Министерство образования и науки Российской Федерации

Калужский филиал

федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный технический университет имени Н.Э. Баумана

(национальный исследовательский университет)»

(КФ МГТУ им. Н.Э. Баумана)

С.Н. Гончаренко, О.С. Макарова

**Изучение методов поиска оптимальных стратегий в условиях информационных конфликтов**

Лабораторный практикум

по курсу «Теория принятия решений в условиях информационных конфликтов»

Калуга, 2018

УДК 519.83

Лабораторный практикум составлен в соответствии с учебным планом КФ МГТУ им. Н.Э. Баумана по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация – «Анализ безопасности информационных систем»).

Лабораторный прктикум рассмотрен и одобрен:

- кафедрой «Защита информации» (ИУ6-КФ)

протокол № \_\_\_ от \_\_\_\_\_\_\_\_\_\_\_\_\_ 2018 г.

Зав. кафедрой ЭИУ6-КФ\_\_\_\_\_\_\_\_\_\_­­­­­\_\_д.т.н., доцент Мазин А.В.

- методической комиссией факультета ИУ

протокол № \_\_\_ от \_\_\_\_\_\_\_\_\_\_\_\_\_ 2018 г.

Председатель метод. комиссии\_\_\_\_\_\_\_\_\_\_\_к.т.н., доцент Адкин М.Ю.

- методической комиссией КФ МГТУ им. Н.Э. Баумана

протокол № \_\_\_ от \_\_\_\_\_\_\_\_\_\_\_\_\_ 2018 г.

Председатель метод. комиссии \_\_\_\_\_\_\_\_\_\_ д.э.н., профессор Перерва О.Л.

Рецензент \_\_\_\_\_\_\_\_\_\_\_ зав. кафедрой ИУ2-КФ, к.т.н., доцент Чухраев И.В.

Авторы \_\_\_\_\_\_\_\_\_\_\_ ассистент кафедры ИУ6-КФ Макарова О.С.

\_\_\_\_\_\_\_\_\_\_\_ д.т.н., профессор кафедры ИУ6-КФ Гончаренко С.Н.

Аннотация

В лабораторном практикуме рассмотрены основные методы поиска оптимальных стратегий в условиях информационных конфликтов, используемые в сфере информационной безопасности, приведены требования к отчету и порядок выполнения лабораторных работ.

© Калужский филиал МГТУ им. Н.Э. Баумана, 2018 г.

Кафедра ИУ6-КФ, 2018 г.

© Макарова О.С., 2018 г.

© Гончаренко С.Н., 2018 г.

ОГЛАВЛЕНИЕ

[Правила безопасности при выполнении лабораторных работ 4](#_Toc526424572)

[Требования к оборудованию 4](#_Toc526424573)

[Модуль 1. Принятие решений в антагонистических конфликтах 5](#_Toc526424574)

[Лабораторная работа № 1.1 5](#_Toc526424575)

[Лабораторная работа № 1.2 10](#_Toc526424576)

[Модуль 2. Принятие решений в неантагонистических конфликтах 16](#_Toc526424577)

[Лабораторная работа № 2.1 16](#_Toc526424578)

[Лабораторная работа № 2.2 21](#_Toc526424579)

[Модуль 3. Многошаговые процессы принятия решений 25](#_Toc526424580)

[Лабораторная работа № 3.1 25](#_Toc526424581)

[Лабораторная работа № 3.2 31](#_Toc526424582)

[Литература 37](#_Toc526424583)

[ПРИЛОЖЕНИЕ А 38](#_Toc526424584)

**Правила безопасности при выполнении лабораторных работ**

1. Запрещается часто включать и выключать компьютер без необходимости.
2. Запрещается прикасаться к экрану и тыльной стороне блоков компьютера.
3. Запрещается работать на средствах вычислительной техники и перифирийном оборудовании мокрыми руками.
4. Запрещается работать на средствах вычислительной техники и перифирийном оборудовании, имеющих нарушение целостности корпуса, нарушения изоляции проводов, неисправную индикацию включения питания, с признаками элетрического напряжения на корпусе.
5. Запрещается класть на средства вычислительной техники и перифирийное оборудование посторонние предметы.

**Требования к оборудованию**

1. Компьютер уровня не ниже, чем Pentium/RAM 128 MB/HDD 1 GB.
2. Операционная система Windows версии 2000 или выше с типовым вариантом установки.
3. Среда разработки Microsoft Visual Studio версии 2005 или выше.
4. Офисная программа Microsoft Office версии 2003 или выше типовым вариантом установки.

**Модуль 1. Принятие решений в антагонистических конфликтах**

**Лабораторная работа № 1.1**

**Решение матричной игры «злоумышленник-администратор» в «чистых» стратегиях**

**Цель работы:** формирование практических навыков решения матричной игры «злоумышленник-администратор» в «чистых» стратегиях.

**Задачи:**

1. Составить модель матричной игры «злоумышленник-администратор».
2. Проанализировать алгоритм нахождения седловой точки.
3. Программно реализовать алгоритм нахождения верхней цены игры, нижней цены игры и седловой точки по заданной платежной матрице для решения задачи «злоумышленник-администратор» в «чистых» стратегиях.
4. Оформить отчёт.

**Теоретические сведения**

Противостояние администратора и злоумышленника – это *конфликт*, т.е. противоборство двух сторон с противоположными интересами, которые каждая сторона пытается удовлетворить, используя ту или иную стратегию действий, и при которых невозможно прийти к удовлетворяющему обе стороны соглашению по поводу находящегося в распрояжени администратора информационного ресурса.

Флормализация содержательного описания конфликта представляет собой математическую модель, которую называют *игрой*, а участника конфликта – *игроками*.

Игровая модель конфликта применяется для оценки и прогнозирования достигнутого уровня защиты информации с учетом выбора наиболее оптимальной стратегии поведения игроков. Предполагается, что при многократном повторении игры реализация оптимальных стратегий обеспечит администратору макмимально возможную защиту компьютерной системы.

Таким образом, теория игр позволяет представить задачу по защите компьютерной системы в математическом виде, позволяющем воспользоваться разработанными критериями нахождения оптимальных стратегий защиты, придерживаясь которых администратор способен устранить, или по крайней мере свести к минимуму наносимый злоумыленником ущерб хранящейся информации, а кроме того, наиболее точным образом оценить затраты на обеспечение безопасности информационного ресурса.

Методика применения теории игр в сфере информационной безопасности:

1. Постановка теоретико-игровой задачи, которая заключается в том, что задача организации защиты компьютерной системы представляетсся в терминах и понятиях теории игр. Определяются игрки, их число и стратегии, платежные функции. Очевидно, что игроки – это системные администраторы и злоумышленники. Сратегии администраторов состоят из программно-аппаратных средств защиты, находящихся в их распрояжении, а стратегии злоумышленников – это способы взлома серверов и способы атак на них.
2. Выбор и построение теоретико-игровой модели (типа игры) конфликта (игры). Иначе говоря, решается вопрос, о какой игре идет речь – матричной или биматричной, с полной или неполной информацией и т.д.
3. Решение игры (нахождение оптимальных стратегий).
4. Анализ решения и его реализация в организации защиты компьютерной системы.

**Порядок выполнения лабораторной работы**

Рассмотрим игру с нулевой суммой администратора со стратегиями и злоумышленника, имеющего стратегии .

Матрица игры – это матрица затрат, которые надо понести для закупки и установки защитного обрудования и программ против каждой угрозы (в тыс. руб.). Одновременно это урон, который наносит злоумышленник в случае спешной атаки, и, следовательно, это выигрыш злоумышленника.

Составим модель матричной игры «злоумышленник-администратор»:



Проанализируем алгоритм нахождения седловой точки:



Величина  называется нижней ценой игры или максиминным выигрышем, или максимином. Стратегия, соответствующая максимину , называется максиминной стратегией.

Величина  называется верхней ценой игры или минимаксным выигрышем, или минимаксом. Стратегия, соответствующая минимаксу , называется минимаксной стратегией.

Принцип осторожности, диктующий игрокам выбор соответствующих стратегий (максиминной и минимаксной), называется принципом минимакса.

Играми с седловой точкой называются игры, для которых нижняя цена игры равна верхней  или .

Общее значение нижней и верхней цены игры  называется чистой ценой игры. Соответствующие седловой точке стратегии ,  называются оптимальными, они образуют равновесную ситуацию или решение игры.

Программно реализуйте алгоритм нахождения верхней цены игры, нижней цены игры и седловой точки по заданной платежной матрице для решения задачи «злоумышленник-администратор» в «чистых» стратегиях.

В случае отсутствия седловой точки в матрице, программа выводит соответствующее сообщение на экран.

Элементы матрицы задаются пользователем с клавиатуры или случайным образом.

**Форма отчётности по выполнению лабораторной работы**

Индивидуальный отчет студента должен быть представлен в распечатанной форме с типовым титульным листом. Отчет должен содержать:

1. Цель.
2. Задачи.
3. Модель матричной игры «злоумышленник-администратор»
4. Листинг программы.
5. Результат работы программы.
6. Выводы.

**Контрольные вопросы и задания**

1. Дайте определение следующим понятиям: ход, стратегия, оптимальная стратегия, цена игры, решение в «чистых стратегиях».
2. Сформулируйте задачи выполненного лабораторного исследования и выводы по выполненной работе.
3. Дайте характеристику программному обеспечению, задействованному в проведении лабораторных работ.
4. Раскройте методику проведения выполненного лабораторного исследования.
5. Выполните анализ и интерпретируйте результаты выполненных лабораторных исследований, оцените их соответствие теоретическим ожиданиям.
6. Приведите классификацию игр.
7. Поясните алгорит нахождения седловой точки.

**Лабораторная работа № 1.2**

**Поиск стратегий обороны в киберпространстве**

**Цель работы:** формирование практических навыков поиска стратегий обороны в киберпространстве.

**Задачи:**

1. Изучить метод Крамера и метод Лагранжа для решения матричных игровых задач размерности nxn.
2. Провести сравнительный анализ методов решения игровых задач размерности nxn.
3. Программно реализовать один из методов решения матричных игр nxn для поиска оптимальных стратегий обороны в киберпространстве.
4. Оформить отчёт.

**Теоретические сведения**

Появление и развитие Интернета привело к тому, что многие государственные частные оргаанизации, финансовые учреждения стали полагаться на него в повседневной деятельности.

Как результат, появилась возможность осуществлять враждебные действия против этих организаций, учреждений и государств через Интернет, которые могут быть взаимными, поэтому правомерным стало появление для компьютерного противостояния в пространстве Интернета, называемого киберпространством, такого термина, как «кибервойна».

Кибервойна – это использование одним государством киберпространства и связанных с ним технологических и информационных средств с целью причинения вреда военной, технологической, экономический политической и информационной безопасности и суверенитету другого государства.

***Решение матричных игр методом Крамера***

Пусть платёжная матрица выглядит следующим образом:



Требуется определить оптимальные стратегии игроков ,  и цену игры .

Замечание: Поскольку данный метод опирается на теорему об активных стратегиях, перед началом решения задачи необходимо убедиться в том, что все стратегии являются активными, т.е. отсутствуют седловая точка и заведомо невыгодные стратегии.

Определим оптимальную стратегию  игрока А в предположении, что А применяет свою оптимальную смешанную стратегию, а В – свои чистые стратегии:



 - условие нормировки.

Далее для нахождения  применяем метод Крамера:



Применив соотношение нормировки, получим:



Подставив выражение для цены игры в формулы для расчета , получим:



Аналогично определяем оптимальную стратегию игрока В, считая, что В применяет оптимальную смешанную стратегию, а А – свои чистые стратегии: 

 - условие нормировки.

В результате использования метода Крамера для решения данной системы уравнений получаем вероятности применения стратегий игрока В:



**Порядок выполнения лабораторной работы**

Предположим, что в распоряжении группы В, отвечающей за компьютерную безопасность, находятся *n* серверов. Группа, в силу ограниченности ресурсов, способна обеспечивать эффективную безопасность только одного сервера. Пусть ценность сервера *i* равна и все числа различны. В таком случае математическое ожидание ущерба, наносимого нападающей стороной А в том случае, если сторона В защищает сервер *j*, а противник нападает на сервер *i*, равно:

,

где *p* – вероятность того, что сервер остается работоспособным и, следовательно, (1-*p*) – это вероятность того, что защита сервера сломана.

Нападающая сторона стремится нанести максимальный ущерб оборонающейся стороне А, которая в свою очередь делает всё, чтобы минимизировать свои потери Интересы сторон антагонистичны, и конфликт можно описать как матричную игру с матрицей выигрышей:

Предположим, что p=0.75.

Используя метод Крамера, описанный в теоретической части, осуществите поиск оптимальных стратегий обороны в киберпространстве.

**Форма отчётности по выполнению лабораторной работы**

Индивидуальный отчет студента должен быть представлен в распечатанной форме с типовым титульным листом. Отчет должен содержать:

1. Цель.
2. Задачи.
3. Листинг программы.
4. Результат работы программы.
5. Выводы.

**Контрольные вопросы и задания**

1. Дайте определение следующим понятиям: активная стратегия.
2. Приведите правила сокращения игровой задачи.
3. Сформулируйте задачи выполненного лабораторного исследования и выводы по выполненной работе.
4. Дайте характеристику программному обеспечению, задействованному в проведении лабораторных работ.
5. Раскройте методику проведения выполненного лабораторного исследования.
6. Выполните анализ и интерпретируйте результаты выполненных лабораторных исследований, оцените их соответствие теоретическим ожиданиям.
7. Раскройте суть метода Крамера при поиске стратегий обороны в киберпространстве.
8. Приведите теорему об активных стратегиях.

**Модуль 2. Принятие решений в неантагонистических конфликтах**

**Лабораторная работа № 2.1**

**Выбор средств эффективной защиты от DoS/DdoS-атак**

**Цель работы:** формирование практических навыков выбора средств эффективной защиты от DoS/DdoS-атак.

**Задачи:**

1. Проанализировать существующие критерии принятия решений в неопределенных ситуациях.
2. Предложить способ применения критериев принятия решений в неопределенных ситуациях при выборе средства эффективной защиты от DoS/DdoS-атак.
3. Разработать методику подбора основных средств защиты от DoS/DdoS-атак.
4. Апробировать методику подбора основных средств защиты от DoS/DdoS-атак на численных расчетах.
5. Оформить отчёт.

**Теоретические сведения**

DDoS-атаки являются распространенным способом нанесения ущерба компьютерным системам. Они бывают двух типов: истощение ресурсов сети и истощение ресурсов хоста. Атаки осуществляются с помощью непосредственной посылки жертве большого количества пакетов (как, например, UDP и ICMP flood) или посредством использоваия для этой цели промежуточных узлов (примеры: Smurf и Fraggle), а также посредством передачи слишком длинных пакетов (Ping Of Death), некорректных пакетов (Land) или большого количества трудоемких запросов (TCP SYN) и т.д.

Для выбора средства эффективной защиты от различного рода атак можно использовать методы теории игр. Матричная игра, в которой игрок взаимодействует с окружающей средой и решает задачу определения наиболее выгодного варианта поведения, называется статистической игрой.

Рассмотрим критерии для принятия решений в статистических играх.

1. *Максиминный критерий Вальда.* При максиминном критерии Вальда оптимальной считается та стратегия ЛПР (лицо, принимающее решение), которая обеспечивает максимум минимального выигрыша:

.

Этот критерий отражает принцип гарантированного результата, т.е. ЛПР выбирает такую стратегию, которая максимизировала бы его выигрыш в саммой неблагоприятной ситуации.

1. *Критерий минимаксного риска Сэвиджа.* Критерий минимаксного риска Сэвиджа предполагает, что оптивальной является та стратегия, при которой величина риска в наихудшем случае минимальна. Этот критерий также называется критерием минимального риска. Согласно критерию Сэвиджа ЛПР пытается выбрать действие, при котором величина риска принимает наименьшее значение в самой неблагоприятной ситуации, т.е.
2. *Критерий пессимизма-оптимизма Гурвица.* Этот критерий рекомендует при выборе решения не руководствоваться ни крайним пессимизмом, ни крайним оптимизмом.

Критерий Гурвица рекомендует стратегию, которая определяется по формуле:

,

где степень пессимизма.

Выбор конкретного значения параметра определяется субъективными факторами: чем опаснее ситуация, тем ближе к единице выбирается значение .

1. *Критерий Лапласа.* При неизвестных вероятностях состояний «природы» можно принять, что все они равновероятны и выбор решения оределяется критерием Лапласа, при котором ЛПР выбирает такую стратегию *Ai,* что

.

Выбор критерия принятия решений является наиболее сложным и ответственным этапом. Если рекомендации, вытекающие из различных критериев, совпадают – тем лучше, можно смело выбирать рекомендуемое ими решение. Если эти рекомендации противоречат друг другу, анализ матрицы игры «с природой» с точки зрения разных критериев часто дает лучшее представление о ситуации, о достинствах и недостатках каждого решения, чем непосредственное рассмотрение матрицы, особенно высокой размерности.

**Порядок выполнения лабораторной работы**

Допустим, имеются информационные ресурсы, которые подвергаются следующим DoS/DdoS-атакам: Smurf-ping (*S1*), ICMP flood (*S2*), UDP flood (*S3*), TCP flood (*S4*).

В качеств средств защиты будем рассматривать лишь часто используемые, а именно файервол (*A1*), средства обнаружения вторжения (*A2*), резервирование канала связи (*A3*).

Пусть задана матрица выигрышей при использовании рассматриваемых средств защиты:

1. Согласно критерию Вальда:

[3;3;**4**]=4.

Значит, следует выбирать третье средство защиты.

1. Согласно критерию Сэвиджа:

Значит, следует выбирать третье средство защиты.

1. Согласно критерию Гурвица:

Значит, следует выбирать второе средство защиты.

1. Согласно критерию Лапласа:

Значит, следует выбирать третье средство защиты.

Поскольку рекомендации трех критериев из четырех рассмотренных сводятся к выбору третьей стратегии, целесообразно остановиться на этом решении.

Напишите программу, которая для заданных типов атак и возможных средств защиты подбирает наиболее эффективное.

**Форма отчётности по выполнению лабораторной работы**

Индивидуальный отчет студента должен быть представлен в распечатанной форме с типовым титульным листом. Отчет должен содержать:

1. Цель.
2. Задание.
3. Описание исходных данных.
4. Листинг программы.
5. По результатам работы программы предложить средство эффективной защиты от DoS/DdoS-атак.
6. Выводы.

**Контрольные вопросы и задания**

1. Сформулируйте задачи выполненного лабораторного исследования и выводы по выполненной работе.
2. Дайте характеристику программному обеспечению, задействованному в проведении лабораторных работ.
3. Раскройте методику проведения выполненного лабораторного исследования.
4. Выполните анализ и интерпретируйте результаты выполненных лабораторных исследований, оцените их соответствие теоретическим ожиданиям.
5. Переслите критерии принятия решений в условиях игр «с природой».

**Лабораторная работа № 2.2**

**Стратегии защиты компьютерной системы при наличии априорной информации о частоте появлений угроз**

**Цель работы:** формирование практических навыков поиска стратегий защиты компьютерной системы при наличии априорной информации о частоте появлений угроз.

**Задачи:**

1. Изучить методы планирование эксперимента в условиях неопределенности.
2. Сравнить алгоритмы планирования «идеального» и «неидеального» экспериментов в условиях неопределенности.
3. Разработать приложение, которое по заданным параметрам реализует методы планирования эксперимента для поиска стратегий защиты компьютерной системы при наличии априорной информации о частоте появлений угроз и определяет целесообразность проведения эксперимента.
4. Оформить отчёт.

**Теоретические сведения**

*Краткие теоретические сведения об «идеальном» эксперименте*

«Идеальным» называется эксперимент, который приводит к точному знанию того состояния «природы», которое имеет место в данной ситуации.

Пусть заданы:

* матрица выигрышей ;
* вероятности  различных состояний «природы» ;
* затраты на проведение эксперимента .

Эксперимент  нужно проводить, если затраты на его осуществление меньше минимального среднего риска :

.

В противном случае от эксперимента следует воздержаться и применить ту стратегию , для которой достигается минимум среднего риска.

Риском  игрока при использовании стратегии  в условиях  называется разность между выигрышем, который он получил бы, если бы знал , и выигрышем, который он получит в тех же условиях, применяя стратегию .

, где .

*Краткие теоретические сведения о «неидеальном» эксперименте*

«Неидеальным» эксперимент  не приводит к выяснению в точности состояния природы , а лишь дает какие-то косвенные сведения в пользу тех или иных событий.

Исходные данные:

* матрица выигрышей ;
* априорные вероятности  различных состояний «природы» ;
* матрица Р условных вероятностей исходов  в условиях  ;
* затраты С на проведение эксперимента .

После осуществления эксперимента, давшего исход , необходимо пересмотреть вероятности условий: состояния «природы»  будут характеризоваться не прежними «априорными» вероятностями , а новыми «апостериорными» вероятностями , т.е. условными вероятностями состояний  при условии, что эксперимент дал исход . Эти апостериорные вероятности рассчитываются по формуле Байеса:



Поскольку априорные вероятности состояний «природы»  заменяются новыми – апостериорными , то и оптимальная стратегия  в общем случае заменяется новой оптимальной стратегией , вычисленной с учетом апостериорных вероятностей (при условии события ).

**Порядок выполнения лабораторной работы**

Рассмотрим задачу, когда администратор компьютерной системы использует *m* своих стратегий против *n* угроз.

Исходными данными являются:

* матрица выигрышей администратора компьютерной системы ;
* априорные вероятности  появления угроз ;
* матрица Р условных вероятностей исходов эксперимента  в условиях появления угроз  ;
* затраты С на проведение эксперимента .

Разработать приложение, которое по заданным параметрам реализует методы планирования эксперимента для поиска стратегий защиты компьютерной системы при наличии априорной информации о частоте появлений угроз и определяет целесообразность проведения эксперимента.

**Форма отчётности по выполнению лабораторной работы**

Индивидуальный отчет студента должен быть представлен в распечатанной форме с типовым титульным листом. Отчет должен содержать:

1. Цель.
2. Задание.
3. Описаание исходных данных.
4. Листинг программы с описанием.
5. Скриншоты с результатам работы приложения.
6. Выводы.

**Контрольные вопросы и задания**

1. Сформулируйте задачи выполненного лабораторного исследования и выводы по выполненной работе.
2. Дайте характеристику программному обеспечению, задействованному в проведении лабораторных работ.
3. Раскройте методику проведения выполненного лабораторного исследования.
4. Выполните анализ и интерпретируйте результаты выполненных лабораторных исследований, оцените их соответствие теоретическим ожиданиям.
5. Назовите отличительные особенности «идеального» и «нидеального» экспериментов.
6. Назовите критерий, который определяет целесообразность проведения «идеального» эксперимента.
7. Назовите критерий, который определяет целесообразность проведения «неидеального» эксперимента.

**Модуль 3. Многошаговые процессы принятия решений**

**Лабораторная работа № 3.1**

**Защита компьютерной системы как позиционная игра с неполной информацией**

**Цель работы:** формирование практических навыков рассмотрения зашиты компьютерной системы как позиционной игры с неполной информацией.

**Задачи:**

1. Проанализировать процесс нормализации позиционной игры с неполной информацией.
2. Реализовать алгоритм нахождения оптимальных стратегий для зашиты компьютерной системы как позиционной игры с неполной информацией.
3. Оформить отчёт.

**Теоретические сведения**

Для решения задачи защиты информации в комьютерных системах каждая компьютерная система должна включать подсистему защиты информации, обеспечивающую комплексную защиту информации. Данная задача может быть решена посредством использования методов теории позиционных игр.

***Позиционная игра*** – это бескоалиционная игра, моделирующая процессы последовательного принятия решений игроками в условиях меняющейся во времени и, вообще говоря, неполной информации.

Процесс игры состоит в последовательном переходе от одного состояния игры к другому состоянию, который осуществляется либо путем выбора игроками одного из возможных действий в соответствии с правилами игры, либо случайным образом (***случайный ход***).

Состояния игры принято называть ***узлами*** или ***позициями***, а возможные выборы в каждой позиции – ***альтернативами***. Окончательные позиции называются ***вершинами***.

Характерной особенностью позиционной игры является возможность представления множества позиций в виде древовидного упорядоченного множества, которое называется ***деревом игры*** ([Рисунок 1](#Рисунок_1)).

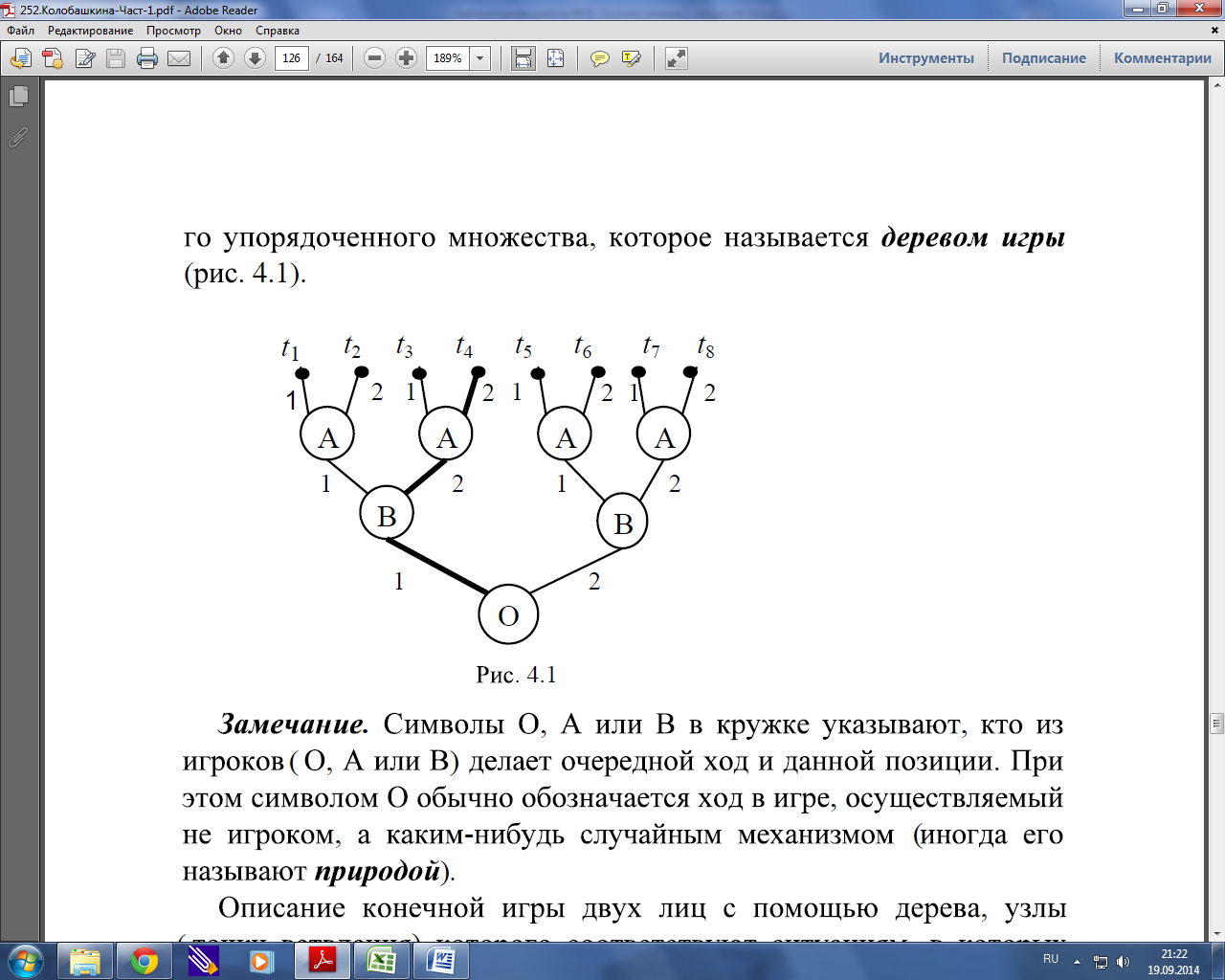


Рисунок 1 – Дерево игры

Символы О,А или В указывают, кто из игроков делает очередной ход в данной позиции (О – ход игры осуществляет «природа»).

Описание конечной игры двух лиц с помощью дерева, узлы которого соответствует ситуациям ,в которых стороны осуществляют свои выборы, а вершины – ситуациям завершения операции, является ***моделью игры в позиционной или развернутой форме***.

Цепь, связывающая начальную позицию с данной вершиной, называется ***партией***.

В позиционных играх с неполной информацией игрок, делающий ход, не знает точно, в какой именно позиции дерева игры он фактически находится. Этому игроку известно лишь некоторое множество позиций, включающее в себя его фактическую позицию. Такое множество позиций называется ***информационным множеством***. Позиции, принадлежащие одному и тому же информационному множеству, объединяются пунктирными линиями. Предполагается, что понятие дерева игры включает и группирование узлов этого дерева в информационные множества, отражающие осведомленность игроков обо всех выборах, предшествующих текущему ходу.

***Нормализация позиционной игры***

***Стратегия игрока в конечной позиционной игре*** есть функция, определенная на всех информационных множествах этого игрока (на дереве игры). Значением этой функции на каждом таком множестве является один из выборов, имеющихся у игрока в этом множестве.

Заранее определенную последовательность ходов игрока, выбранную им в зависимости от информации о ходах другого игрока и ходах игрока О (природы), будем называть ***чистой стратегией*** этого игрока.

В том случае, если в игре нет случайных ходов, выбор игроками чистых стратегий однозначно определяет исход игры – приводит к окончательной позиции, где игрок А и получает свой выигрыш. Это обстоятельство позволяет сводить позиционную игру к матричной игре.

Процесс сведения позиционной игры к матричной называется ***нормализацией позиционной игры***.

Пример.

1-й ход. Игрок А выбирает число x из множества двух чисел .

2-й ход. Игрок В выбирает число y из множества двух чисел ,не зная выбора числа x игроком А.

Задана функция  выплат игроку А за счет игрока В:



Дерево игры и информационные множества для данного случая показаны на [Рисунке 2](#Рисунок_2):

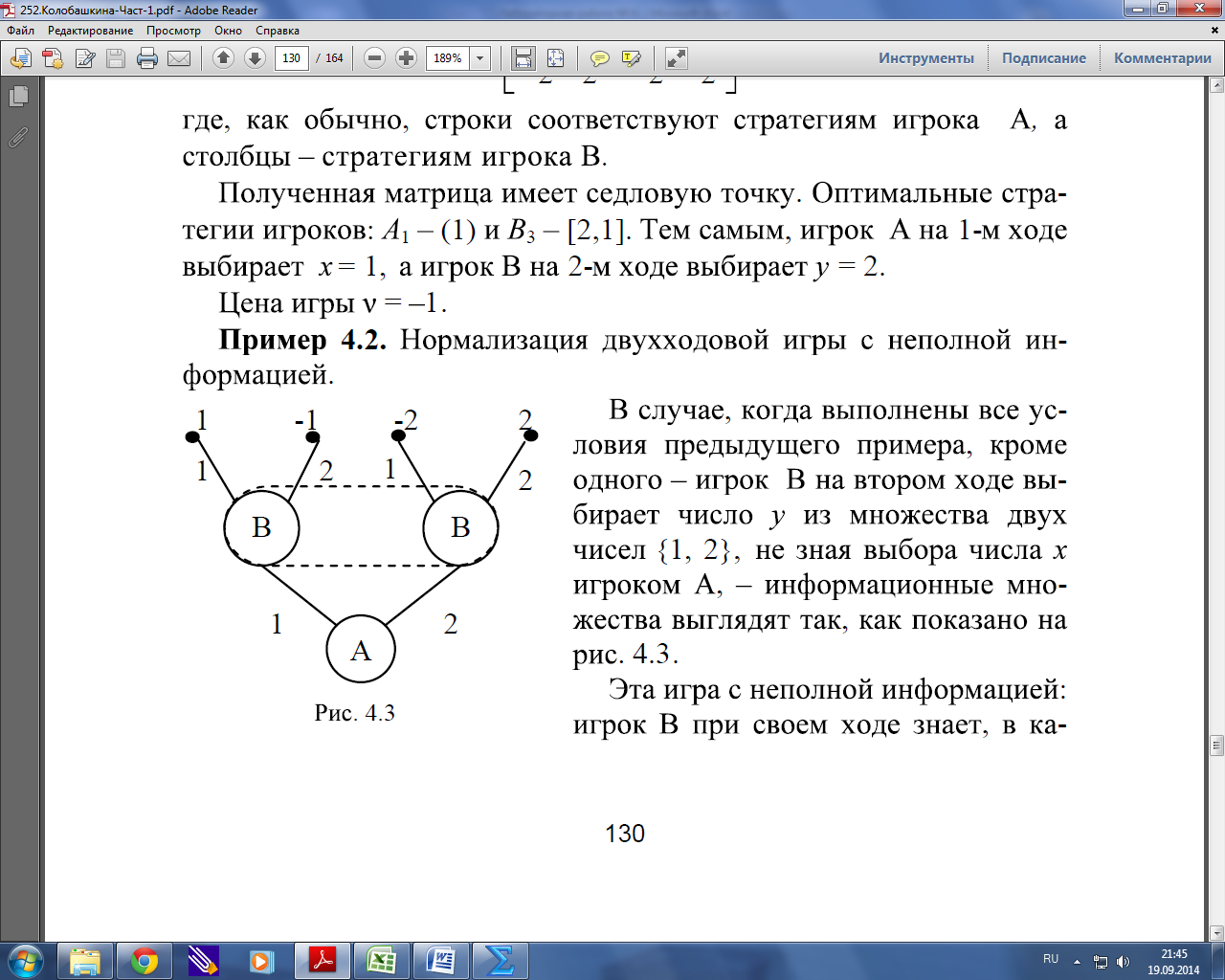


Рисунок 2 – Дерево игры

Рассмотрим стратегии игроков.

Стратегию игрока А можно задать числом x, показывающим, какую альтернативу, первую или вторую, выбрал игрок. Тем самым, у игрока А две чистые стратегии:

 - «выбрать », - «выбрать ».

Поскольку игроку В выбор игрока А неизвестен, то есть игрок В не знает, в какой именно из двух позиций он находится, то у него те же две стратегии:

 - «выбрать », - «выбрать ».

Соответствующие таблица выигрышей игрока А и матрица игры имеют вид:

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |



Полученная матрица седловой точки не имеет. Оптимальные смешанные стратегии игроков, полученные аналитическим методом:

; .

Цена игры .

**Порядок выполнения лабораторной работы**

Пусть злоумышленник – игрок А – обладает *n* стратегиями атаки на компьютерную систему. Каждая такая стратегия – это *i*-ая угроза, способная нарушить работу компьютерной системы. Аминистратор – игрок В – располагает *m* способами защиты ресурса. Посколько игрок В не знает, какой способ атаки избрал хакер, то данная задача сводится к озиционной игре с неполной информацией. Необходимо реализовать алгоритм нахождения оптимальных стратегий для зашиты компьютерной системы как позиционной игры с неполной информацией посредсвом разработки соответсвующего приложения. Функция выплат, количество стратегий игроков и осведомленность игрок о предыдущих шагах задается пользователем.

**Форма отчётности по выполнению лабораторной работы**

Индивидуальный отчет студента должен быть представлен в распечатанной форме с типовым титульным листом. Отчет должен содержать:

1. Цель.
2. Задание.
3. Листинг программы с опиисанием.
4. Скриншоты результатов работы приложения.
5. Выводы.

**Контрольные вопросы и задания**

1. Сформулируйте задачи выполненного лабораторного исследования и выводы по выполненной работе.
2. Дайте характеристику программному обеспечению, задействованному в проведении лабораторных работ.
3. Раскройте методику проведения выполненного лабораторного исследования.
4. Выполните анализ и интерпретируйте результаты выполненных лабораторных исследований, оцените их соответствие теоретическим ожиданиям.
5. Дайте определение следующим понятиям: позиционная игра, информационное множество, нормализация позиционной игры.

**Лабораторная работа № 3.2**

**Защита компьютерной системы как позиционная игра с полной информацией**

**Цель работы:** формирование практических навыков рассмотрения зашиты компьютерной системы как позиционной игры с полной информацией.

**Задачи:**

1. Проанализировать процесс нормализации позиционной игры с полной информацией.
2. Сравнить равновесные ситуации и цены игры при условии доброжелательного и недоброжелательного отношения игроков.
3. Реализовать алгоритм нахождения оптимальных стратегий для зашиты компьютерной системы как позиционной игры с полной информацией
4. Оформить отчёт.

**Теоретические сведения**

***Позиционная игра*** – это бескоалиционная игра, моделирующая процессы последовательного принятия решений игроками в условиях меняющейся во времени и, вообще говоря, неполной информации.

Процесс игры состоит в последовательном переходе от одного состояния игры к другому состоянию, который осуществляется либо путем выбора игроками одного из возможных действий в соответствии с правилами игры, либо случайным образом (***случайный ход***).

Состояния игры принято называть ***узлами*** или ***позициями***, а возможные выборы в каждой позиции – ***альтернативами***. Окончательные позиции называются ***вершинами***.

Характерной особенностью позиционной игры является возможность представления множества позиций в виде древовидного упорядоченного множества, которое называется ***деревом игры*** ([Рисунок 3](#Рисунок_3)).

Символы О,А или В указывают, кто из игроков делает очередной ход в данной позиции (О – ход игры осуществляет «природа»).

Описание конечной игры двух лиц с помощью дерева, узлы которого соответствует ситуациям ,в которых стороны осуществляют свои выборы, а вершины – ситуациям завершения операции, является ***моделью игры в позиционной или развернутой форме***.

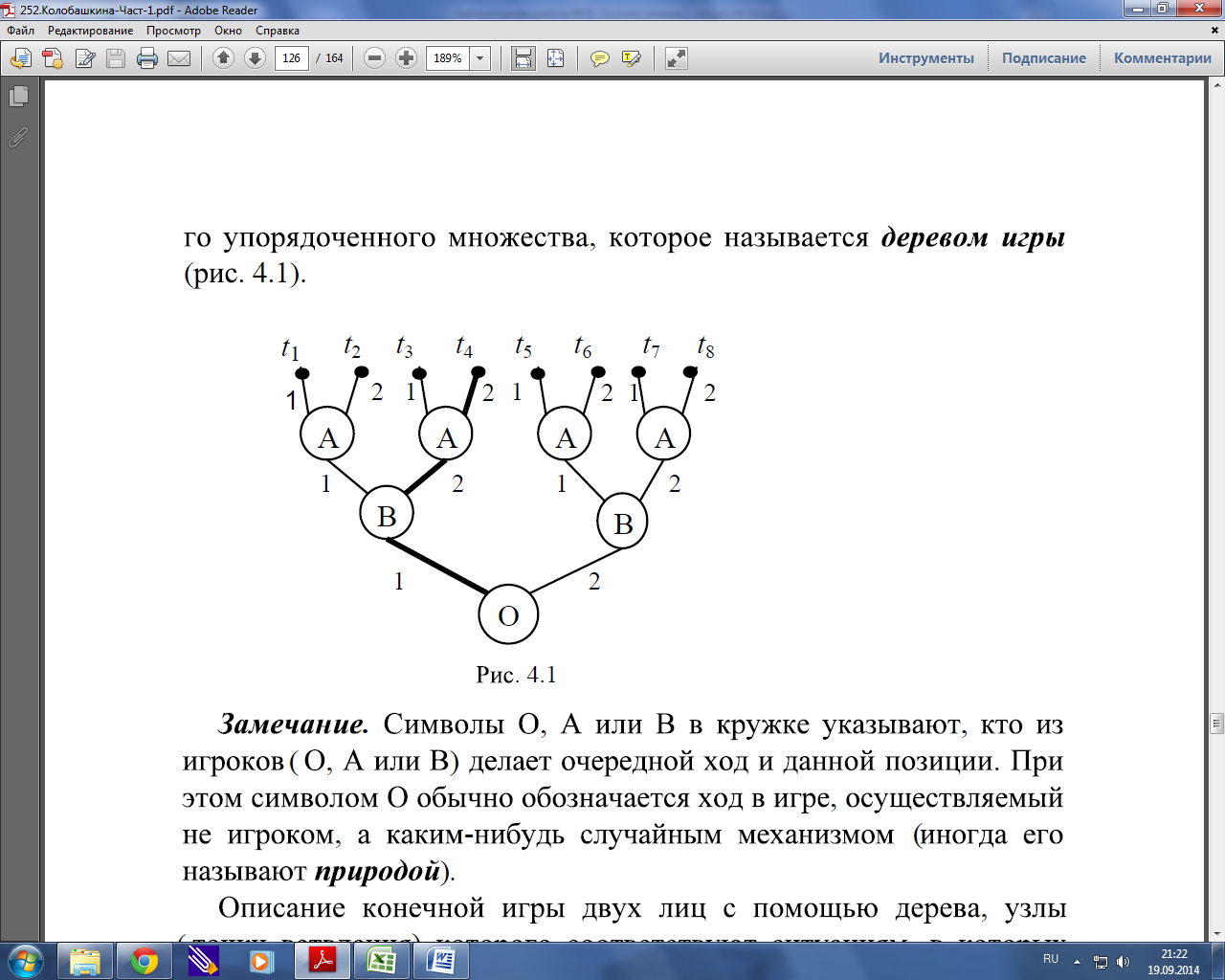


Рисунок 3 – Дерево игры

Цепь, связывающая начальную позицию с данной вершиной, называется ***партией***.

Позиционная игра называется игрой с ***полной информацией***, если в любой точке любой ее партии игрок, делающий ход, точно знает, в какой позиции он находится и какие выборы были сделаны ранее, а следовательно, из-за древовидности графа игры может восстановить и все предыдущие позиции. В графическом исполнении каждый узел такой игры будет представлять собой отдельное информационное множество, и поэтому в такой игре информационные множества пунктиром не отмечаются.

***Теорема.*** В любой конечно-шаговой игре с полной информацией на конечном древовидном графе существует ситуация абсолютного равновесия по Нэшу.

Каждый ход игрока однозначно определяет последующую позицию дерева игры. В результате последовательного выбора позиций игроков однозначно реализуется некоторая последовательность узлов, определяющая путь в древовидном графе, исходящий из начальной позиции и достигающий одной из конечных вершин. Такой путь называется ***партией игры***.

Разобьём все множество позиций дерева игры на три подмножества:

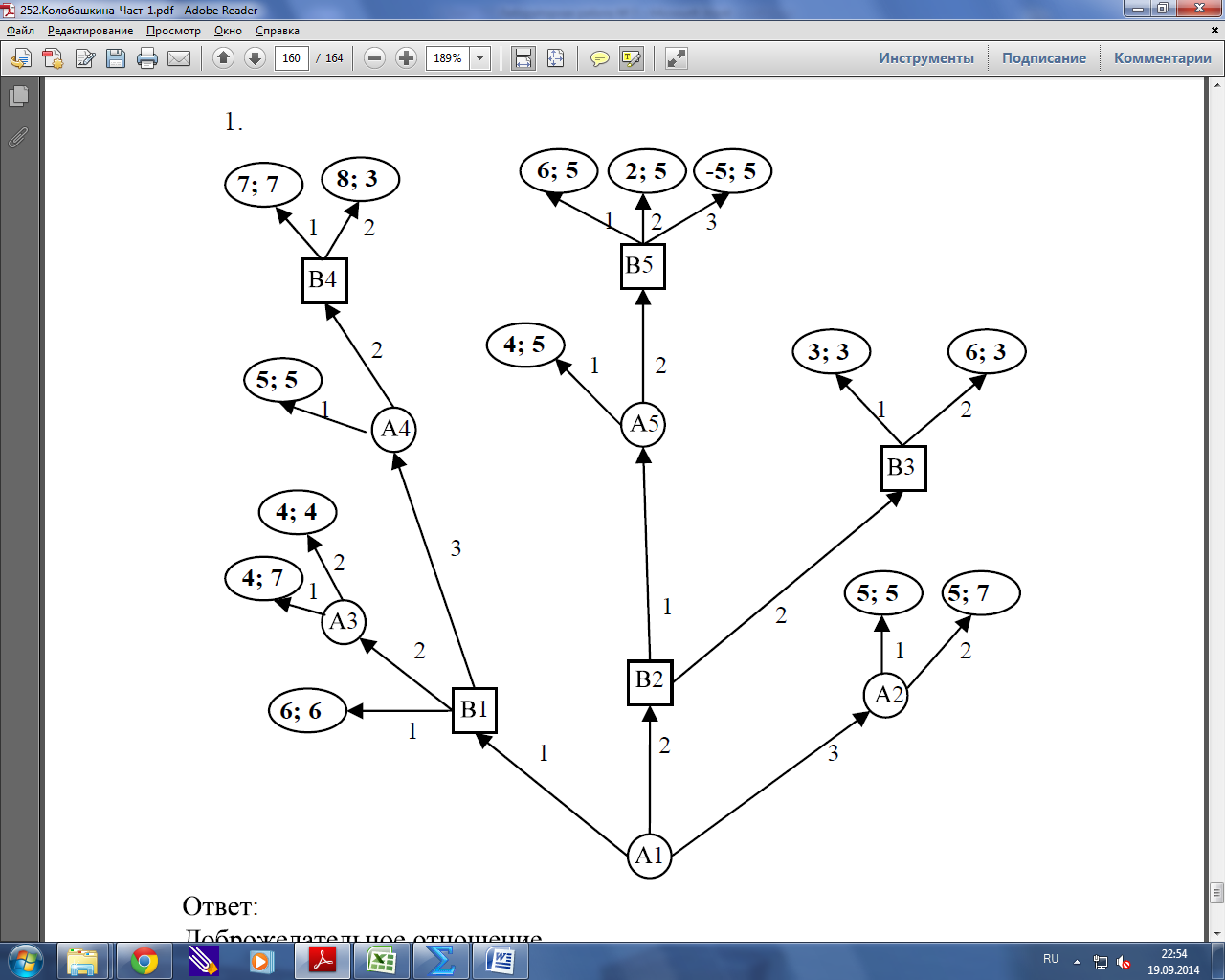
*  - множество очередности игрока А, т.е. множество позиций игрока А, в которых ему предоставлено право выбора очередной альтернативы. для наглядности будем изображать на дереве игры эти позиции кружками;
*  - множество очередности В, т.е. множество позиций игрока В, в которых ему предоставлено право выбора очередной альтернативы. для наглядности будем изображать на дереве игры эти позиции квадратами;
*  - множество конечных вершин, в которых задаются функции выигрышей игроков в виде: (на первом месте стоит выигрыш игрока А в партии игры, определяемой данной вершиной, на втором – выигрыш игрока В). Для наглядности будем изображать на дереве игры конечные вершины овалами, в которых проставлены выигрыши игроков.

Ребра, выходящие из каждого узла, определяют альтернативы выбора на данном этапе. Поскольку выбор альтернативы в узле дерева игры эквивалентен выбору следующей позиции, будем считать, что стратегии указывают в каждой позиции номер ребра, по которому следует двигаться далее.

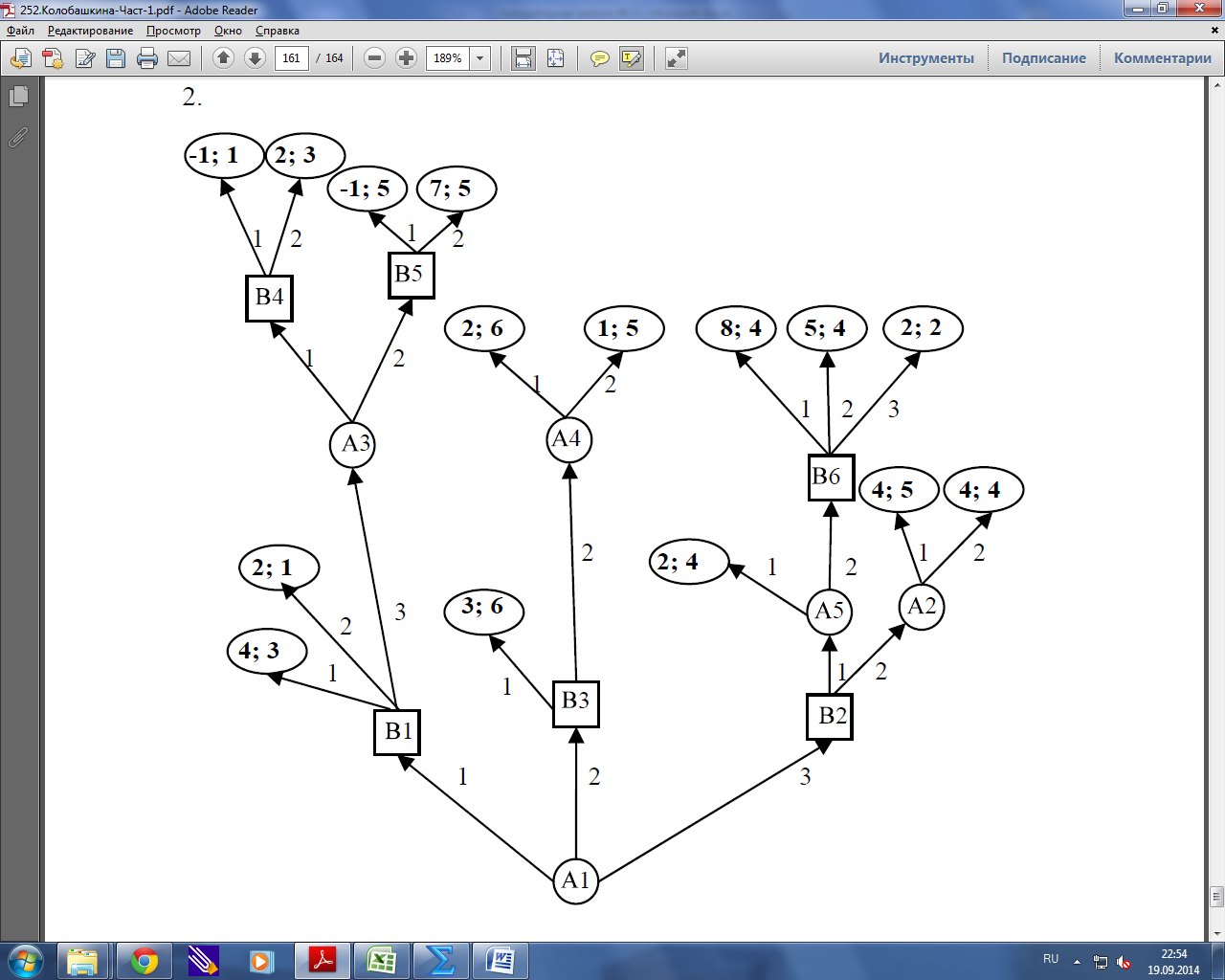
**Порядок выполнения лабораторной работы**

Пусть процесс выбора игроками А и В (злоумышленник и администратор) своих ходов описан с помощью представленного дерева игры. Необходимо определить равновесные ситуации и цены игры при условии доброжелательного и недоброжелательного отношения игроков:

Вариант №1



Вариант №2

.

**Форма отчётности по выполнению лабораторной работы**

Индивидуальный отчет студента должен быть представлен в распечатанной форме с типовым титульным листом. Отчет должен содержать:

1. Цель.
2. Задание.
3. Исходное дерево игры.
4. Значение функции Беллмана во всех позициях дерева игры.
5. Результативное дерево игры.
6. Опптимальные стратегии игроков и ценаа игры.
7. Выводы.

**Контрольные вопросы и задания**

1. Сформулируйте задачи выполненного лабораторного исследования и выводы по выполненной работе.
2. Дайте характеристику программному обеспечению, задействованному в проведении лабораторных работ.
3. Раскройте методику проведения выполненного лабораторного исследования.
4. Выполните анализ и интерпретируйте результаты выполненных лабораторных исследований, оцените их соответствие теоретическим ожиданиям.
5. Дайте определение следующим понятиям: позиционная игра, информационное множество, дерево игры.
6. Поясните, в чем разница между позиционными играми с полной и неполной информацией.

**Литература**

1. Гадельшина, Г.А. Введение в теорию игр [Электронный ресурс]: учебное пособие / Г.А. Гадельшина, А.Е. Упшинская, И.С. Владимирова; Министерство образования и науки России, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Казанский национальный исследовательский технологический университет». - Казань: Издательство КНИТУ, 2014. - 112 с. – Режим доступа: [http://biblioclub.ru/index.php?page=book&id=428702](http://biblioclub.ru/index.php?page=book_red&id=428702).
2. Гуц, А.К. Теория игр и защита компьютерных систем [Электронный ресурс] : учебное пособие / А.К. Гуц, Т.В. Вахний. — Электрон. текстовые данные. — Омск: Омский государственный университет им. Ф.М. Достоевского, 2013. — 160 c. — Режим доступа: <http://www.iprbookshop.ru/24947.html>.
3. Колобашкина, Л.В. Информационные технологии принятия решений в условиях конфликта: учебное пособие для вузов: в 2 ч. Ч.1. Основы теории игр [Электронный ресурс] : учеб. пособие / Л.В. Колобашкина, М.В. Алюшин. — Москва : НИЯУ МИФИ, 2010. — 164 с. — Режим доступа: https://e.lanbook.com/book/75864.
4. Макарова, О.С. Использование методов теории принятия решений в условиях информационных конфликтов специалистами по защите информации: курс лекций по дисциплине «Теория принятия решений в условиях информационных конфликтов» / О.С. Макарова– Калуга: Изд-во КФ МГТУ им. Н.Э. Баумана, 2017. – 88 с.
5. Царев, Р.Ю. Программирование на языке Си [Электронный ресурс]: учебное пособие / Р.Ю. Царев. - Красноярск : Сибирский федеральный университет, 2014. - 108 с. : табл., схем. URL: [http://biblioclub.ru/index.php?page=book&id=364601](http://biblioclub.ru/index.php?page=book_red&id=364601).

**ПРИЛОЖЕНИЕ А**

**Оформление титульного листа отчёта по лабораторной работе**

|  |  |  |
| --- | --- | --- |
| |  |  | | --- | --- | | ***Gerb-BMSTU_01*** | ***Министерство науки и высшего образования Российской Федерации***  *Калужский филиал*  *федерального государственного бюджетного*  *образовательного учреждения высшего образования*  ***«Московский государственный технический университет***  ***имени Н.Э. Баумана***  ***(национальный исследовательский университет)»***  ***(КФ МГТУ им. Н.Э. Баумана)*** | |
| **ФАКУЛЬТЕТ** «Информатика и управление»  **КАФЕДРА** «Защита информации»  ОТЧЕТ  Лабораторная работа № 2.1  **ДИСЦИПЛИНА:** «Теория принятия решений в условиях  информационных конфликтов»  **ТЕМА:**  «Поиск стратегий обороны в киберпространстве»  Выполнил студент гр. БАС.И-71 Иванов И.И. \_\_\_\_\_\_\_\_\_\_\_\_  Проверил: Макарова О.С. \_\_\_\_\_\_\_\_\_\_\_\_  Дата сдачи (защиты) лабораторной работы:  Результаты сдачи (защиты):  Количество рейтинговых баллов  Оценка  Калуга, 2018 г. |