тельное наполнение контента портала, более эффективную технологию обработки информации, что повлечет за собой повышение эффективности управления образовательным процессом в целом.

Литература.

1. Ризен Ю. С, Захарова А. А., Минин М. Г. Модель подготовки выпускника вуза и повышение эффективности применения образовательных технологий. // [Электронный ресурс] Режим доступа: http://www.problem-info.ru/2012-5/35.pdf (Дата обращения 23.03.14)
2. Захарова А. А. , Чернышева Т. Ю. , Молнина Е. В. Интегрированная траектория формирования компетенций будущего IT-специалиста // Профессиональное образование в России и за рубежом. - 2013 - №. 3(11). - С. 92-99
3. Захарова А. А. , Чернышева Т. Ю. , Молнина Е. В. Реализация ООП магистратуры «Прикладная информатика в аналитической экономике» в ЮТИ ТПУ [Электронный ресурс] // Уровневая подготовка специалистов: государственные и международные стандарты инженерного образования: сборник трудов научно-методической конференции, Томск, 26-30 Марта 2013. - Томск: ТПУ, 2013 - С. 81-83. - Режим доступа: http://www.lib.tpu.ru/fulltext/c/2013/C09/C09.pdf [8029-2013].
4. Молнина Е. В., Молнин С. А., Картуков К. С. Реализация комплексной системы формирования информационно-коммуникационной компетентности обучающихся через IT-университет // В мире научных открытий. - 2013 - №. 11.7(47). - С. 120-124.
5. Захарова А.А. Интегрированная инновационно-ориентированная траектория подготовки ИТ-специалиста //Качество. Инновации. Образование. 2010. № 1(56). С. 10-14
6. Панина Т.С., Дочкин С.А., Клецов Ю.В. Уровни информационно-коммуникационной компетентности педагогических работников // [Электронный ресурс] ГОУ ДПО «Кузбасский региональный институт развития профессионального образования». 2008. Режим доступа: http://www.krirpo.ru/etc.htm?id=744. (Дата обращения 23.03.14)
7. Багова Е.В., Букаев Ю.А., Токарев К. Е. Когнитивное моделирование процесса подготовки в ВУЗе. // [Электронный ресурс] Режим доступа: http://www.scienceforum.ru/2014/pdf/822.pdf (Дата обращения 23.03.14).
8. Марухина О.В., Берестнева О.Г. Определение показателей качества образовательного процесса на основе экспертного оценивания//Материалы VIIМеждународной НПК «Качество – стратегия XXI века»/Томское отделение академии качества, ТУСУР, 2002.- С. 112-114.
9. Берестнева О.Г. Моделирование интеллектуальной компетентности студента// Известия ТПУ. 2005. – Т.308. – №2. – С.152-156.
10. Берестнева О.Г. Качество обучения студентов в техническом ВУЗе. Томск: Изд-во ТПУ.– 2004. – 202 с.

АВТОРИЗАЦИИ ПОЛЬЗОВАТЕЛЕЙ В СИСТЕМЕ ГРАФИЧЕСКОГО ПАРОЛЯ С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ

А.В. Шокарев, к.т.н., доцент кафедры ИС, В.В. Останин, студент
Юргинский технологический институт (филиал) Национального исследовательского Томского политехнического университета
652055, Кемеровская обл., г. Юрга, ул. Ленинградская, 26
E-mail: Shokarev_AV@mail.ru

Введение.

Пользователи имеют определенную трудность запоминания сложных, псевдослучайных паролей в течение определенного времени. Большинство из них забывают пароль, который не используется регулярно в случае, когда пользователи имеют несколько паролей к различным системам, сегодня практически универсальное условие. Пользователь может или смешать элементы различных паролей или помнить пароль, но путать, какой системе это соответствует[7].

Пользователи обычно справляются с проблемами запоминания пароля, уменьшая сложность и число паролей, тем самым, уменьшая безопасность систем для взлома. Безопасный пароль должен быть не менее 8 символов, желательно случайным с верхними регистрами символов, символами нижнего регистра, цифрами, и специальными символами. С такими паролями у пользователя возникает проблема в запоминании. В большинстве случаев, пользователи игнорируют такие рекомендации, используя вместо этого короткие, простые пароли, которые являются относительно простыми для обнаружения. Практика показывает, что пользователи часто выбирают короткие пароли, состоящие из имен, фамилий семьи или друзей, названия домашних животных, и даже не редко встречается

слово "пароль"[7]. А чтобы не забывать пароли записывают их на бумагу, либо используют тот же самый пароль для многократных систем, иногда с единственной цифрой в конце.

Описание модели аутентификации системы графического пароля.

В связи с трудностью запоминания паролей и в связи с уменьшением степени защищенности систем пользователями, различными институтами и университетами по всему миру ведутся разработки систем графических паролей, призванных избавить пользователя от заучивания сложных паролей и повышения защищенности различных ресурсов[1,6]. Одним из недостатков разрабатываемых систем графических паролей является то, что большинство из них основаны на присвоении определенных символов изображению, выбранного пользователем для аутентификации. Предлагаемая далее система графических паролей на основе ЦВЗ избавлена от этого недостатка путем встраивания в графические файлы случайных символов, выработанных генератором случайных последовательностей[5].

Предлагаемая модель системы ЦВЗ для разграничения доступа пользователей к защищенным ресурсам, применяемая в построении системы графического пароля[10], показана на рисунке 1.

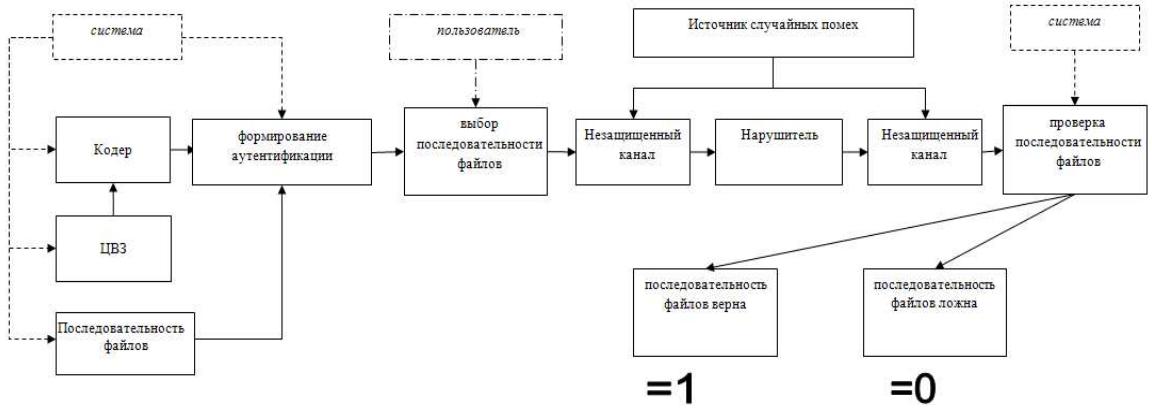


Рис. 1. Обобщенная модель системы для аутентификации

Системой предлагаются выбрать пользователю последовательность графических файлов, далее на все предложенные графические файлы система накладывает цифровой водяной знак W, индивидуальный для каждого графического объекта, который преобразовывается в кодере к удобному виду для встраивания в заверяемое сообщение. Алгоритм формирования такой конструкции водяного знака A представим в виде:

$A = F(I, W)$, где F - функция, зависящая от I – контейнер (графический файл), W – водяной знак.

Затем в формирователе заверенных сообщений конструкция водяного знака A встраивается с помощью функции Z в графический контейнер, используя конфиденциальный ключ K:

$Z = \Psi(A, I, K)$, где Ψ – функция, зависящая от A – конструкции водяного знака, I – контейнера (графического файла) и K – секретного ключа.

После выбора пользователем последовательности графических объектов для своей аутентификации система передает ее по каналу связи. В канале связи на заверенное сообщение Y воздействуют нарушитель, а также случайные и преднамеренные помехи. В результате этого воздействия на приеме в устройство проверки водяных знаков поступает модифицированное сообщение Y. По алгоритму обнаружения водяного знака формируется оценка водяного знака W' вида:

$W' = G(Y, W, K)$, где G – функция с зависимостями от Y – модифицированное сообщение, W – водяной знак, K – секретный ключ.

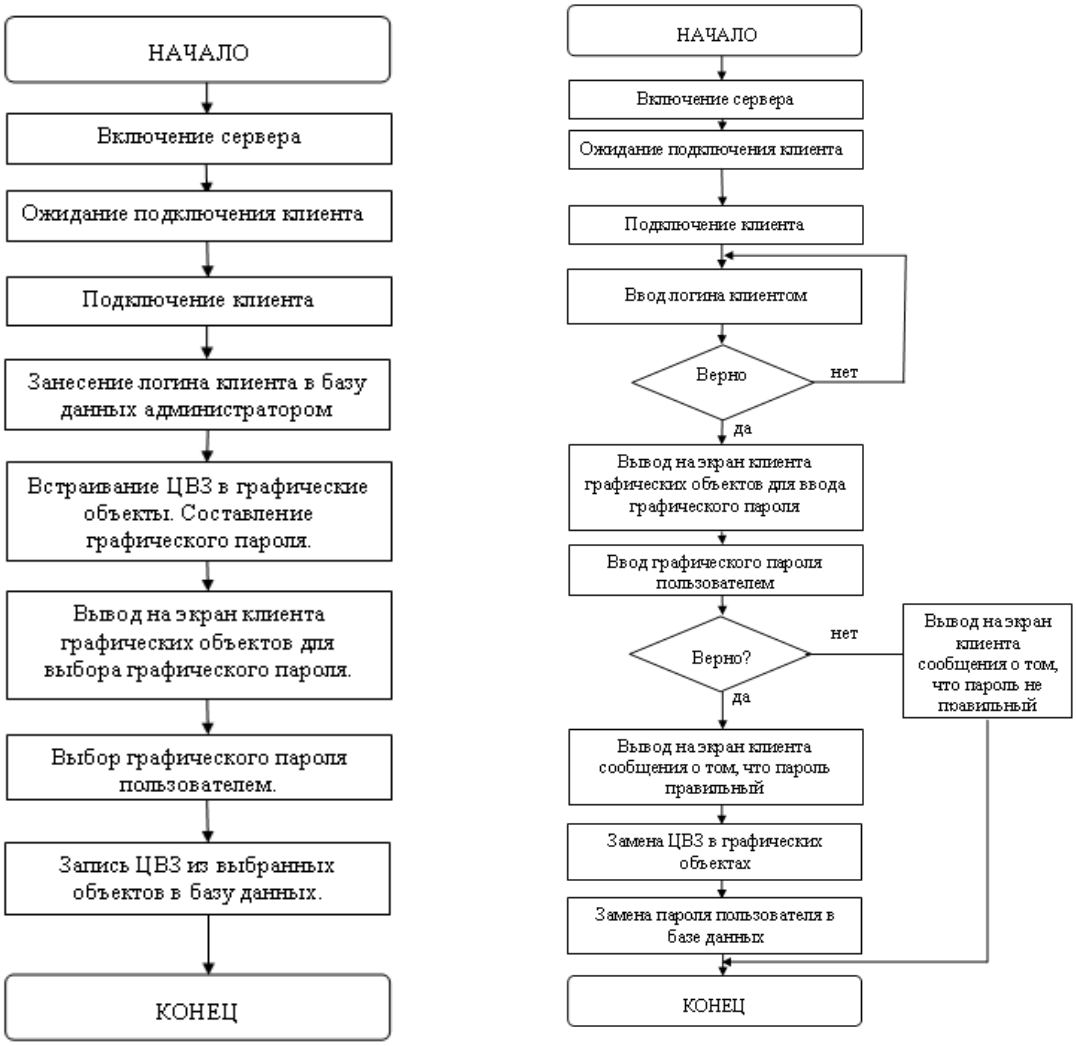
Подлинность пользователя определяется в соответствии с этой оценкой. Возможны решения вида W' = 1 (подлинность сообщения подтверждена) или W' = 0 (подлинность сообщения не подтверждена). Также возможны и другие решения вида $0,5 \le W_j' \le 1$ (j-й фрагмент скорее всего подлинный) или $0 \le W_j' < 0,5$ (j-й фрагмент скорее всего навязан или искажен помехами передачи). При формировании оценки водяных знаков могут возникнуть ошибки их обнаружения получателем сообщения[2,10].

Описание общей модели системы графического пароля.

По сравнению с криптографическими системами аутентификации, система аутентификации пользователей на основе ЦВЗ имеет следующие особенности:

- заверяемое сообщение и встроенный в него ЦВЗ взаимозависимы, то есть при разрушении первого разрушается и второй, а если водяной знак сохранил свою целостность, то и принятое сообщение ее не потеряло;
- при приеме искаженного фрагмента сообщения получатель может, не отказываясь от всего сообщения в целом, отказаться лишь от данного фрагмента.
- В отличие от сравнительных методов, методы контроля подлинности на основе водяных знаков обладают существенными достоинствами:
- высокой устойчивостью к удалению аутентификатора заверенного сообщения без разрушения самого сообщения;
- обнаружением несанкционированного копирования заверенных сообщений;
- согласованность с источниками сообщений, обладающими существенными статистическими зависимостью и памятью, такими как изображение и звуковой сигнал.

Полученная система графического пароля основывается на использовании стеганографических методов[4], которые повышают безопасность всей системы аутентификации по отношению к существующим системам графических паролей. Обобщенная модель регистрации и авторизации пользователя показана на рисунке 2.



а) б)

Рис. 2. а) регистрация нового пользователя, б) идентификация/аутентификация пользователя в системе графического пароля

Предлагаемая система имеет следующие этапы:

1. Регистрация пользователя:

а. Администратором системы выбираются N графических объектов, которые будут предложены пользователю для аутентификации;

б. Генератором генерируются случайные последовательности символов, состоящие как из цифр, так и из букв латиницы и кириллицы с различным регистром;

в. Стеганографической подсистемой выполняется встраивание полученных последовательностей в виде ЦВЗ с секретным ключом K;0

г. Пользователем либо администратором вводится имя будущего пользователя. Далее система графического пароля предлагает пользователю N выбранных администратором системы графических объектов уже со встроенными в них ЦВЗ, из которых он должен выбрать определенное количество <N и запомнить последовательность их выбора;

д. Серверная часть системы графического пароля заносит в базу данных нового пользователя и сопоставляет его логину извлеченные ЦВЗ в виде символов.

2. Аутентификация пользователя:

а. Для доступа к защищенному ресурсу клиентской частью системы графического пароля предлагается пользователю ввести свой логин и выбирать предлагаемые системой графические объекты в той же последовательности, что и при регистрации;

б. В серверной части происходит сравнение лигина пользователя и полученных ЦВЗ с имеющимися данными в базе данных. Если ЦВЗ совпадает с имеющейся последовательностью, то вход пользователя будет произведен, в обратном случае система сообщает о неправильном вводе данных;

в. В случае успешного выполнения входа системой генерируются новые последовательности символов и отправляются клиентской части для последующего встраивания во все имеющиеся N графические файлы. Новая последовательность, используемая в качестве пароля пользователя, вносится и в базу данных на сервере;

г. При следующем вызове клиентской части системы графические объекты располагаются случайным образом.

Алгоритм встраивания ЦВЗ состоит из трех основных этапов[3,4]:

- Генерации ЦВЗ
- Встраивания ЦВЗ в кодере
- Обнаружения ЦВЗ в детекторе.

Рассмотрим генерацию ЦВЗ.

Пусть W^*, K^*, I^* и B^* есть множества возможных ЦВЗ, ключей, контейнеров и скрываемых символов, соответственно. Тогда генерация ЦВЗ может быть представлена в виде:

$$F : I^* \times K^* \times B^* \to W^*, \qquad W = F(I,K,B),$$

где I,K,B – представители соответствующих множеств. Вообще говоря, функция F может быть произвольной, но на практике требования робастности ЦВЗ накладывают на нее определенные ограничения. Так, как в большинстве случаев, $F(I,K,B) \approx F(I+\varepsilon,K,B)$, то есть незначительно измененный контейнер не приводит к изменению ЦВЗ. Функция F обычно является составной:

$F = T \circ G$, где $G : K^* \times B^* \to C^*$ и $T : C^* \times I^* \to W^*$

Оператор T модифицирует кодовые слова C^*, в результате чего получается ЦВЗ W^*.На эту функцию можно не накладывать ограничения необратимости, так как соответствующий выбор G гарантирует необратимость F. Функция T должна быть выбрана так, чтобы незаполненный контейнер I_0, заполненный контейнер I_w и незначительно модифицированный заполненный контейнер I'_w порождали бы один и тот же ЦВЗ:

$$T(C,I_0) = T(C,I_w) = T(C,I_w)$$

То есть она должна быть робастной[9] и, соответственно устойчивой к малым искажениям контейнера.

Процесс встраивания ЦВЗ W(i,j) в исходное изображение I_0(i,j), описывается как суперпозиция двух сигналов:

$$\varepsilon : I^* \times W^* \times L^* \to I_w^*, \; I_w(i,j) = I_0(i,j) \oplus L(i,j)W(i,j)p(i,j).$$

Где L(i,j) маска встраивания ЦВЗ, которая учитывает характеристики зрительной системы человека и служит для уменьшения заметности ЦВЗ.

$p(i, j)$ является проектирующей функцией, зависящей от секретного ключа K. Цель данной функции состоит в том, чтобы распределить ЦВЗ по области графического файла.

Самой важной частью в стеганографической системе является стегодетектор[8]. В зависимости от типа он может выдавать решения различных систем исчисления о наличии либо отсутствии ЦВЗ (в случае детектора с мягкими решениями). Рассмотрим более простой случай «жесткого» детектора стего. Обозначим операцию детектирования через D. Тогда :

$$D: I_w^* \times K^* \to \{0,1\},\ D(I_w, W) = D(I_w, F(I_w, K)) = \begin{cases} 1, & \text{если } W \text{ есть} \\ 0, & \text{если } W \text{ нет} \end{cases}$$

Выводы.

Из описанных выше моделей аутентификации пользователей и системы графических паролей можно выделить основные требования к системам ЦВЗ, при использовании для авторизации пользователей в защищаемых системах. Данные системы должны обладать следующими свойствами:

- имитостойкостью, то есть невозможностью формирования нарушителем, не знающим конфиденциального ключа подписи, любого сообщения с формально верным водяным знаком;
- практическим отсутствием не обнаруживаемого несанкционированного копирования заверенного сообщения;
- при внедрении в один контейнер нескольких сообщения разными водяными знаками, должна прослеживаться очередность подписей, а сами подписи не должны разрушать друг друга;
- невозможностью отказа от авторства подписанного сообщения (для систем с конфиденциальным ключом подписи и открытым ключом проверки);
- невозможностью формирования получателем формально верного водяного знака отправителя сообщения (для систем с конфиденциальным ключом подписи и открытым ключом проверки);
- невозможностью удаления или разрушения водяного знака без разрушения самого сообщения;
- устойчивостью водяного знака к воздействию случайных и преднамеренных помех, не приводящих к разрушению информационного содержания заверенного сообщения;
- для формирования и проверки водяного знака сообщения не должно требоваться участие третьей доверенной стороны;
- сопрягаемостью с современными методами передачи, хранения, криптографической защиты и повышения помехоустойчивости;
- возможностью обработки заверенных сообщений стандартными методами (архивация, масштабирование, фильтрация, сжатие, и т. д.) без разрушения водяных знаков.

Безопасность предлагаемого метода аутентификации пользователя на основе ЦВЗ будет зависеть от нескольких факторов:

- чем больше графических объектов предлагается для выбора пользователю системой, тем труднее будет злоумышленнику осуществить перебор всех возможных вариантов;
- вход в систему должен осуществляться строгой последовательностью графических объектов, выбранной пользователем в качестве пароля;
- минимальная последовательность для аутентификации должна состоять не менее 3 графических объектов;
- графические объекты, подписанные ЦВЗ и выводимые на экран для аутентификации, должны размещаться на дисковом пространстве компьютера пользователя и содержать только его данные для аутентификации в системе. Это позволит избежать взлома всей системы;
- пользователь должен не иметь полных прав на использование защищаемого ресурса;
- при встраивании ЦВЗ должны использоваться неформатные методы;
- при каждом вызове диалогового окна система должна менять случайным образом графические объекты, выводимые на экран для аутентификации;
- после каждой успешной аутентификации пользователя должна происходить замена ЦВЗ на всех графических объектах, используемых для аутентификации пользователя (использование одноразовых паролей);
- система для устойчивости то взлома ЦВЗ должна использовать несколько методов встраивания.

Предлагаемый метод графического пароля обладает следующими отличительными особенностями:

- впервые используются ЦВЗ для идентификации/аутентификации пользователей в системах графического пароля.

- графические объекты меняется случайным образом, что делает систему не уязвимой при подглядывании или использовании программ регистрирующих нажатия клавиш и координаты выбора графических объектов мышью.
- использование ЦВЗ в качестве одноразовых паролей, делает систему не уязвимой при сетевом перехвате.
- размещение графических объектов для аутентификации на рабочем месте пользователя не дает нарушителю взломать систему в целом.

Заключение

Использование предложенного метода аутентификации позволяет пользователю быстрее запоминать пароли и увеличить стойкость систем графических паролей с использованием ЦВЗ к взломам злоумышленниками, а так же уменьшает время авторизации в системах пользователей. Описанная система графического пароля применяет разовые пароли для авторизации, и после успешного входа пользователя в систему автоматически происходит смена ЦВЗ в графических объектах, что, несомненно делает перехват передаваемой последовательности для авторизации бесполезным.

Литература.

1. Brostoff, S., Sasse M.A. Are Passfaces more usable than passwords: A field trial investigation // People and Computers XIV - Usability or Else, Proceedings of HCI, 2000. - P. 405-424.
2. Craver S. On public-key steganography in the presence of an active warden. //Proc. 2nd Intern Workshop on Inform. Hiding, 1998, LNCS, v.1525, 355-368.
3. Farid H. Detection Steganographic Message in Digital Images // Technical Report TR2001-412, 2001.
4. Petitcolas F.A., AndersonR.J., KuhnM.G. Information hiding – a survey //Proceeding of the IEEE, vol. 87, № 7, 1999, pp.1062–1078.
5. Shokarev A. V. Current Graphical Password Systems. Implementation Algorithms by Digital Watermarking // Applied Mechanics and Materials. - 2013 - Vol. 379. - p. 229-234
6. Sobrado L., Birget J.C., Graphical passwords. // The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, Vol. 4, 2002.
7. Афанасьев А.А., Веденьев Л.Т., Воронцов А.А.и др. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам // Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2009. – 552 с.
8. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. //М.: Солон-Пресс, 2009. – 272с.
9. Шелупанов А.А, Шокарев А.В. Теоретико-информационный и Теоретико-сложностный подходя для оценки стойкости стеганографических систем //Вестник СибГАУ «Системная интеграция и безопасность». – Красноярск, 2006. – Спец. выпуск. С.121-123
10. Шокарев А.В. Использование цифровых водяных знаков для аутентификации передаваемых сообщений //Вестник СибГАУ «Системная интеграция и безопасность». – Красноярск, 2006. – Спец. выпуск. С.123-127

ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ ИНВЕСТИЦИОННОЙ ДЕЯТЕЛЬНОСТИ В МАШИНОСТРОЕНИИ РОССИИ

А.Н. Алексеев, д.э.н, проф.
Московский университет им. С.Ю. Витте
115432, г. Москва, 2-й Кожуховский проезд, д. 12, стр. 1, тел. (495)783-68-48
E-mail: alexeev_alexan@mail.ru

Развитие машиностроения длится уже более двух веков и по объемам выпускаемой продукции отрасль занимает первое место среди всех отраслей мировой промышленности. Несомненно, что уровень развития машиностроения является одним из важнейших показателей уровня развития всей национальной экономики. В развитой рыночной экономике машиностроительная отрасль традиционно имеет социально-ориентированный и инфраструктурный оттенок, с учетом достижений технического прогресса может регулировать конкурентные условия для большинства отраслей промышленности. Для России, с её чрезмерно развитым топливно-энергетическим комплексом, поступательное развитие машиностроения является важнейшим условием устойчивого экономического роста и повышения благосостояния граждан.

Исследованию экономических и управленческих проблем развития отраслей промышленности и, в частности, машиностроения посвящены труды таких отечественных исследователей, как Л.И. Абалкин, С.Ю. Глазьев, Р.С. Гринберг, В.Ю. Комаров, В.И. Маевский, Н.Н. Миронова, М.И. Мурака-