Раздел II. Защита информационных процессов в компьютерных системах

УДК 004.056

П.М. Присталов, А.С. Афанасьев

РАЗРАБОТКА МОДЕЛИ УГРОЗ СИСТЕМ ТЕСТИРОВАНИЯ

Целью исследования является формирование требований безопасности к системам удаленного компьютерного тестирования на основании модели угроз, учитывающей в первую очередь угрозы получения необъективных результатов тестирования. На основании требований безопасности возможно создание систем удаленного компьютерного тестирования с определенным уровнем защищенности.

Система тестирования; угроза; уязвимость; модель нарушителя.

P.M. Pristalov, A.S. Afanasiev

DEVELOPMENT OF SECURITY REQUIREMENTS FOR REMOTE TESTING SYSTEM

This article is dedicated to development of security requirements for remote testing system based for threat model that consider the threat of reception of nonobjective result as the main one. In account of security requirements it's probable to create a remote testing system with desirable safety level.

Testing system; threat; exposure; violator's model.

Общие положения

В последнее время в нашей стране уделяется особое внимание качеству образовательных услуг, о чем свидетельствует принятие и проведение приоритетной национальной программы «Образование», а также множество проводимых в данной сфере реформ. Перестройка системы образования приводит к появлению новых принципов и подходов к проведению учебного процесса, содержанию программ, а также контролю результатов.

Контроль результатов как одна из важнейших задач образовательного учреждения осуществляется различными способами: путем сдачи зачетов, экзаменов, защиты курсовых и дипломных работ, проведением контрольных и самостоятельных работ и т.д. Оценка качества перечисленных выше работ зависит от мнения принимающего их лица, а значит, является субъективной.

К формам контроля знаний учащихся, которые в большей степени объективны, следует отнести тестирование, а также проверку знаний независимыми экспертами. И если проведение экспертной оценки знаний является достаточно редким явлением и используется в случаях, когда крайне важно получить объективную

оценку знаний ученика или студента (например, при проведении ЕГЭ), то тестирование используется в учебных заведениях весьма часто.

К причинам широкого распространения тестирования можно отнести следующие:

- простота процесса тестирования, а также составления тестов и их проверки;
- относительно высокая объективность результатов тестирования;
- возможность проведения удаленного контроля знаний посредством рассылок ранее составленных тестов;
- возможность автоматизации тестирования.

Автоматизированные системы тестирования в настоящее время чрезвычайно распространены. В учебных заведениях используется множество компьютерных приложений для тестирования знаний обучаемых, различающихся в основном программной архитектурой.

Использование компьютерных систем тестирования, как и любых других компьютерных программ, связано с созданием, накоплением, обработкой, передачей, хранением и уничтожением информации. В рассматриваемом случае некоторая информация, циркулирующая в системе, может представлять интерес для тестируемого. В случае если тестируемый имеет возможность читать, создавать, модифицировать или удалять данные, он теоретически сможет повлиять на объективность результатов.

Ясно, что при проверке знаний обучаемых при помощи автоматизированных средств компьютерного тестирования для таких средств необходимо обеспечить соответствующий уровень защищенности путем разработки, внедрения, применения и усовершенствования политики безопасности. Для этого необходимо для каждой конкретной архитектуры приложения выявить уязвимости, определить актуальные угрозы, модель нарушителя, а также выработать механизмы защиты.

Целью работы является построение модели угроз для различных реализаций систем тестирования, определение актуальных угроз и возможных уязвимостей, а также моделей нарушителя и рекомендаций по защите таких систем от преднамеренных атак. Система должна быть построена таким образом, чтобы было возможно проведение на ее основе удаленного тестирования знаний студентов.

Предполагается, что результаты исследований, проводимых в рамках данной работы, будут использоваться при проектировании программных систем тестирования студентов, разрабатываемых и используемых в Пензенском государственном университете для удаленного обучения, а также при проведении текущего контроля знаний учащихся.

Разработка информационно-логической модели систем тестирования

Как сказано выше, данная работа проводится с целью построения модели угроз для последующего определения методов защиты различных реализаций систем тестирования. Эти методы разнятся в зависимости от программной архитектуры, на которой построена система. Для обеспечения возможности проведения удаленного тестирования, очевидно, необходимо использовать архитектуру «клиент-сервер». В соответствии с методикой, описанной в ГОСТ 15408, для построения модели угроз необходимо выполнить следующие основные шаги: спроектировать структуру информационной разрабатываемой системы; определить ресурсы, подлежащие защите; установить наиболее критичные ресурсы, описать возможные методы нападения, после чего предложить механизмы защиты [1].

На первом этапе разработки информационно-логической модели систем тестирования необходимо определить цель организации.

В Уставе Пензенского государственного университета сказано, что «основной целью образовательной деятельности Университета… является повышение образовательного и культурного уровня населения Российской Федерации, подготовка и воспитание специалистов с высшим образованием и специалистов высшей квалификации по характерному для университетов широкому спектру уровней, направлений, специальностей и научных направлений обучения и в соответствии с действующими образовательными программами».

Достижение цели производится путем выполнения множества функций, среди которых можно выделить следующие основные:

– проведение научных изысканий по различным направлениям;
– подготовка, переподготовка, повышение квалификации работников с высшим образованием и научно-педагогических работников высшей квалификации.

Каждая из описанных функций состоит из ряда более мелких подфункций, так, например, подготовка специалистов предполагает контроль их знаний, проводимый в соответствии с действующими образовательными стандартами.

Одним из методов такого контроля является проведение тестирования студентов по основным образовательным дисциплинам. Зачастую тестирование проводится в компьютерных классах при помощи автоматизированных систем.

Как сказано выше, для таких систем необходимо разрабатывать политику безопасности. Рассматривая подфункцию проведения тестирований как часть функции подготовки, переподготовки и повышения квалификации специалистов, представим ее в виде процесса, для которого можно выделить следующие характеристики:

– входной информацией являются вопросы к тесту, варианты ответов на вопросы теста, ответы тестируемого на вопросы теста;
– процесс обработки информации представляет собой сравнение ответов тестируемого на вопросы теста с правильными ответами;
– выходной информацией является результат прохождения теста в виде оценки тестируемого, выставляемой по определенной шкале.

Описание процесса позволяет идентифицировать информационные ресурсы, которые участвуют в процессе. Ими будут:

– перечень вопросов теста;
– варианты ответов на вопросы теста;
– правильные ответы на вопросы теста;
– ответы тестируемого на вопросы теста;
– результат проверки ответов тестируемого.

По степени критичности относительно доступности могут быть следующие виды информации:

– *критическая* – информация, без которой работа системы останавливается;
– *очень важная* – информация, без которой система может работать, но очень короткое время;
– *важная* – информация, без которой система может работать некоторое время, но рано или поздно она понадобится;
– *полезная* – информация, без которой система может работать, но ее использование экономит ресурсы;

– *несущественная* – устаревшая или неиспользуемая информация, не влияющая на работу системы.

По степени критичности относительно целостности могут быть следующие виды информации:

– *критическая* – информация, несанкционированное изменение которой приведет к неправильной работе системы; последствия модификации необратимы;
– *очень важная* – информация, несанкционированное изменение которой приведет к неправильной работе системы через некоторое время, если не будут предприняты некоторые действия; последствия модификации необратимы;
– *важная* – информация, несанкционированное изменение которой приведет к неправильной работе системы через некоторое время, если не будут предприняты некоторые действия; последствия модификации обратимы;
– *значимая* – информация, несанкционированное изменение которой скажется через некоторое время, но не приведет к сбою в работе системы; последствия модификации обратимы;
– *незначимая* – информация, несанкционированное изменение которой не скажется на работе системы.

По степени критичности относительно конфиденциальности могут быть выделены следующие виды информации:

– *критическая* – информация, разглашение которой приведет к невозможности реализации целей системы;
– *очень важная* – информация, разглашение которой приведет к значительному ущербу, если не будут предприняты некоторые действия;
– *важная* – информация, разглашение которой приведет к незначительному ущербу, если не будут предприняты некоторые действия;
– *значимая* – информация, разглашение которой приведет только к моральному ущербу;
– *незначимая* – информация, разглашение которой не влияет на работу системы.

В табл. 1 представлены оценки степени критичности информационных ресурсов относительно свойств информационной безопасности.

Исходя из данных табл. 1, можно выделить основные угрозы информационным ресурсам процесса тестирования в виде угроз нарушения целостности, доступности и конфиденциальности информации:

– несанкционированное чтение перечня вопросов теста;
– несанкционированная модификация перечня вопросов теста;
– несанкционированное удаление перечня вопросов теста;
– несанкционированное чтение вариантов ответов на вопросы теста;
– несанкционированная модификация вариантов ответов на вопросы теста;
– несанкционированное удаление вариантов ответов на вопросы теста;
– несанкционированное чтение правильных ответов на вопросы теста;
– несанкционированная модификация правильных ответов на вопросы теста;
– несанкционированное удаление правильных ответов на вопросы теста;
– несанкционированное чтение ответов тестируемого на вопросы теста;

- несанкционированная модификация ответов тестируемого на вопросы теста;
- несанкционированное удаление ответов тестируемого на вопросы теста;
- несанкционированное чтение результатов проверки ответов тестируемого;
- несанкционированная модификация результатов проверки ответов тестируемого;
- несанкционированное удаление результатов проверки ответов тестируемого.

Таблица 1

Степени критичности ИР

	По степени критичности относительно доступности	По степени критичности относительно целостности	По степени критичности относительно конфиденциальности
Перечень вопросов теста	*Критическая*	*Критическая*	*Незначимая*
Варианты ответов на вопросы теста	*Критическая*	*Критическая*	*Очень важная*
Правильные ответы на вопросы теста	*Критическая*	*Критическая*	*Очень важная*
Ответы тестируемого на вопросы теста	*Критическая*	*Критическая*	*Значимая*
Результат проверки ответов тестируемого	*Критическая*	*Критическая*	*Незначимая*

Описание угроз для системы тестирования

После того как определены актуальные угрозы, можно определить наиболее вероятные атаки, при помощи которых угрозы могут быть реализованы. Очевидно, что к наиболее вероятным атакам можно отнести следующие:

- подсказки со стороны не проходящего тестирование лица (преподавателя, системного администратора, контролирующего лица и тд.), а также со стороны других тестируемых;
- списывание из имеющихся бумажных и электронных источников;
- поиск информации в режиме онлайн;
- атака на передаваемые по сети данные;
- атака на систему с целью нарушения ее работы либо подмены данных.

Разработка защитных мер

Исходя из необходимости защиты от описанных выше угроз, был сформулирован перечень требований к защите проектируемой системы тестирования.

Во-первых, весь трафик между клиентом и сервером должен быть зашифрован с использованием отечественных криптоалгоритмов, а также алгоритма рас-

пределения ключей Диффи–Хеллмана. Во-вторых, система должна обеспечивать непрерывную запись и потоковую передачу аудио- и видеоданных, снимаемых соответственно с микрофона и веб-камеры, установленных на рабочем месте тестируемого. Эти данные обрабатываются и передаются в отдельных потоках, а на стороне сервера записываются в один файл при помощи стандартных кодеков. Система должна быть защищена от исследования, атак на пароли и ключи сессий, а также от атак типа «отказ в обслуживании». При запуске программы-клиента системы тестирования всем остальным приложениям должен блокироваться доступ к сети, а также передача информации в другие окна и обработка системных сигналов. Сервер приложения должен обеспечивать ведение логов, а также журнала аудита событий безопасности.

В результате применения данных защитных мер при разработке системы тестирования создана защищенная система компьютерного тестирования, позволяющая проводить тесты даже в условиях неконтролируемой среды.

В настоящее время проводится отладка и тестирование данной системы, а также проверяется надежность ее работы в условиях преднамеренных и непреднамеренных атак.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *В.М. Алексеев* Оценка защищенности информационной системы организации: Методические указания к практическим занятиям. – Пенза: Изд-во Пензенского гос. ун-та, 2006. – 39 с.

Афанасьев Алексей Сергеевич
ГОУВПО «Пензенский государственный университет».
E-mail: ghost_87@mail.ru.
440000, г. Пенза, ул. Лермонтова, 26.
Тел.: 8 (902) 347-4428.
Кафедра информационной безопасности систем и технологий; студент.

Afanasev Aleksey Sergeevich
Penza State University.
E-mail: ghost_87@mail.ru.
26, Lermontov str., Penza, 440000, Russia.
Phone: 8 (902) 347-4428.
The Department of Information Security of Systems and Technologies; student.

Присталов Павел Михайлович
ГОУВПО «Пензенский государственный университет», г. Пенза.
E-mail: pripav@rambler.ru.
440000, г. Пенза, пр-т Победы, 84, кв. 144.
Тел.: 8 (904) 265-9185.
Кафедра информационной безопасности систем и технологий; студент.

Pristalov Pavel Mihailovich
Penza State University.
E-mail: pripav@rambler.ru.
App. 144, 84, Pobedy avenue, Penza, 440000, Russia.
Phone: 8 (904) 265-9185.
The Department of Information Security of Systems and Technologies; student.