто до сих пор не задавался вопросом, из чего вытекают все эти предпочтения, запреты и т.д.

В декабре 2008 г. автор статьи присутствовал на лекции, которую читала в Москве г-жа профессор Гудрун Ершофф из ФРГ. Она является известным специалистом в области классической русской литературы, однако в последнее время активно занимается теорией и практикой межкультурной коммуникации. По её мнению, общение между русскими и немцами (особенно в деловой сфере) сильно затрудняется тем, что в немецкой культуре (точнее, в социокультурной области) присутствуют и постоянно репрезентируются «Grundwerte» («базовые ценности»)[1], в русской культуре отсутствующие. Г-жа проф. Ершофф выделила семь таких понятий:

- Sachorientierung (ориентация на дело);
- Wertschätzung von Strukturen und Regeln (высокая оценка структур и правил);
- Regelorientierte Kontrolle (контроль за соблюдением правил);
- Zeitplanung (планирование времени);
- Trennung von Lebensbereichen (разделение сфер жизни);
- Individualismus (*здесь*: самостоятельность и самоценность личности);
- Schwacher Kontext (*здесь*: прямота и ясность в общении).

Автор статьи очень во многом не согласен с позицией г-жи проф. Ершофф. Понятно, что невозможно жить в обществе, не соблюдая никаких правил, никак не планируя время, не осознавая себя как личность и т.д. Такое общество было бы в принципе нежизнеспособным.

Следовательно, в русской культуре эти понятия (или заменяющие их) существуют, но несут в себе иное содержание и формируют иную систему базовых ценностей.

Второе, и очень важное следствие существования и постоянной репрезентации в повседневности определенной системы ценностей заключается в том, что у этого явления не может не быть *отрицательных*

[1] Пер. с нем. везде - автора статьи.