В.В. Гуров

ВЛИЯНИЕ ЧЕЛОВЕЧЕСКОГО ФАКТОРА НА ЗАЩИЩЕННОСТЬ ПРОГРАММНЫХ СРЕДСТВ УЧЕБНОГО НАЗНАЧЕНИЯ

V.V. Gurov
National Nuclear Research University MEPHI, 115409, Moscow, Kashirskoe sh., 31, e-mail: vvgurov@mephi.ru

The influence of human factor on security of software intended for educational purposes

Keywords:educational software, Attack Tree , information security
The report considers the construction and analysis of attack tree on the software tools intended for educational purposes. This takes into account different groups of attackers. The criterion of security for such tools is introduced.

В.В. Гуров
Национальный исследовательский ядерный университет «МИФИ», 115409, г. Москва, Каширское ш., 31, e-mail: vvgurov@mephi.ru

ВЛИЯНИЕ ЧЕЛОВЕЧЕСКОГО ФАКТОРА НА ЗАЩИЩЕННОСТЬ ПРОГРАММНЫХ СРЕДСТВ УЧЕБНОГО НАЗНАЧЕНИЯ

Ключевые слова: обучающие программные средства, дерево атак, защищённость информации
В настоящее время подавляющее большинство вузов в своем учебном процессе используют различные программные средства учебного назначения (ПСУН). Программы данного типа играют важную роль в учебном процессе, о чём свидетельствуют многочисленные публикации в различных источниках [1-7]. В разработке таких средств участвует большой коллектив людей, включая студентов, профессорско-преподавательский, инженерный и обслуживающий персонал. Защищенность данных программных средств (ПС) во многом определяется квалификацией и мотивацией каждого из членов коллектива (зачастую, таких коллективов может быть несколько). В данной статье рассматриваются вопросы повышения защищённости ПСУН на основе использования несанкционированного доступа в виде дерева атак и введённого критерия защищённости таких средств.

Программные средства учебного назначения включают в себя педагогические, обучающие, контролирующие, демонстрационные программные средства, а также ПС для тренажеров, для моделирования и т.д. [8]. Одним из важнейших показателей качества любой программной системы является её защищенность. Согласно [9], защищенность – это совокупность свойств программного средства, характеризующая его способность предотвращать несанкционированный доступ как случайный, так и умышленный, к программам и данным, а также степень удобства и полноты обнаружения результатов такого доступа или действий по разрушению программ и данных. С точки зрения атак на ПСУН, наибольший интерес для злоумышленника представляют те из них, которые влияют на выставление итоговой оценки по какой-либо дисциплине, а именно, контролирующие программные средства, а также программные средства для тренажеров и компьютерные обучающие программы, включающие в себя контроль результатов обучения. В данной работе рассматриваются вопросы, связанные с умышленным несанкционированным доступом.

Одним из методов определения защищенности ПС является построение дерева атак на данное программное средство [10]. Дерево атак – это методология описания угроз и мер противодействия для защиты системы. Дерево состоит из узлов типа И и типа ИЛИ. Узлы И представляют собой отдельные шаги для достижения одной цели. ИЛИ – это узел альтернатив, позволяющих достичь цели. Завершив построение дерева, необходимо присвоить определённые значения листьям деревьев, чтобы оценить достижимость цели злоумышленниками. Эти

значения могут базироваться на различных показателях: степень необходимых специальных знаний, время на достижение цели, степень риска для нападающего и т.д.

Уточняя определённые характеристики атак, можно узнать больше о защищенности системы. Точность данной модели зависит от целого ряда факторов. Одним из таких факторов является портрет потенциального злоумышленника.

Лиц, предпринимающих атаки на те или иные программные системы, можно разделить на различные группы. Например, в [10] выделены следующие группы:

- нарушители-одиночки,
- злонамеренные посвященные лица,
- промышленные шпионы,
- организованные преступные группы,
- полиция,
- национальные разведывательные организации.

В области компьютерных обучающих программ наибольший интерес представляет деятельность первых двух групп атакующих.

В литературе имеется целый ряд исследований личности нарушителя-одиночки [11-15] применительно к различным областям использования компьютерных технологий. В случае несанкционированного доступа к программам учебного назначения к таким лицам можно отнести студентов, пытающихся получить хорошую оценку с помощью несанкционированного доступа к ПСУН.

Другая группа потенциальных злоумышленников – это злонамеренные посвященные лица. Атака со стороны посвященных лиц менее вероятна, чем со стороны посторонних, но системы гораздо более уязвимы перед ними. Посвященные лица не всегда нападают на систему, иногда они просто используют ее в преступных целях. В наиболее серьезных с точки зрения безопасности случаях посвященное лицо имеет высокую квалификацию, и еще хуже, если оно участвовало в проектировании системы. Мотивация нападений посвященных лиц может быть различна: месть, финансовая выгода или даже реклама. Степень риска, на который готовы идти злонамеренные посвященные лица, зависит от того, движимы они "высокой целью", например, продемонстрировать своё якобы имеющееся превосходство в данной области, или простой жадностью.

По данным ряда статистических исследований большинство компьютерных преступлений совершается при непосредственном участии служащих данной организации. Так результаты анализа, приведенные в [16], показывают, что до 70% компьютерных преступлений в банковской сфере совершается при непосредственном участии самих служащих банков. Эти действия не всегда носят заведомо преступный характер, а зачастую совершаются просто по беспечности. Так проведенный в Великобритании социологический опрос среди работников организаций, чья деятельность связана с информационными технологиями, показал, что 35% опрошенных были готовы дать свой личный пароль для доступа в компьютерную систему компании незнакомому человеку просто так, ещё 11% попросили бы за такую услугу небольшой презент [12]. В ФБР была разработана специальная "Матрица компьютерных преступников", описывающая их обобщенные типы по категориям правонарушителей с указанием организационных, рабочих, поведенческих, ресурсных характеристик.

Злонамеренных посвященных лиц в области проектирования и использования ПСУН можно разбить на два класса:

1) разработчики программ;
2) обслуживающий персонал.

Программные системы учебного назначения могут поставляться специализированными фирмами – разработчиками программного обеспечения. В то же время ряд программ, особенно

в технических вузах, создается сравнительно небольшим коллективом, в состав которого, как правило, входят аспиранты, студенты старших, а иногда и младших курсов, работающие под руководством преподавателя.

В случае поставки программных средств сторонней организацией вряд ли следует опасаться наличия в них каких-либо "закладок" или специальных "дыр", которые обеспечат несанкционированный доступ к ним. Получение высокой оценки конкретным студентом за конкретный вид работы – не та цель, которая может преследоваться солидной фирмой. В то же время студенты – разработчики программ могут рассматриваться в качестве потенциальных злоумышленников.

Ситуация, когда часть работы выполняется временными сотрудниками, является типичной для большинства компаний. По статистике [17] в любой компании мира работает от 5 до 10% временных сотрудников. К таким временным сотрудникам можно отнести и студентов – членов творческих коллективов по разработке ПСУН. При оценке их влияния на защищенность системы следует учитывать характеристики их личности. В некоторых источниках, например, работе [18], особое внимание уделяется тем личным качествам программиста, которые могут, в той или иной степени, оказать влияние на надежность и безопасность разрабатываемого им программного обеспечения. К таким качествам относятся

- внутренняя/внешняя управляемость;
- высокая/низкая мотивация;
- умение быть точным.

Эти и ряд других качеств необходимо учитывать при оценке веса тех листьев в дереве атак, которые определяются разработчиками соответствующих программных средств.

Таким образом, в нашем случае мы имеем дело со следующими потенциальными злоумышленниками:

1) студенты, изучающие данный курс,
2) студенты, участвовавшие и, возможно, продолжающие участвовать, в разработке ПСУН для данного курса;
3) обслуживающий персонал.

Структура дерева атак определяется формой организации учебного процесса, принятой в данном учебном заведении, а может быть, даже в его отдельном подразделении, и зависит от специфики изучаемой дисциплины.

Рассмотрим наиболее распространенную форму, при которой оценка за курс определяется оценками за выполнение определенного количества электронных уроков, входящих в состав лабораторного практикума, и оценок за проводимое с той или иной частотой тестирование по различным разделам курса. Получение общей высокой оценки включает наличие высоких оценок по каждой составляющей, то есть корневой узел дерева – это узел типа И.

Получить максимально высокую оценку за электронный урок можно различными способами, например:

– получить доступ к исходному коду урока с целью исправить его таким образом, чтобы получать высокую оценку при любом реальном выполнении программы;

– запускать программу многократно до получения хорошей оценки, чтобы именно этот результат продемонстрировать преподавателю;

– и, наконец, просто исправить итоговую оценку в протоколе результатов выполнения электронных уроков.

Хорошие результаты тестирования могут быть получены

– путем взлома базы данных тестирования (БД вопросов и ответов или БД результатов тестирования);

– многократным запуском системы тестирования с фиксацией правильных ответов на отдельные вопросы с тем, чтобы при контрольном тестировании получить необходимый результат.

При этом дерево атак будет иметь вид, представленный на рис.1.
Оно построено для следующих условий функционирования ПСУН:
– отсутствует система автоматической регистрации результатов выполнения электронного урока;
– режим доступа к используемым базам данных (логины, пароли) не меняется на протяжении цикла обучения по данной дисциплине;
– анализ результатов тестирования проводится преподавателем после каждого теста.

Вероятность достижения поставленной злоумышленником цели можно оценить, рассматривая все возможные пути, ведущие к вершине дерева, и оценивая вероятности достижения всех промежуточных узлов. Таким образом, приходим к взвешенному ориентированному графу, вес каждой вершины которого определяется конкретными условиями использования.

Рис. 1. Дерево атак на программные системы учебного назначения

Рассмотрим случай, когда оценка за любую работу не дифференцируется и выставляется по принципу "зачёт-незачёт", общая оценка складывается из оценок за выполнение двух электронных уроков и двух тестирований. Тогда граф, получаемый на основе рассмотренного дерева атак, будет иметь вид, представленный на рис.2. Вершины X введены в граф для наглядности.

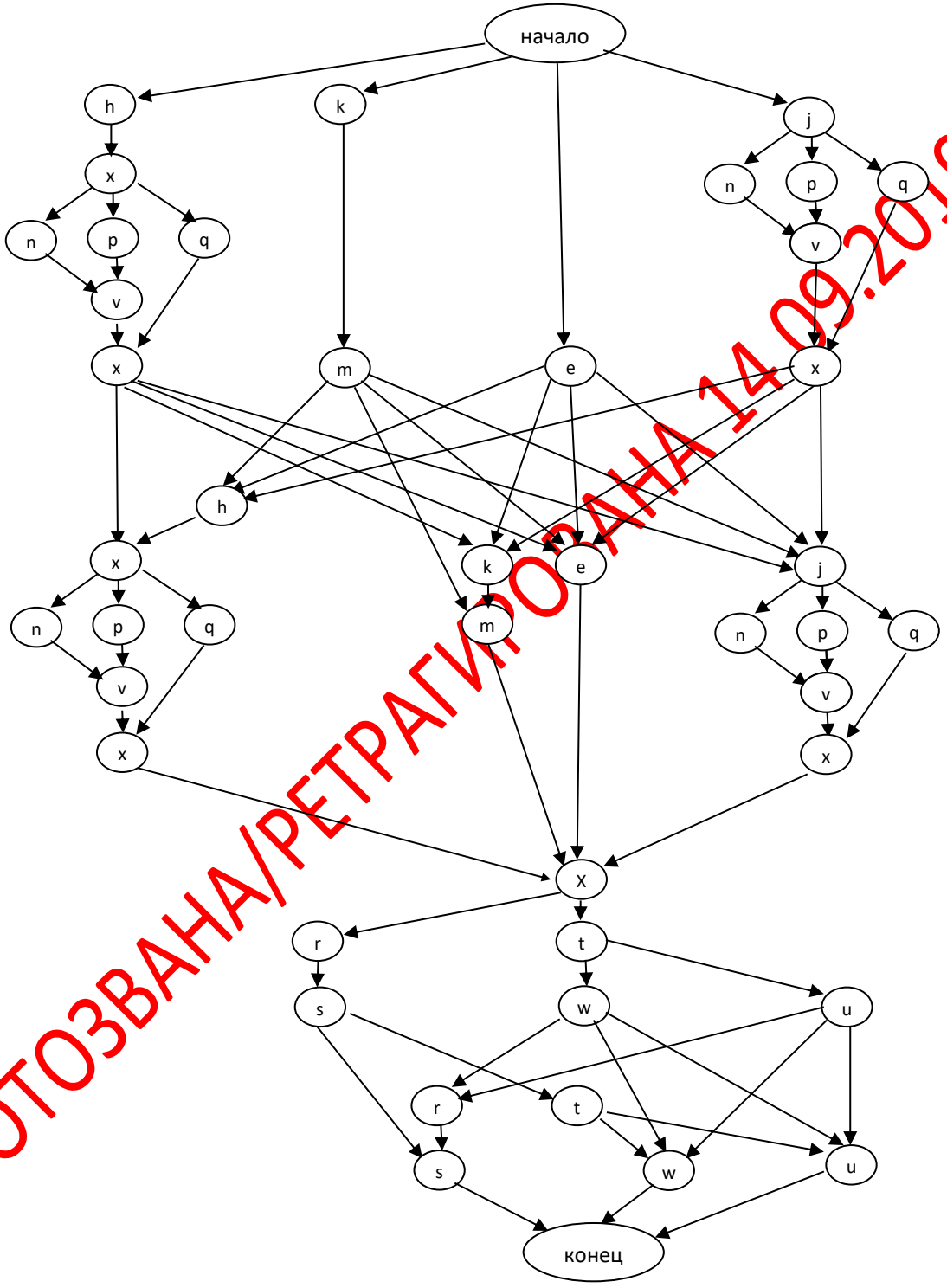

Рис.2. Граф атак на программные средства учебного назначения

Согласно существующей статистике, в коллективах людей, занятых той или иной деятельностью, как правило, только около 85% являются вполне лояльными (честными), а остальные 15% делятся примерно так: 5% могут совершить что-нибудь противоправное,

если, по их представлениям, вероятность заслуженного наказания мала; 5% готовы рискнуть на противоправные действия, даже если шансы быть уличенным и наказанным складываются 50 на 50; 5% готовы пойти на противозаконный поступок, даже если они почти уверены в том, что будут уличены и наказаны [17].

В области ПСУН подобной статистики пока не существует, но можно предположить, что она будет близка к указанным цифрам. Исходя из этого, положим, что около 5% обслуживающего персонала готовы всё-таки на содействие злоумышленникам из корыстных либо каких-то иных соображений. Такую вероятность и заложим для узлов, связанных с доступом к БД через злонамеренных лиц из обслуживающего персонала. Вероятность достижения цели при этом будет зависеть от квалификации злоумышленника и сложности действий, которые необходимо выполнить с базой данных.

Возможность самостоятельной модификации программы, базы данных или получение информации из БД злоумышленником зависит от его квалификации. Однако в случае, если он получает соответствующее программное средство на неограниченный или, по крайней мере, весьма длительный срок, можно полагать, что атакующий найдёт возможности взломать любую программу. В последнее время появились стандартные методы взлома, почти все этапы взлома формализованы и подробно описаны на хакерских сайтах. В интернете для свободного доступа выложено множество хакерских программ, например, [18-21] (поиск незащищенных систем, получение к ним доступа, получение паролей, удалённое управление компьютером). Большинство из этих программ имеет интуитивно понятный интерфейс и руководство к действию.

Некоторые оценки доступности тех или иных вершин графа атак в зависимости от используемого режима программных средств представлены в табл.1. Вероятность доступа к вершинам графа, связанным с доступом к серверу, существенно возрастает в случае, когда используется локальный вариант работы, при котором фактически доступ к серверу заменяется получением программного средства с персонального компьютера. При этом для совершения несанкционированного действия может не потребоваться помощь обслуживающего персонала. Для студентов – разработчиков программ ввиду временного характера творческого коллектива доступна лишь часть всех программных систем учебного назначения: система тестирования или один электронный урок. Для них в этом случае вероятность получения соответствующего программного средства равна 1. В остальных случаях они оцениваются как и прочие студенты. Многократный запуск программы до получения хорошего результата возможен лишь в случае отсутствия регистрации действий пользователя.

Таблица 1. Вероятность успешного выполнения действия злоумышленником при различных режимах работы

Узел	**Действие**	**Злоумышленник**		
		Студент	**Студент - разработчик электронного урока**	**Студент - разработчик системы тестирования**
h	Получить программу электронного урока с сервера	0,05**	0,05**	0,05**
j	Получить программу у разработчика электронного урока	0,05	1	0,05
k	Получить доступ к БД результатов электронных уроков	0,05**	0,05**	0,05**

Узел	Действие	Злоумышленник		
		Студент	Студент - разработчик электронного урока	Студент - разработчик системы тестирования
m	Исправить запись в БД результатов электронных уроков	0,5	0,5	0,5
n	Заменить вывод на высокую оценку при любом реальном ответе	0,5	1*	0,5
p	Внести изменения в текст урока с целью генерации только заранее известных вариантов	0,5	1*	0,5
e	.Запускать программу многократно до появления хорошей оценки	0,7***	0,7***	0,7***
q	Сформировать образ экрана, на который выводится хорошая оценка за урок	0,5	1*	0,5
v	Поместить исправленный текст урока на сервер	0,05**	0,05**	0,05**
r	Получить доступ к БД результатов тестирования	0,05**	0,05**	0,05**
s	Исправить запись в БД результатов тестирования	0,5	0,5	1
t	Получить доступ к БД тестирования	0,05**	0,05**	0,05**
w	Прочитать вопросы и ответы в БД тестирования	0,5	0,5	1
u	Многократно запускать тест для определения правильных ответов	0,5	0,5	0,8

* – только для одного электронного урока
** – для сетевого режима использования
*** – для локального режима использования без протоколирования результатов

Полученный граф атак на ПСУН может использоваться для определения мест системы, которые в наименьшей степени защищены от несанкционированного доступа. В то же время хорошая система безопасности объединяет три звена: предупреждение, обнаружение, реагирование. Поэтому целесообразно рассмотреть не только вероятность достижения цели злоумышленником по тому или иному пути дерева атак, но и вероятность его обнаружения на этом пути. С этой целью для каждого узла дерева атак необходимо указать вероятность того, что действия злоумышленника здесь не будут обнаружены. Данные вероятности также должны определяться отдельно в каждом конкретном случае использования ПСУН.

Предполагаем, что при сетевом режиме работы доступ к программным средствам проводится обслуживающим персоналом и поэтому не может быть обнаружен. Однако, если в этом случае попытаться заменить какой-либо электронный урок на другую версию программы, которая всем пользователям будет выдавать высокую оценку, то такие действия будут обнаружены с высокой вероятностью. При локальном режиме злоумышленник получает программы со своего персонального компьютера. Вероятность

того, что его действия в этом случае не будут обнаружены, положим равной 0,5. Исходя из этого, представим такие вероятности в табл.2. Здесь полагаем, что вероятность обнаружения попыток взлома системы со стороны всех трех выделенных ранее групп злоумышленников одинакова.

Таблица 2. Вероятность необнаруженных действий злоумышленника при различных режимах работы

Узел	Действие	Злоумышленник
h	Получить программу электронного урока с сервера	$1_а/0{,}2_б$**
j	Получить программу у разработчика электронного урока	1
k	Получить доступ к БД результатов электронных уроков	$1_а/0{,}2_б$**
m	Исправить запись в БД результатов электронных уроков	0,5**
n	Заменить вывод на высокую оценку при любом реальном ответе	0,5/0,1*
p	Внести изменения в текст урока с целью генерации только заранее известных вариантов	0,8/0,3*
e	.Запускать программу многократно до появления хорошей оценки	0,1
q	Сформировать образ экрана, на который выводится хорошая оценка за урок	0,3/0,1*
v	Поместить исправленный текст электронного урока на сервер	$1_а/0{,}2_б$**
r	Получить доступ к БД результатов тестирования	$1_а/0{,}2_б$**
s	Исправить запись в БД результатов тестирования	$1_а/0{,}2_б$**
t	Получить доступ к БД тестирования	$1_а/0{,}2_б$**
w	Прочитать вопросы и ответы в БД тестирования	$1_а/0{,}2_б$**
u	Многократно запускать тест для определения правильных ответов	0,5

* – для локального/сетевого режима работы
** – для сетевого режима использования
а – при доступе через злонамеренных лиц из обслуживающего персонала
б – при самостоятельном доступе

Реакция на обнаруженную атаку зависит от особенностей учебного процесса и администрирования ПСУН. Возможные реакции на некоторые обнаруженные атаки представлены в табл.3.

Таблица 3. Возможные реакции на обнаруженные атаки

Ситуация	Реакция
Атака обнаружена, но не выявлено конкретное лицо, ее предпринявшее	Пересмотр дерева атак с целью усиления защиты тех мест, на которые была предпринята атака
Атака со стороны обслуживающего персонала	Принятие административных мер
Атака со стороны студента – разработчика электронного урока	Принятие административных мер к студенту. Исключение данного урока из учебного процесса.
Атака со стороны студента – разработчика системы тестирования	Принятие административных мер к студенту. Модернизация системы тестирования.
Атака со стороны студента, изучающего данную дисциплину.	Принятие административных мер к студенту. В зависимости от объекта атаки и её успешности возможно исключение данного программного средства из учебного процесса или его существенная модернизация.

В.В. Гуров

ВЛИЯНИЕ ЧЕЛОВЕЧЕСКОГО ФАКТОРА НА ЗАЩИЩЕННОСТЬ ПРОГРАММНЫХ СРЕДСТВ УЧЕБНОГО НАЗНАЧЕНИЯ

Механизмы реакции на возможные атаки должны закладываться, по возможности, на ранних стадиях проектирования программных средств, которые будут внедряться в учебный процесс.

Представленный анализ показывает, что защищенность различных частей системы зависит не только от вероятности успешного преодоления злоумышленником его защиты, но и от вероятности обнаружения таких действий. Поэтому для определения наиболее опасных с точки зрения несанкционированного доступа путей проникновения злоумышленников в систему введем критерий защищенности системы. Определим его следующим образом:

$$F = \max_{i \in N} \frac{P_i}{P_{i\,\text{обн}}} \qquad (1)$$

где P_i – вероятность достижения цели злоумышленником на i-м пути, $P_{i\,\text{обн}}$ – вероятность того, что его действия будут обнаружены на этом пути; N – количество всех путей, ведущих к цели.

Коэффициентом защищенности j-й вершины на i-м пути будем называть величину, равную отношению вероятности выполнения злоумышленником действия, характеризующего эту вершину (P_{ij}), к вероятности того, что это действие будет обнаружено ($P_{ij\,\text{обн}}$): $A_{ij} = \frac{P_{ij}}{P_{ij\,\text{обн}}}$. Тогда формулу (1) можно представить в следующем виде:

$$F = \max_{i \in N} \left\{ \frac{\prod_{j \in N_i} P_{ij}}{\prod_{j \in N_i} P_{ij\,\text{обн}}} \right\} = \max_{i \in N} \prod_{j \in N_i} A_{ij} \qquad (2)$$

где N_i – i-й путь графа атак.

В этом случае задача проектирования структуры программных систем учебного назначения с точки зрения их защищенности требует минимизации величины критерия (2) защищенности системы.

Оценка вероятностей достижения цели различными группами злоумышленников и вероятности обнаружения этих действий была проведена методом экспертных оценок среди преподавателей – разработчиков и пользователей ПСУН, обслуживающего персонала, студентов – разработчиков ПСУН и студентов, использующих эти средства в учебном процессе. Полученные экспертные оценки, а также расчетные значения коэффициента защищенности вершин от обычного студента при сетевом режиме использования ПСУН без помощи злонамеренных лиц из обслуживающего персонала, приведены в табл.4.

Таблица 4. Экспертные оценки коэффициентов защищенности вершин

Узел	**Вероятность успешного выполнения действия злоумышленником, P_{ij}**	**Вероятность обнаружения действий злоумышленника, $P_{ij\,\text{обн}}$**	**Коэффициент защищенности вершины, A_{ij}**
q	0,651	0,500	1,303
j	0,333	0,276	1,203
e	0,534	0,571	0,936
u	0,543	0,468	0,870
w	0,365	0,430	0,848
h	0,379	0,468	0,810
r	0,280	0,403	0,695
k	0,312	0,486	0,643
t	0,281	0,458	0,613
m	0,310	0,510	0,609
s	0,333	0,612	0,544
n	0,265	0,526	0,503

Узел	Вероятность успешного выполнения действия злоумышленником, P_{ij}	Вероятность обнаружения действий злоумышленника, $P_{ij}^{обн}$	Коэффициент защищенности вершины, A_{ij}
p	0,258	0,552	0,468
v	0,181	0,643	0,281

Выводы

Представленный в статье подход позволяет определить критические пути в дереве атак на основании критерия (2). Поиск таких путей может осуществляться различными математическими методами, например, по алгоритмам Дийкстры, Флойда или по волновому алгоритму [22]. Так как защищённость системы определяется наиболее слабым её звеном, то разработка структуры программных средств, обеспечивающей повышения защищенности узлов на критическом пути позволит повысить защищенность системы в целом.

СПИСОК ЛИТЕРАТУРЫ:

1. Tao Yuan Experiment and Analysis on Setting on Some Computer Lessons for Academician Who Is Major in Math in Normal University. Procedia Engineering, Volume 15, 2011, Pages 4157-4161

2. Hasegawa, D. ; Sakuta, H. Student interactions with e-learning systems: User and topic analysis. Ugurlu, Y. Global Engineering Education Conference (EDUCON), 2014 IEEE, 45 – 49 INSPEC Accession Number: 14351196, Conference Location : Istanbul DOI: 10.1109 / EDUCON.2014.6826066 .

3. Özcan Özyurt, Hacer Özyurt. Learning style based individualized adaptive e-learning environments: Content analysis of the articles published from 2005 to 2014. Computers in Human Behavior. Volume 52, November 2015, Pages 349-358.

4. Tatyana Filippova. Priority Fields of E-learning Development in Russia. Procedia - Social and Behavioral Sciences. Volume 206, 17 October 2015, Pages 348-353

5. Dina Bakalo, Artem Grigoryev. EFL Teaching in the E-Learning Environment: Updated Principles and Methods Julia Shishkovskaya, Procedia - Social and Behavioral Sciences. Volume 206, 17 October 2015, Pages 199–204 XVth International Conference "Linguistic and Cultural Studies: Traditions and Innovations"

6. Lucia Kovacova, Martina Vackova. Implementation of e-learning into the Process Security Education in Universities. Procedia - Social and Behavioral Sciences, Volume 182, 13 May 2015, Pages 414-419.

7. Tomáš Moravec, Petr Štěpánek, Petr Valenta. The Influence of Using E-learning Tools on the Results of Students at the Tests. Procedia. Social and Behavioral Sciences, Volume 176, 20 February 2015, Pages 81-86.

8. Общероссийский классификатор продукции ОК 005-93 ОКП, утвержденный Постановлением Госстандарта России от 30 декабря 1993 г. N 301. Издание официальное, тома 1 - 2, Госстандарт России, М., 1995.

9. ГОСТ 28806-90. Качество программных средств. Термины и определения. – Госстандарт России, г.Москва, 1990.

10. Шнайер Брюс Секреты и ложь. Безопасность данных в цифровом мире. – СПб.: Питер, 2003, 368 с.

11. Букин М. В доступе отказать. - PC WEEK , 09.01.2008. [Электронный ресурс] – Режим доступа: http://www.pcweek.ru/themes/detail_print.php?ID=105619&print= Y

12. Вершинин М. Современные молодежные субкультуры: хакеры. [Электронный ресурс] – Режим доступа: http://psyfactor.org/lib/vershinin4.htm#8

13. К 2008 году число персональных компьютеров в мире достигнет миллиарда: Лента.ru. 12 июня 2007. [Электронный ресурс] – Режим доступа: http://www.lenta.ru/

14. Стенг Д., Мун С. Секреты безопасности сетей. – К.: "Диалектика", 1995.

15. Сырков Б. Компьютерная преступность в России. Современное состояние. – //Системы безопасности связи и телекоммуникаций, 1998, №21. – С.70-72.

16. Дорошенко Н. Современная карьера.- //Власть денег, Июль 2006, (№92) [Электронный ресурс] – Режим доступа: (http://www.vd.net.ua/journals/articles-1321).

17. Казарин О.В. Безопасность программного обеспечения компьютерных систем. – М.: Изд. МГУЛ, 2003, 212 с. ISBN 5-283-01667 УДК 621.382.26 [Электронный ресурс] – Режим доступа: http://www.compdoc.ru/secur/protect/safesoftware/

18. Кто такой хакер. [Электронный ресурс] – Режим доступа: http://determion.narod.ru/hacker.html

19. Peter Sommer Criminalising hacking tools Digital Investigation, Volume 3, Issue 2, June 2006, Pages 68-72 DOI: 10.1016 / j.diin.2006.04.005

20. Paul Marks Expired emails provide easy route to hacking 8 New Scientist Volume 218, Issue 2916, 11 May 2013, DOI: 10.1016 / S0262-4079 (13) 61176- 21

21. Fred Donovan Year of the Hack Infosecurity Volume 8, Issue 6, November–December 2011, Pages 8–10 doi:10.1016/S1754-4548(11)70077-8

22. Харари, Ф. Теория графов; пер. с англ. – изд. 4-е. – М.: Либроком, 2009. – 300 с. ISBN 978-5-397-00622-4

REFERENCES:

1. Tao Yuan Experiment and Analysis on Setting on Some Computer Lessons for Academician Who Is Major in Math in Normal University. Procedia Engineering, Volume 15, 2011, Pages 4157-4161

2. Hasegawa, D. , Sakuta, H. Student interactions with e-learning systems: User and topic analysis. Ugurlu, Y. Global Engineering Education Conference (EDUCON), 2014 IEEE, 45 – 49 INSPEC Accession Number: 14351196, Conference Location : Istanbul DOI: 10.1109 / EDUCON.2014.6826066 .

3. Özcan Özyurt, Hacer Özyurt. Learning style based individualized adaptive e-learning environments: Content analysis of the articles published from 2005 to 2014. Computers in Human Behavior. Volume 52, November 2015, Pages 349-358.

4. Tatyana Filippova. Priority Fields of E-learning Development in Russia. Procedia - Social and Behavioral Sciences. Volume 206, 17 October 2015, Pages 348-353

5. Dina Bakalo, Artem Grigoryev. EFL Teaching in the E-Learning Environment: Updated Principles and Methods Julia Shishkovskaya, Procedia - Social and Behavioral Sciences. Volume 206, 17 October 2015, Pages 199–204 XVth International Conference "Linguistic and Cultural Studies: Traditions and Innovations"

6. Lucia Kovacova, Martina Vackova. Implementation of e-learning into the Process Security Education in Universities. Procedia - Social and Behavioral Sciences, Volume 182, 13 May 2015, Pages 414-419.

7. Tomáš Moravec, Petr Štěpánek, Petr Valenta. The Influence of Using E-learning Tools on the Results of Students at the Tests. Procedia. Social and Behavioral Sciences, Volume 176, 20 February 2015, Pages 81-86.

8. All-Russian classification of products. OC 005-93 OCP. – Moscow, 1995.

9. GOST 28806-90. The software quality. Terms and definitions. – Moscow, 1990.

10. Schneier Bruce. Secrets and lies. Data security in the digital world. – SPb, Piter, 2003.

11. Bukin M. Access to refuse, from http://www.pcweek.ru/themes/detail_print.php?ID=105619&print= Y

12. Vershinin M. Modern youth subcultures: hackers, from http://psyfactor.org/lib/vershinin4.htm#8

13. By 2008, the number of personal computers in the world will reach billion, from https://lenta.ru/news/2007/06/12/billion/

14. Steng D., Mun S. Secrets security networks, Kiev, Dialectika, 1995.

15. Syirkov B. Computer crime in Russia. The modern condition. – //Security and telecommunications, 1998, №21. – P.p. 70-72.

16. Doroshenko N. Modern career, from http://www.vd.net.ua/journals/articles-1321.

17. Kazarin O. V. Security software of computer systems, from http://www.compdoc.ru/secur/protect/safesoftware/ ISBN 5-283-01667

18. Who is the hacker, from http://determion.narod.ru/hacker.html

19. Peter Sommer Criminalising hacking tools Digital Investigation, Volume 3, Issue 2, June 2006, Pages 68-72 DOI: 10.1016 / j.diin.2006.04.005

20. Paul Marks Expired emails provide easy route to hacking 8 New Scientist Volume 218, Issue 2916, 11 May 2013, DOI: 10.1016 / S0262-4079 (13) 61176- 21

21. Fred Donovan Year of the Hack Infosecurity Volume 8, Issue 6, November–December 2011, Pages 8–10 doi:10.1016/S1754-4548(11)70077-8

22. Harari, F. Graph theory – Moscow, Librocom, 2009. ISBN 978-5-397-00622-4