ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

УПРАВЛЕНИЕ ДИСТАНЦИОННОГО ОБУЧЕНИЯ И ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Кафедра «Вычислительные системы и информационная безопасность»

СБОРНИК УПРАЖНЕНИЙ

по дисциплине

«Управление информационной безопасностью»

Автор
Газизов А.Р.

Ростов-на-Дону, 2015

Аннотация

Методические указания к лабораторным работам по дисциплине «Управление информационной безопасностью» для студентов очной формы обучения по направлению подготовки 090900.62 «Информационная безопасность (бакалавр).

В компактной форме приводятся краткие теоретические сведения к выполнению лабораторных работ, порядок выполнения лабораторных работ, индивидуальные задания и контрольные вопросы.

Автор

Кандидат педагогических наук Газизов Андрей Равильевич

Оглавление

ЛАБОРАТОРНАЯ РАБОТА 1
МЕНЕДЖМЕНТ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цель занятия – приобретение обучаемыми необходимого объёма знаний о целях, задачах, предпосылках и направлениях организационной и управленческой работы в сфере информационной безопасности.

Время – 2 часа.

Учебные вопросы:

1. **Теоретическая часть:**

1) Цели и задачи менеджмента в сфере информационной безопасности.

2) Структура организационно-управленческой деятельности сфере информационной безопасности.

2. **Практическая часть:**

1) Вопросы по разделу.

2) Задание.

3) Порядок отчетности и форма контроля выполнения работы.

3. **Материально-техническое обеспечение.**

1. Теоретическая часть.

1) Цели и задачи менеджмента в сфере информационной безопасности.

Под понятием «информационная безопасность» принято иметь в виду состояние (уровень) защищенности информационных ресурсов – информационных объектов и информационных систем от негативных воздействий (как случайных, так и осуществляемых преднамеренно), которые могут нанести ущерб самой информации и средствам ее передачи и обработки, а, следовательно, отрицательно отразиться на владельцах информационных ресурсов, государстве, обществе и других участниках процессов информационного обмена. Большинство современных информационных ресурсов, а также информационных систем практически не могут рассматриваться в отрыве от комплекса элементов (факторов), связанных с обеспечением информационной безопасности – угроз для информационных ресурсов, различных средств и мер защиты, барьеров для проникновения, а также уязвимостей в системах защиты информации.

Таким образом, под информационной безопасностью в более общем виде следует понимать совокупность средств, методов и процессов (процедур), обеспечивающих защиту информационных активов и, следовательно, гарантирующих сохранение эффективности и практической полезности, как технической инфраструктуры информационных систем, так и сведений, которые в таких системах хранятся и обрабатываются.

Понятие информационной безопасности неразрывно связано с рисками для информационных ресурсов, под которыми (рисками) понимается возможность (вероятность) нанесения ущерба информационным ресурсам, снижения уровня их защищенности. Риски могут иметь различную природу и характеристики; одной из основных классификаций рисков для информационной безопасности (так же, как и многих других рисков в экономике и управлении) является их разделение:

– на системные риски: неуправляемые риски, связанные с той средой и технической инфраструктурой, в которой функционируют информационные системы;

– операционные риски: как правило, управляемые риски, связанные с особенностями использования определенных информационных систем, их технической реализации, применяемыми алгоритмами, аппаратными средствами и др.

В качестве методической основы для детализированного анализа рисков в практической работе может быть использован ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

Все негативные воздействия на информационные активы, защиту от которых (воздействий) предполагает информационная безопасность, могут быть разделены на три основных вида:

1) нарушение конфиденциальности информации;
2) разрушение (утеря, необратимое изменение) информации;
3) недоступность информационных ресурсов – возникновение ситуаций, когда пользователи (все или их часть) на некоторый период времени теряют возможность доступа к необходимым данным (или информационным системам).

Непосредственным источником рисков и негативных воздействий являются угрозы, под которыми понимаются потенциальные или реально возможные действия по отношению к информационным ресурсам, нарушающие информационную безопасность. Выделяется множество типов угроз и множество критериев для классификации угроз информационной безопасности. Одним из основных таких кри- териев является расположение

источника нарушений к информационным ресурсам, в отношении которых осуществляется негативное воздействие. В соответствии с этим критерием нарушения могут быть разделены:

– на обусловленные внутренними факторами (персоналом предприятия, работой собственных информационных систем);

– обусловленные внешними факторами (злоумышленниками, не имеющими непосредственного отношения к компании – владельцу информационных активов, природными факторами и др.).

Другим важным критерием является наличие намерений осуществить нарушение. В соответствии с ним выделяют:

– целенаправленные воздействия (могут быть осуществлены как собственным персоналом, так и внешними противниками);

– случайные воздействия (ошибки пользователей и администраторов, сбои и случайные нарушения в работе оборудования, непредвиденные воздействия природных факторов).

Также можно выделить следующие классификации угроз:

– по объектам (персонал, материальные и финансовые средства, информация);

– по величине ущерба (предельный, значительный, незначительный);

– по вероятности возникновения (весьма вероятные, вероятные, маловероятные);

– по типу ущерба (моральный, материальный)

На практике основными наиболее распространенными способами нарушения информационной безопасности являются:

– получение несанкционированного доступа (в том числе и путем превышения прав при санкционированной работе с информационными системами) к определенным сведениям или массивам данных, распространение которых ограничено, с целью их изучения, копирования, распространения, незаконного использования и др.;

– несанкционированное использование информационных ресурсов (ресурсов вычислительных и телекоммуникационных систем) с целью получения выгоды или нанесения ущерба (как тем системам, которые незаконно используются, так и третьим лицам);

– несанкционированная злонамеренная модификация (изменение) данных;

– кража денежных средств в электронных платежных системах и системах «клиент-банк», а также кража бездокументарных ценных бумаг и иные формы незаконного присвоения имуще-

ственных прав;

– вывод из строя (полный или частичный) программных и аппаратных средств обработки, передачи и хранения информации;

– осуществление атак типа «отказ в обслуживании» – DoS (в частности, в отношении серверов в сети Интернет);

– распространение вирусов и других вредоносных программ, осуществляющих различные негативные воздействия.

Современная практика использования информационных систем характеризуется большим количеством и постоянным ростом числа нарушений информационной безопасности. Одним из важных факторов этого является постоянно растущая доступность современных информационных технологий для преступников, а также постоянно растущая привлекательность информационных систем как потенциальных объектов нападения. Также важным обстоятельством является постоянное усложнение и рост разнообразия используемых информационных систем и, в частности, программных продуктов. Так, например, объем (и, соответственно, сложность) одной из наиболее распространенных операционных систем – Microsoft Windows – увеличился с примерно 4 миллионов строк программного кода в 1992 году (Windows NT) до более чем 35 миллионов строк в 2000 году (Windows 2000). С учетом того, что в среднем каждая тысяча строк программного кода может содержать от 5 до 15 ошибок, появление все большего числа различных уязвимостей, создающих угрозы для информационной безопасности, становится практически неизбежным.

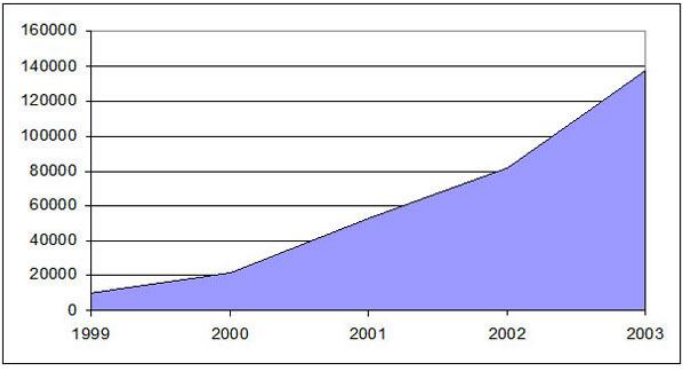


Рис. 1. Число сообщений о происшествиях, связанных с нарушениями информационной безопасности, которые поступили в CERT/CC.

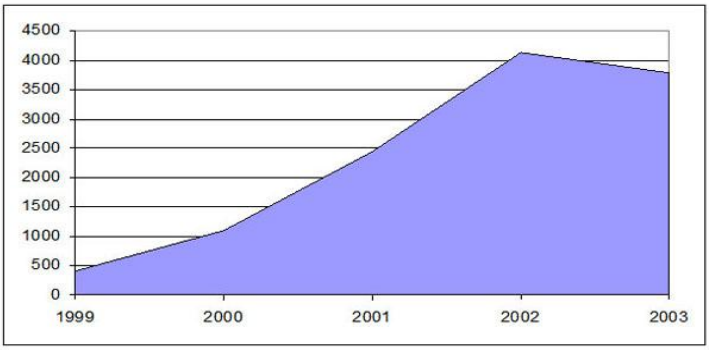


Рис. 2. Число сообщений о выявленных уязвимостях в информационных системах, поступивших в CERT/CC

Результатом этого является постоянный рост количества различных нарушений, связанных с информационной безопасностью. Число сообщений о различных инцидентах в сфере защиты информации, полученных одним только «Центром реагирования на инциденты, связанные с информационной безопасностью» при университете Карнеги-Меллон (CERT), в период с 1999 по 2003 годы увеличилось более чем в 14 раз, а число получаемых ежегодно сообщений о выявленных уязвимостях в различных информационных системах примерно в 10 раз (данные представлены на рис.1 и 2).

Таким образом, все перечисленные обстоятельства: рост многообразия возможных нарушений, увеличение их количества, увеличение сложности информационных технологий, постоянно возрастающая доступность компьютеров и телекоммуникационных средств для преступников объясняют рост потребности владельцев информационных ресурсов (предприятий, организаций, государственных ведомств) в реализации систематических, всеобъемлющих мер по обеспечению информационной безопасности.

Отдельные процессы, процедуры, механизмы и инструменты защиты информации, используемые владельцами информационных ресурсов и информационных систем, могут быть направлены:

- на ограничение и разграничение доступа;
- информационное скрытие;
- введение избыточной информации и использование избыточных информационных систем (средств хранения, обработки и передачи информации);
- использование методов надежного хранения, преобра-

зования и передачи информации;

- нормативно-административное побуждение и принуждение.

На практике современные технологии защиты информации основаны на различных базовых сервисах (таких, как аутентификация, обеспечение целостности, контроль доступа и др.), и используют различные механизмы обеспечения безопасности (такие, как шифрование, цифровые подписи, управление маршрутизацией и др.). Однако комплексность и массовость использования информационных технологий, их интеграция в повседневную деятельность предприятий, организаций, правительственных учреждений не позволяют решать задачи информационной безопасности только одними техническими средствами.

2) Структура организационно-управленческой деятельности сфере информационной безопасности.

Во всем комплексе деятельности по защите информации одно из наиболее важных мест занимает организационно-управленческая деятельность – организационное обеспечение информационной безопасности, которое представляет собой одно из четырех основных направлений работы в общей системе мер в сфере информационной безопасности, включающей в себя также разработку специализированного программного обеспечения, изготовление и использование специальных аппаратных средств, и совершенствование криптографических (математических) методов защиты информации (рис. 3).

Рис. 3. Структура деятельности в сфере информационной безопасности.

Основными задачами организационно-управленческой деятельности (менеджмента) в сфере информационной безопасности являются:

- обеспечение комплексности всех решений, реализуемых в

процессе обеспечения информационной безопасности;

– обеспечение непрерывности и целостности процессов информационной безопасности;

– решение методических задач, лежащих в основе эффективного управления информационной безопасностью, таких, как вопросы управления рисками, экономическое моделирование и т.п.;

– управление человеческими ресурсами и поведением персонала с учетом необходимости решения задач информационной безопасности.

Под комплексностью решения задач информационной безопасности подразумевается взаимоувязанное выявление всех значимых информационных объектов, а также существующих и потенциально возможных угроз. На основе этого анализа необходимо обеспечить исчерпывающе полное (комплексное) внедрение и применение средств защиты информации, которые в той или иной мере могли бы нейтрализовать все существенные угрозы на всех потенциально уязвимых участках прохождения информационных потоков в течение всех этапов жизненного цикла информационных систем и организационных процедур. Меры по нейтрализации рисков также должны быть реализованы в комплексе с другими механизмами, такими, как, например, страхование. Другими словами, задачей менеджмента является системное использование всех необходимых частных (узкоспециальных) технологий и решений для каждой конкретной ситуации таким образом, чтобы во всей системе мер по защите информационных ресурсов не осталось «узких мест» –уязвимых участков, через которые могут быть осуществлены нападения и в которых могут произойти непреднамеренные нарушения. Сложность такого рода задач связана с тем, что они предполагают по возможности исчерпывающий анализ, как всех информационных ресурсов, так и всех возможных сценариев нападения на них и последующий подбор наиболее подходящих средств защиты.

Непрерывность процессов обеспечения информационной безопасности предполагает выделение необходимых ресурсов и организацию выполнения необходимых функций по защите информации в течение всего времени функционирования информационных систем и выполнения бизнес-функций (в том числе и в режиме «24x7x365» в тех случаях, когда это необходимо).

Разработка, совершенствование и поддержание в актуальном состоянии методических основ управления информационной безопасностью включает в себя, главным образом, приме-

нение общих для многих сфер менеджмента концепций и теорий – таких как, например, математические модели оценки рисков или теория инвестиционного анализа – применительно к ресурсам, используемым для обеспечения информационной безопасности, и информационным процессам.

Управление человеческими ресурсами в рамках управления информационной безопасностью включает в себя комплекс задач, охватывающий все основные аспекты деятельности людей: отбор и допуск персонала для работы с определенными информационными ресурсами, обучение, контроль правильности выполнения обязанностей, создание необходимых условий для работы и т.п.

При этом конкретная структура и состав всех основных задач управления и организации в сфере информационной безопасности, а также непосредственно используемые методы будут определяться как уровнем, на котором осуществляется управленческая и организационная деятельности, так и конкретными условиями, в которых функционируют информационные системы, нуждающиеся в защите. Настоящий курс основан на концепции разделения всего многообразия методов и задач организации и управления в сфере информационной безопасности на несколько основных уровней и дальнейшего представления организационно-управленческих методов для каждого из этих уровней.

Под организационным обеспечением и менеджментом в сфере информационной безопасности обычно принято понимать решение управленческих вопросов на уровне отдельных субъектов (предприятий, организаций) или групп таких субъектов (партнеров по бизнесу, организаций, которые совместно решают определенные задачи, требующие защиты информации).

Однако сложность и комплексность современных проблем в сфере информационной безопасности, глобализация информационных взаимодействий требуют более полного и широкого понимания организационной работы и менеджмента в этой области. В частности, по мере глобализации информационных взаимодействий, усложнения программных и аппаратных средств обработки информации, проникновения информационных технологий в повседневную деятельность всех организаций и жизнь большинства людей появилась необходимость в специальных организационных и управленческих усилиях, направленных не на обеспечение защищенности отдельных информационных активов, а на поддержание различных элементов информационной инфраструктуры, которая в той или иной мере работает на обеспечение ин-

формационной безопасности определенных сообществ (заранее не определенного множества пользователей информационных систем и владельцев информационных ресурсов). Таким образом, с развитием информационных технологий и интенсификацией информационного обмена организационная и управленческая работа в сфере информационной безопасности оказывается направленной не только на собственно защиту определенных информационных ресурсов, но и на более «глобальный» объект – создание и развитие безопасной информационной инфраструктуры (в разных смыслах этого термина и с учетом различных его аспектов). На практике такая инфраструктура может включать в себя:

- надежную инфраструктуру передачи информации и рынок услуг доступа к таким каналам связи;
- рынок программных и аппаратных средств, обеспечивающих защиту информации;
- систему подготовки, переподготовки и повышения квалификации специалистов в сфере информационной безопасности;
- общие правила использования информации, а также ее передачи, совместной эксплуатации информационных сетей (в том числе протоколы информационного обмена);
- систему обмена информацией и распространения знаний о существующих уязвимостях тех или иных информационных технологий, возможных угрозах информационной безопасности и способах их нейтрализации;
- законодательную и правоприменительную систему, обеспечивающую охрану имущественных и иных интересов всех участников информационного обмена
- и другие составляющие.

Потребность в целенаправленном развитии и поддержании такой инфраструктуры порождает необходимость в выработке специфичных организационных и управленческих приемов, как правило, не характерных для информационной безопасности в привычном («узком») ее понимании. Такое расширение сферы интересов менеджмента информационной безопасности объясняет причины, по которым необходимо разделять несколько относительно самостоятельных организационных уровней, характеризующихся специфическими задачами, подходами к решению этих задач и используемыми организационными методами.

1. Уровень международных профессиональных объединений (как правило, неправительственных и некоммерческих), так или иначе связанных со сферой информационных технологий, телекоммуникаций и информацион- ной безопасности.

2. Уровень крупных компаний, работающих в сфере информационных технологий и в значительной мере определяющих (прямо или косвенно) состояние информационной безопасности в сообществе пользователей информационных систем, а также влияющих на безопасность различных элементов информационной инфраструктуры.

3. Государственный уровень – уровень государственных и межправительственных организаций, так или иначе влияющих на жизнь общества, состояние правовой системы, развитие экономики и технологий.

4. Уровень отдельных компаний (предприятий и организаций) – сообщество пользователей информационных систем, так или иначе заинтересованных в собственной информационной безопасности и обеспечивающих защиту имеющихся у них информационных ресурсов собственными силами.

Также отдельно можно выделить дополнительный промежуточный уровень, включающий в себя консалтинговые и внедренческие компании, учебные центры (включая также сообщество специалистов, занимающихся консультациями, внедрениями и обучением в индивидуальном порядке), работающие в сфере информационной безопасности и действующие

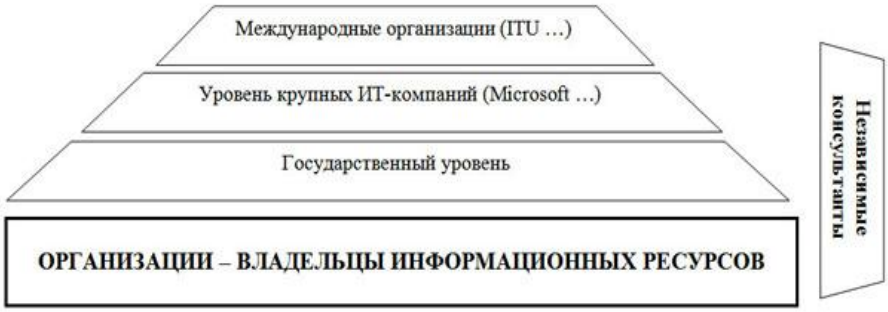


Рис. 4. Иерархия уровней организационной работы в сфере информационной безопасности.

как связующее звено между различными организационными уровнями, а также представляющие интересы различных участников информационного взаимодействия. Все эти составляющие образуют своеобразную организационную иерархию, представленную на рис. 4.

Следует понимать, что субъекты, находящиеся на верхних ступенях данной иерархии (в частности, государственные органы,

крупные IT-корпорации), выступают не только как владельцы собственных информационных ресурсов, требующих защиты, но и как субъекты, которые воздействуют на инфраструктуру, лежащую в основе обмена и хранения информации, а также на общественно-экономические отношения, влияющие на информационную безопасность. И тот факт, что такие субъекты сами уделяют значительное внимание защите собственных ресурсов (вкладывают существенные средства в обеспечение информационной безопасности, инициируют новые разработки для собственных нужд, используют наиболее передовые технологии в этой сфере и т.п.), не должен отвлекать внимание от того обстоятельства, что эти субъекты фактически создают инфраструктуру для повседневной деятельности множества компаний, организаций, людей, профессиональных и бизнес-сообществ и используют для этого организационные методы и приемы, которые существенно отличаются по своей природе от методов, характерных для работы по обеспечению информационной безопасности отдельных субъектов и защите отдельных информационных активов.

Итак, необходимость самостоятельного рассмотрения субъектов, относящихся к верхнему уровню, с точки зрения организационного используют и методы, характерные для субъектов нижнего уровня представленной иерархии, т.к. являются владельцами собственных информационных ресурсов.

Представленное разделение на уровни должно быть основой для более целенаправленного развития системы менеджмента и налаживания взаимосвязей между различными уровнями организационной работы. Важность выделения и самостоятельного рассмотрения верхних уровней управленческой работы обусловлена тем, что целенаправленное осознание организационных вопросов, специфичных для верхних уровней иерархии, и их решение позволит более эффективно решать задачи развития национальных и региональных экономик в целом и отдельных отраслей (телекоммуникации, финансовые услуги и т.п.), а не только решать задачи отдельных субъектов, участвующих в информационном обмене.

Основные особенности организационной работы на каждом из перечисленных уровней организации представлены в таблице 1.

Таблица 1 и рис. 5 наглядно демонстрируют причины, по которым каждый из уровней организационной работы в сфере информационной безопасности нуждается в индивидуальном подходе и применении специфич- ных методов организации и

управления. В соответствии с этим разделением и строится структура настоящего курса, она включает в себя рассмотрение основных форм и приемов организации работы по обеспечению информационной безопасности на основных перечисленных уровнях:

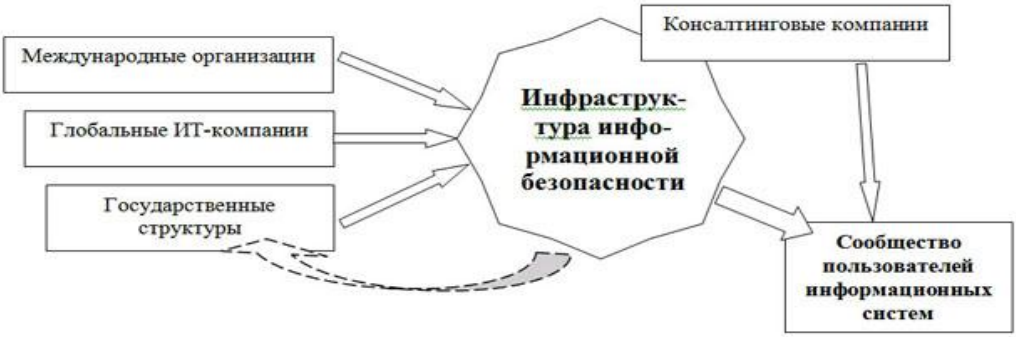


Рис. 5. Взаимосвязи уровней организации информационной безопасности.

1) на уровне международных профессиональных организаций и бизнес-сообществ;

2) на уровне крупных поставщиков технических (программных и аппаратных) средств обработки и передачи информации, имеющих влияние на состояние информационной безопасности большого числа предприятий, организаций и индивидуальных пользователей;

3) на уровне государственных органов (в частности, правительств отдельных стран);

4) на уровне отдельных предприятий, учреждений и организаций, являющихся непосредственными владельцами и пользователями информационных ресурсов.

Также рассматриваются вопросы работы специализированных компаний (консалтинговых, технологических, страховых), предоставляющих различные услуги, которые связаны с обеспечением информационной безопасности.

Таблица 1

Задачи, роли и методы, используемые на различных уровнях организационной работы в сфере информационной безопасности

Организационный уровень	Основные задачи и роли	Основные специфичные методы организационной работы
Международные организации	Разработка правил и стандартов (в том числе и сетевых протоколов), имеющих глобальное значение. Обмен актуальной информацией и предупреждениями о новых угрозах	Координация работы специалистов, экспертов и исследователей, представляющих различные заинтересованные стороны
Глобальные ИТ-компании	Методологическая и организационная поддержка использования продуктов и услуг, поставляемых на рынок	Гибкое взаимодействие с клиентами (пользователями продуктов и услуг) с целью повышения эффективности использования информационных систем и получения отзывов для дальнейшего повышения качества поставляемых продуктов и услуг
Государственные организации	Регулирование использования информационных систем и распространения информации с целью недопущения противоправных действий, ущерба другим участникам информационного обмена, обществу и государственным органам	Разработка национальных и международных правил (законов, конвенций, соглашений и т.п.), регулирующих отношения в информационной сфере Осуществление контроля (в различных формах). Осуществление правоприменительной и правоохранительной деятельности
Пользователи информационных систем – владельцы информации	Защита собственных информационных ресурсов	Выделение подразделений и специалистов, отвечающих за ИБ. Разработка и применение внутренних политик и правил безопасности

Консалтинговые и внедренческие компании, работающие в сфере ИБ	Выполнение некоторых функций ИБ на условиях аутсорсинга. Разработка и внедрение индивидуальных решений в сфере ИБ более эффективно, чем это могли бы сделать сами владельцы информационных ресурсов	Накопление и обобщение теоретических знаний и практических навыков с целью создания и внедрения организационных и технических решений в интересах клиентов

2. Практическая часть.

1) Вопросы по разделу:

1) Классификация рисков информационной безопасности?

2) Виды негативных воздействий на информационные активы, защиту от которых предполагает информационная безопасность?

3) Что понимается под угрозой информационной безопасности?

4) Что понимается под организационно-управленческой деятельностью в сфере информационной безопасности и её основные задачи?

5) Задачи, роли и методы, используемые на различных уровнях организационной работы в сфере информационной безопасности?

2) Задание.

1) Разработать презентацию «Цели, задачи, предпосылки и направления организационной и управленческой работы в сфере информационной безопасности».

2) Разработать презентацию «Основные понятия и определения в сфере информационной безопасности».

3) Порядок отчетности и форма контроля выполнения работы.

Контроль выполнения задания производится по окончании занятия и на консультациях в форме защиты выполненной работы, предоставленной в электронном и в бумажном виде в форме «Отчет по лабораторной работе …».

3. Материально-техническое обеспечение.

Специализированная мебель и технические средства для представления учебной информации, включая проекционное оборудование; компьютерный класс с компьютерами AMD 2400 – 12 шт., оснащенными операционной системой Windows XP и пакетом Microsoft Office.

ЛАБОРАТОРНАЯ РАБОТА 2
МЕНЕДЖМЕНТ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ГОСУДАРСТВЕННОМ УРОВНЕ В РФ

Цель занятия – приобретение обучаемыми необходимого объёма знаний об управлении информационной безопасностью на государственном уровне: общих принципах и российской практике.

Время – 2 часа.

Учебные вопросы:

1. **Теоретическая часть:**

1) Предпосылки развития государственного менеджмента в сфере информационной безопасности.

2) Методология и структура организационного обеспечения информационной безопасности на уровне государства.

3) Общая политика РФ в сфере информационной безопасности.

2. **Практическая часть:**

1) Вопросы по разделу.

2) Задание.

3) Порядок отчетности и форма контроля выполнения работы.

3. **Материально-техническое обеспечение.**

1. Теоретическая часть.

1) Предпосылки развития государственного менеджмента в сфере информационной безопасности.

Основные задачи государственных органов в сфере информационной безопасности, также как и во многих других сферах, связаны с охраной общественных интересов, предотвращением противоправной деятельности, а также с защитой информации, имеющей государственную важность (военных сведений, информации о космических и ядерных технологиях и др.). При этом решение вопросов информационной безопасности в частном секторе экономики, как правило, является прерогативой самих частных компаний и организаций, а вмешательство государства в эту сферу должно быть минимизировано. Таким образом, на практике деятельность органов власти, как правило, концентрируется на решении вопросов инфор- мационной безопасности внут-

ри отдельных сфер, которые считаются наиболее важными для обеспечения государственной безопасности и достижения тических целей: вооруженные силы, внешняя разведка, стратегические технологии (например, космические, атомные и военные), государственные финансы, общественная стабильность и некоторые другие. Решению вопросов информационной безопасности в других областях государственными органами, как правило, уделяется меньше внимания. Государственные органы могут решать определенные задачи информационной безопасности, не относящиеся напрямую к защите государственных информационных систем, в тех случаях, когда выгоды от государственного вмешательства существенно превышают затраты и решения, предлагаемые государством, не составляют конкуренции альтернативным решениям (услугам, технологиям, методикам и др.), которые предлагаются (или потенциально могут быть предложены) частными компаниями.

Деятельность государства в сфере информационной безопасности, как правило, строится на более общих задачах государственной власти, таких как:

- сохранение суверенитета государства;
- сохранение государственной и политической стабильности в стране;
- сохранение и развитие демократических институтов общества, а также обеспечение прав и свобод граждан;
- укрепление законности и правопорядка;
- обеспечение социально-экономического развития страны и устойчивости финансовой системы;
- участие в жизни международного сообщества.

По своей природе факторы, определяющие состояние информационной безопасности и, соответственно, деятельность государства в этой сфере, подразделяются на:

- политические;
- социально-экономические;
- организационно-технические.

Организационная деятельность государства в сфере информационной безопасности, как правило, сводится к противодействию различным угрозам:

- внешним, таким как деятельность иностранных спецслужб и вооруженных сил, враждебная экономическая и техническая политика отдельных государств, агрессивные рыночные стратегии крупных международных корпораций и финансово-промышленных групп, незаконная деятельность международных преступных и

террористических группировок и др.;

– внутренним, таким как деятельность криминальных структур в сфере обращения информации, неправомерные действия государственных структур, халатность или целенаправленные нарушения, допускаемые гражданами и организациями при использовании информационных систем и обращении информации, нарушения в работе информационных и телекоммуникационных систем и др.

Таким образом, деятельность государства в этой сфере направлена на нейтрализацию существующих угроз информационной безопасности с учетом всех факторов, воздействующих как на сами управляющие государственные структуры, так и на информационные системы.

2) Методология и структура организационного обеспечения информационной безопасности на уровне государства.

Для решения основных задач в сфере информационной безопасности действуют все основные органы государственной власти и управления: судебные, органы исполнительной власти, правоохранительные органы, организации и предприятия, которые контролируются государством и имеют доступ к информации, составляющей государственную тайну, и другие.

Для обеспечения информационной безопасности государственные органы выполняют следующие основные функции:

– создают законодательную базу, обеспечивающую защиту базовых прав частных лиц, предприятий и государства, таких как право на защиту частной информации, право на защиту коммерческой и банковской тайны, право на беспрепятственный доступ к информации и др. Данная функция осуществляется законодательными органами в сотрудничестве с органами исполнительной власти, общественными организациями, научно-исследовательскими учреждениями и другими заинтересованными участниками;

– осуществляют правоприменительную деятельность, непосредственно реализуют меры по защите информационных ресурсов государственного управления, а также выполняют все функции, необходимые для реализации требований законодательства;

– выполняют судебные функции в отношении лиц, которые допустили правонарушения, связанные с использованием информационных ресурсов, и участвуют в хозяйственных спорах, связанных с нарушениями информационной безопасности.

Функции создания и по- стоянного совершенствования

законодательно-правовой базы, обеспечивающей защиту законных частных, коммерческих, общественных и государственных интересов, реализуются законодательными органами (парламентами) государств. Как правило, все законодательные функции в данной сфере в большинстве стран осуществляются центральными (федеральными) органами законодательной власти, а местные (региональные), органы таких полномочий не имеют. Для создания и поддержания в актуальном состоянии законодательства в сфере информационной безопасности в законодательных органах могут создаваться профильные комитеты и комиссии, которые состоят из членов данного законодательного органа, имеющих некоторые базовые знания и навыки в сфере информационных технологий и правового регулирования вопросов информационного обмена. Кроме того, вопросы совершенствования законодательства в сфере обеспечения информационной безопасности также могут решаться в различных профильных комитетах, подкомитетах и рабочих группах, специализирующихся на смежных проблемах государственного управления и социально-экономического регулирования, таких как:

- оборона;
- национальная безопасность;
- политика в сфере связи, информации и информатизации;
- промышленная и экономическая политика;
- наука и образование
- и др.

Для разработки соответствующих нормативно-правовых актов подразделения (комитеты и подкомитеты) органов законодательной власти могут привлекать для совместной работы ответственных специалистов, руководителей, аналитиков и экспертов, работающих в:

- органах исполнительной власти (министерствах, отвечающих за научное и техническое развитие, т.н. «силовых» министерствах и ведомствах, юридических ведомствах и др.);
- частных компаниях, а также общественных и профессиональных организациях, которые занимаются оказанием информационных услуг, поставкой информационно-технических продуктов, специализирующихся на развитии информационных технологий и др.;
- научно-исследовательских организациях, специализирующихся на соответствующих проблемах информационных технологий и управления.

Процедуры согласова- ния, принятия и утверждения

законодательных актов, а также процедуры контроля за действиями органов исполнительной власти в каждой стране определяются в соответствии с действующим законодательством (конституцией).

Деятельность исполнительных органов государственной власти в сфере обеспечения информационной безопасности направлена на реализацию действующих в государстве законов и непосредственную защиту интересов государственной власти, гражданских прав и прав компаний, осуществляющих хозяйственную деятельность.

Конкретная работа органов исполнительной власти в сфере информационной безопасности, как правило, осуществляется по нескольким относительно самостоятельным направлениям:

1. Установление конкретных правил производства, продажи, экспорта, импорта и использования средств защиты информации, а также организация системы контроля за соблюдением действующих законов и установленных правил.
2. Лицензирование и сертификация предприятий и организаций, занимающихся производством, продажей установкой и настройкой программных и аппаратных средств защиты информации.
3. Осуществление правоохранительной деятельности в сфере защиты информации (уголовного преследования лиц и преступных группировок, совершающих противоправные действия, содержащие признаки уголовных преступлений в соответствии с действующим уголовным законодательством).
4. Непосредственное осуществление функций защиты информации в государственных учреждениях и службах (правительство, вооруженные силы, органы внутренних дел и др.).
5. Разработка государственных стандартов, относящихся к организации и технологиям защиты информации (программным и аппаратным средствам, средствам криптографии и др.).
6. Поддержка образования и подготовки кадров, а также регулирование деятельности образовательных учреждений (включая установку образовательных стандартов).
7. Поддержка научных исследований в сфере информационной безопасности.
8. Осуществление международного сотрудничества в сфере защиты информации (взаимодействие с правительствами и правоохранительными органами др. стран) как в целях общего развития инфраструктуры информационной безопасности, так и для разрешения отдельных инци- дентов (раскрытия преступле-

ний и др.).

Судебные функции, как правило, реализуются судами общей юрисдикции, так же как и для всех остальных гражданских и уголовных дел. Специальных судебных инстанций, которые были бы предназначены для рассмотрения дел, связанных с информационной безопасностью (таких как, например, суды по правам человека или военные суды), не существует. При этом могут создаваться судебные лаборатории, специализирующиеся на проведении экспертиз, анализов и исследований различных элементов информационных систем в связи с расследованиями и судебными разбирательствами по делам о нарушениях в сфере информационной безопасности.

Основой организации государственной деятельности в сфере информационной безопасности является национальная политика (доктрина, национальный план, национальная стратегия) информационной безопасности. Этот документ, издаваемый, как правило, главой исполнительной ветви власти (президентом страны) отражает:

- признание государственной властью существенной значимости проблем защиты информации для общества, личности, экономики и самого государства;
- современное понимание общего ландшафта информационной безопасности на национальном уровне: потенциально уязвимые информационные объекты, источники угроз и др.;
- основные направления, в которых государство намерено осуществлять активные действия с целью повышения уровня информационной безопасности на национальном уровне (создание систем безопасности, упорядочивание взаимоотношений различных субъектов, пресечение правонарушений, развитие инфраструктуры и технологий безопасности и др.).

В рамках утвержденной государственной доктрины информационной безопасности:

- создаются специализированные правительственные организации, отвечающие за реализацию политики информационной безопасности и решение отдельных задач в этой сфере;
- отдельные правительственные учреждения наделяются специфическими функциями и полномочиями, связанными с управлением информационной безопасностью (как в общегосударственном масштабе, так и в рамках определенных сфер ответственности), а также создаются специальные структурные подразделения, отвечающие за решение вопросов защиты информации и информационной инфра- структуры;

– создается система локальных правовых актов, регулирующих отношения в сфере защиты информации, а также система государственных стандартов, относящихся к технологиям и организации защиты информации.

Специализированные органы, создаваемые в структуре исполнительной власти для решения задач информационной безопасности на государственном уровне, как правило, подчиняются непосредственно главе исполнительной ветви власти, носят статус федеральных агентств, комитетов или комиссий и наделены правом самостоятельно издавать нормативные акты в рамках имеющихся полномочий, установленных действующим законодательством. Издаваемые таким образом локальные нормативные акты (указы, постановления, инструкции, порядки, правила и др.) непосредственно регулируют отношения в сфере создания, распространения и использования средств автоматизации и защиты информации.

Государственная стандартизация технологий и методов, используемых в процессах защиты информации, осуществляется уполномоченными государственными органами с целью упорядочивания знаний о современном состоянии технологий и методов защиты и установления универсальных критериев надежности и функциональности для определенных технологий.

Государственная стандартизация позволяет достичь универсальности при оценке используемых технологий и методов и, таким образом, до определенной степени упорядочить многие взаимоотношения, связанные с использованием таких технологий и методов.

Стандартизация, осуществляемая отдельными государственными органами, как правило, опирается на существующую систему имеющихся международных стандартов, а национальные органы, занимающиеся стандартизацией, могут принимать участие в разработке международных стандартов. Основными объектами государственной и международной стандартизации могут выступать:

– методы шифрования и криптографической защиты данных;

– технологии идентификации пользователей информационных систем;

– методы аутентификации;

– методы тестирования (проверки) и оценки информационных систем на предмет их защищенности;

– некоторые другие эле- менты систем обеспечения

формационной безопасности.

3) *Общая политика РФ в сфере информационной безопасности.*

Основой современной политики РФ в сфере информационной безопасности можно считать «Доктрину информационной безопасности РФ», утвержденную Президентом РФ В.В.Путиным 09.09. 2000 г. Этот документ:

- описывает основные предпосылки формирования государственной политики в данной сфере (потребность в безопасности, существующие интересы, угрозы, источники угроз и др.);
- формулирует базовые задачи государства и общества, основанные непосредственно на необходимости выполнения требований Конституции, обеспечения суверенитета страны и др.;
- описывает состояние дел в сфере общегосударственного регулирования процессов информационной безопасности на момент утверждения Доктрины (основные достижения и недостатки);
- перечисляет приоритетные направления деятельности государства (задачи, требующие безотлагательного решения) по обеспечению информационной безопасности;
- формулирует основные методики, которые государство должно использовать для обеспечения информационной безопасности, а также специфику применения этих методов в отдельных областях общественной жизни;
- перечисляет основные информационные объекты (в различных сферах), на охрану которых должна быть направлена государственная политика;
- описывает основные направления международного сотрудничества в сфере информационной безопасности;
- перечисляет основные организационные инструменты, используемые для реализации государственной политики и осуществления государственного управления в сфере информационной безопасности;
- описывает распределение ответственности между основными органами государственной власти, решающими задачи в сфере информационной безопасности.

В соответствии с Доктриной государство должно уделять внимание информационной безопасности в таких основных сферах, как:

- экономика;
- внутренняя политика;

- внешняя политика;
- наука и техника;
- духовная жизнь;
- информационные системы государственного управления;
- оборона.

К числу первоочередных мероприятий, которые должны быть реализованы на государственном уровне, Доктрина относит:

- совершенствование законодательной базы в сфере информационных отношений;
- разработку механизмов управления государственными средствами массовой информации и реализации государственной информационной политики;
- подготовку кадров для работы в сфере информационной безопасности;
- совершенствование и развитие системы государственных стандартов в сфере информатизации и обеспечения информационной безопасности;
- принятие и реализацию федеральных программ, решающих определенные задачи информатизации и обеспечения информационной безопасности: создание информационных архивов и информационно-телекоммуникационных систем органов власти, развитие информационной культуры населения и др.

Как можно видеть из этого перечня, а также в целом из текста Доктрины, она предполагает определенное расширение понятия «информационная безопасность» и включение в него некоторых вопросов, которые связаны с деятельностью средств массовой информации и другими аспектами информационной политики, не имеющими прямого отношения к категории «информационная безопасность» в ее первоначальном понимании.

Помимо Доктрины также важным основополагающим документом, в значительной мере определяющим политику государства в сфере информатизации и обеспечения защиты информации, можно считать Федеральную целевую программу «Электронная Россия», реализация которой планируется в три этапа в период с 2002 по 2010 год. В частности, одной из заявленных целей реализации данной Программы является обеспечение реализации прав на «обеспечение конфиденциальности любой охраняемой законом информации, имеющейся в информационных системах». В целом предполагается, что весь комплекс мероприятий, предусмотренных Программой, должен обеспечить принципиально более высокий уровень надежности ключевых информационных потоков на государственном уровне.

Кроме того, важными организующими документами, действующими в этой сфере на государственном уровне, являются:

- Федеральный Закон «О государственной тайне»:
- Федеральный Закон «Об информации, информационных технологиях и о защите информации»;
- Федеральный Закон «Об участии в международном информационном обмене».

Структура органов государственной власти, обеспечивающих информационную безопасность в РФ:

1. Основным государственным органом, определяющим политику РФ в сфере безопасности страны в целом и информационной безопасности в частности, является Совет безопасности РФ.
2. Ведущим государственным учреждением, непосредственно ответственным за реализацию государственной политики в сфере информационной безопасности и защиту государственных интересов на общенациональном уровне, является Федеральная служба по техническому и экспортному контролю – ФСТЭК.
3. Важную роль в системе органов государственной власти, отвечающих за решение задач информационной безопасности, играет также Служба специальной связи и информации («Спецсвязь РФ»), с 2004 года входящая в состав Федеральной службы охраны.

Вопросы повышения качества информационной работы и информационной безопасности решают также другие федеральные органы (в пределах своей компетенции):

1. Министерство связи и массовых коммуникаций РФ;
2. Министерство внутренних дел РФ.

Также отдельные государственные ведомства, предъявляющие особые требования к уровню защищенности информации, реализуют собственные мероприятия по обеспечению защиты информации:

1. ФСБ (Управление компьютерной и информационной безопасности, а также Центр по лицензированию, сертификации и защите государственной тайны, Управление специальной связи и НИИ информационных технологий);
2. Минатом РФ и система подведомственных ему предприятий (в составе которого функционирует Центр «Атомзащитаинформ»);
3. Центральный банк РФ (в составе которого функционирует Главное управление безопасности и защиты информации) и др.

Совет Безопасности РФ, возглавляемый Президентом РФ, состоит из ключевых министров и рассматривает вопросы внут-

ренней и внешней политики РФ в области обеспечения безопасности, стратегические проблемы государственной, экономической, общественной, оборонной, информационной, экологической и иных видов безопасности. Основными функциями Совета Безопасности являются:

– подготовка решений Президента РФ по соответствующим вопросам, в т.ч. по вопросам информационной безопасности;

– рассмотрение законопроектов, в рамках своей компетенции;

– организация и координация разработки стратегии в области внутренней, внешней и военной политики, военно-технического сотрудничества и информационной безопасности РФ;

– осуществление контроля за реализацией этой стратегии органами власти, оценка внутренних и внешних угроз жизненно важным интересам объектов безопасности и выявление их источников и др.

Для решения задач, связанных с обеспечением информационной безопасности, в составе СБ функционирует созданное в 1997 году Управление информационной безопасности (одно из восьми профильных управлений), а также Межведомственная комиссия по информационной безопасности. Функциями Управления информационной безопасности являются:

– подготовка предложений Совету Безопасности по выработке и реализации основных направлений политики государства в области обеспечения информационной безопасности РФ;

– анализ и прогнозирование ситуации в области информационной безопасности РФ;

– выявление источников опасности, оценка внешних и внутренних угроз информационной безопасности и подготовка предложений Совету Безопасности по их предотвращению;

– рассмотрение в установленном порядке проектов федеральных целевых программ, направленных на обеспечение информационной безопасности РФ, подготовка соответствующих предложений;

– участие в подготовке материалов по вопросам обеспечения информационной безопасности РФ для ежегодного послания Президента РФ Федеральному Собранию и для докладов Президента РФ;

– подготовка предложений по проектам решений Совета Безопасности и информационно-аналитических материалов к его заседаниям по вопросам обес- печения информационной

безопасности РФ;

– подготовка предложений Совету Безопасности по разработке проектов нормативных правовых актов, направленных на обеспечение информационной безопасности РФ.

Федеральная служба по техническому и экспортному контролю (ФСТЭК), до августа 2004 года известная как Государственная техническая комиссия при Президенте РФ (Гостехкомиссия РФ), была создана в январе 1992 года на базе Гостехкомиссии СССР по противодействию иностранным технологическим разведкам, которая, в свою очередь ведет отсчет своего существования с декабря 1973 года.

Произошедшее в 1992 году преобразование было связано со сменой политических приоритетов, интенсивным развитием электронных коммуникаций и средств вычислительной техники, отменой государственной монополии на многие сферы экономической и технической деятельности, развитием рыночных отношений, расширением международных связей и другими факторами. ФСТЭК, ранее подчинявшаяся напрямую Президенту РФ, в процессе административной реформы была подчинена Министерству обороны. ФСТЭК является коллегиальным органом – в состав Коллегии входят около двадцати представителей различных министерств и ведомств (главным образом, в ранге заместителей министров и директоров департаментов), таких как МВД, МИД, ФСБ, Минатом, ФСО, СВР и др.

Основными функциями ФСТЭК являются:

– проведение единой технической политики и координация работ по защите информации;

– организация и контроль за проведением работ по защите информации в органах государственного управления, объединениях, концернах, на предприятиях, в организациях и учреждениях (независимо от форм собственности) от утечки по техническим каналам, от несанкционированного доступа к информации, обрабатываемой техническими средствами, и от специальных воздействий на информацию с целью ее уничтожения и искажения;

– поддержание системы лицензирования деятельности предприятий, организаций и учреждений по осуществлению мероприятий и (или) оказанию услуг в области защиты информации и сертификации средств защиты информации.

Для реализации функций по лицензированию в составе ФСТЭК функционируют 7 региональных управлений (по федеральным округам), а также 20 отраслевых аттестационных (лицензионных) центров.

Служба специальной связи и информации (Спецсвязь РФ), созданная в марте 2003 года в рамках Федеральной службы охраны на базе упраздненного Федерального агентства правительственной связи и информации (ФАПСИ), в целом призвана обеспечивать функционирование президентской связи, организацию, эксплуатацию и развитие специальной связи для государственных органов и решать другие аналогичные задачи.

При этом задачами Спецсвязи также являются:

- проведение работ по защите технических средств специальной связи, устанавливаемых в категорированных помещениях государственных органов, включая особо важные;
- организация в системе специальной связи шифровальной деятельности, отнесенной к компетенции Спецсвязи РФ;
- участие в разработке нормативной технической документации по вопросам защиты информации в системах специальной связи;
- участие в разработке и реализации мер по обеспечению информационной безопасности Российской Федерации, защите сведений, составляющих государственную тайну;
- участие в создании, обеспечении и развитии системы электронного документооборота государственных органов с использованием удостоверяющих центров;
- организация и проведение мероприятий по предотвращению утечки по техническим каналам информации в системах специальной связи, информационно-технологических, информационно-аналитических и информационно-телекоммуникационных системах, находящихся в ведении Спецсвязи РФ;
- выполнение требований обеспечения информационной безопасности объектов государственной охраны.

Министерство связи и массовых коммуникаций РФ в лице подчиняющегося ему Федерального агентства по информационным технологиям (Росинформтехнологии) осуществляет и организует следующие виды работ в сфере информационной безопасности:

- подтверждение подлинности электронных цифровых подписей уполномоченных лиц удостоверяющих центров в выданных ими сертификатах ключей подписей;
- ведение единого государственного реестра сертификатов ключей подписей удостоверяющих центров и реестра сертификатов ключей подписей уполномоченных лиц федеральных органов государственной власти, а также обеспечение доступа к ним граждан, организаций, органов государственной власти и орга-

нов местного самоуправления;

– выполнение функции государственного заказчика научно-технических и инвестиционных программ и проектов в сфере информационных технологий.

Уполномоченным органом по ведению реестра доверенных удостоверяющих центров является ФГУП НИИ «Восход».

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) является уполномоченным федеральным органом исполнительной власти по защите прав субъектов персональных данных. В полномочия данного органа входит пресечение нарушений, которые могут возникать при обработке персональных данных граждан РФ.

В системе законодательной власти основным структурным подразделением, призванным решать вопросы формирования и реализации государственной политики в сфере информационной безопасности, является Комитет по безопасности Государственной думы Федерального собрания Российской Федерации. В составе этого Комитета функционирует Подкомитет по информационной безопасности. В законодательной работе в рамках этого Комитета принимают участие:

– специалисты и руководители профильных подразделений ФСБ, СВР, ФСТЭК, МВД и др. ведомств;

– руководители Совета безопасности РФ и др. правительственных органов;

– представители общественных организаций, фондов и профессиональных объединений;

– представители крупных коммерческих компаний – лидеров в развитии организации и технологий информационной безопасности (в том числе банков, технологических компаний и др.);

– представители ведущих научно-исследовательских учреждений и учебных заведений.

2. Практическая часть.

1) Вопросы по разделу:

1) Задачи, роли и методы, используемые на различных уровнях организационной работы в сфере информационной безопасности?

2) Основные задачи и функции государственных органов РФ в сфере информационной безопасности?

3) Основа современной политики РФ в сфере информационной безопасности?

4) Структура органов государственной власти, обеспечивающих информационную безопасность в РФ?

5) Основные функции и **направления деятельности** исполнительных органов государственных органов для обеспечения информационной безопасности?

2) Задание.

1) Разработать презентацию «Методология и структура организационного обеспечения информационной безопасности на уровне государства».

2) Разработать презентацию «Общая политика РФ в сфере информационной безопасности».

3) Порядок отчетности и форма контроля выполнения работы.

Контроль выполнения задания производится по окончании занятия и на консультациях в форме защиты выполненной работы, предоставленной в электронном и в бумажном виде в форме «Отчет по лабораторной работе …».

3. Материально-техническое обеспечение.

Специализированная мебель и технические средства для представления учебной информации, включая проекционное оборудование; компьютерный класс с компьютерами AMD 2400 – 12 шт., оснащенными операционной системой Windows XP и пакетом Microsoft Office.

ЛАБОРАТОРНАЯ РАБОТА 3
МЕЖДУНАРОДНЫЕ ОРГАНИЗАЦИИ В СФЕРЕ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цель занятия – приобретение обучаемыми необходимого объёма знаний и практических навыков для самостоятельной оценки деятельности международных организаций в сфере управления информационной безопасностью.

Время –4 часа.

Учебные вопросы:

1. **Теоретическая часть:**

1) Цели, принципы и специфика работы международных организаций в сфере управления информационной безопасностью.

2) Международные профессиональные объединения по вопросами информационной безопасности.

2. **Практическая часть:**

1) Вопросы по разделу.

2) Задание

3) Порядок отчетности и форма контроля выполнения работы.

3. **Материально-техническое обеспечение.**

1. Теоретическая часть.

1) Цели, принципы и специфика работы международных организаций в сфере управления информационной безопасностью.

В числе международных организаций, действующих в сфере информационной безопасности и оказывающих существенное влияние на функционирование глобальных информационных систем и деятельность всего информационного сообщества, выделяются организации следующих типов.

1. Крупные международные некоммерческие и неправительственные организации, объединяющие специалистов в определенных областях, существующие, как правило, уже в течение многих лет и охватывающие множество основных направлений развития компьютерной инженерии, электроники и телекоммуникаций, включая, в том числе и определенные вопросы обеспечения безопасности современных информационных технологий.

2. Отдельные относитель- но небольшие организации,

которые специализируются на более или менее узких вопросах информационной безопасности, имеющих глобальное значение для всего сообщества пользователей информационных систем, и появились на базе частных компаний или исследовательских структур в течение последнего десятилетия, когда проблемы информационной безопасности стали особенно актуальными.

3. Совместные структуры (комитеты, альянсы и др.), создаваемые (иногда временно) крупными компаниями (иногда при участии крупных исследовательских центров, учебных заведений и правительственных структур) для решения определенных задач в сфере информационных технологий и информационной безопасности.

Каждый из типов организаций, в свою очередь, имеет свои специфические организационные особенности, однако все они, как правило, решают задачу разработки, согласования и дальнейшего распространения, общих для всего сообщества пользователей информационных систем технических и организационных решений, таких как:

- протоколы глобальных сетей;
- архитектуры, алгоритмы, протоколы публичных средств шифрования данных;
- правила построения глобальных сетей обмена данными и других элементов глобальной инфраструктуры информационной безопасности.

Также важными элементам организационной работы на уровне международных структур являются:

- организация обмена знаниями и актуальными новостями в среде специалистов по информационной безопасности в таких формах, как публикация специализированных периодических изданий и сборников научных работ, организация специализированных научно-практических конференций, семинаров и др.;
- организация и поддержание в актуальном состоянии баз данных и баз знаний, которые содержат сведения, необходимые пользователям информационных систем, администраторам, разработчикам и другим участникам для обеспечения информационной безопасности.

Примерами таких баз данных являются базы данных, содержащие сведения о выявленных уязвимостях различных программных и аппаратных платформ информационных систем.

В целом организационная работа на уровне международных структур не является универсальной, и в большинстве случаев они строят свою работу самостоятельно. Однако можно

выделить некоторые основные организационные принципы, рактерные для деятельности многих из них.

1. Принцип добровольности участия в работе таких структур и в отдельных проектах или во всей работе.
2. Принцип открытости (доступности) результатов работы (всех или их части) для сообщества специалистов в сфере информационных технологий.
3. Принцип самофинансирования.

Работа крупных международных профессиональных (отраслевых) организаций (объединений), как правило, имеет следующие отличительные особенности:

1. Она, как правило, не направлена только на решение задач информационной безопасности – задачи информационной безопасности решаются в комплексе со множеством других проблем (развития информационных технологий, построения телекоммуникационных систем и др.).
2. Она в определенной мере может опираться на поддержку со стороны различных государственных структур.
3. Она объединяет большое количество специалистов из различных исследовательских, учебных, коммерческих организаций, но при этом большинство участников (членов) может не иметь конкретных обязательств, обязывающих вносить вклад в работу и достигать определенных целей.

Основными наиболее крупными и известными международными профессиональными объединениями, так или иначе связанными с вопросами информационной безопасности, являются:

- ITU – International Telecommunication Union;
- IEEE – Institute of Electrical and Electronics Engineers;
- ACM – Association for Computing Machinery;
- W3 Consortium;
- ISSA – Information Systems Security Association;
- ISO – International Organization for Standardization;
- IETF – Internet Engineering Task Force;
- ICSA – International Computer Security Association;
- Information Systems Audit and Control Association (ISACA);
- Internet Security Alliance.

International Telecommunication Union (ITU) – Международный союз электросвязи является старейшей международной организацией, связанной с информационными технологиями. Она была основана в 1885 году как Международный телеграфный союз и получила свое новое название в 1934 году. В настоящее время ITU объединяет 189 государств. Как понятно из названия, ос-

новной ее задачей изначально было управление и координация деятельности в сфере передачи информации и, в частности, в радиосвязи и телеграфной связи. Однако по мере развития глобальных компьютерных сетей и интеграции компьютерных и телекоммуникационных систем, область деятельности ITU была значительно расширена и в настоящее время включает в себя множество вопросов, связанных с построением компьютерных сетей, передачей цифровых данных, обработкой информации и др.

Членами ITU-T являются:

- государственные органы власти (министерства и ведомства связи отдельных стран);
- научные организации и компании – производители телекоммуникационного оборудования;
- региональные и международные телекоммуникационные организации.

Функциональными органами ITU-T являются:

- Всемирная ассамблея по стандартизации телекоммуникаций (World Telecommunication Standardization Assembly), проводимая каждые четыре года, – основной руководящий орган сектора стандартизации;
- Бюро по стандартизации телекоммуникаций (Telecommunication Standardization Bureau) – исполнительное подразделение сектора стандартизации;
- Исследовательские группы (всего их 14);
- Консультативная группа по стандартизации телекоммуникаций (Telecommunication Standardization Advisory Group) – вспомогательное подразделение, осуществляющее координационную работу.

Высшим органом власти Союза является Полномочная Конференция (Plenipotentiary Conference), собрание делегаций государств – членов Союза, проходящее раз в четыре года. Основные исполнительные органы — Совет и Генеральный секретариат ITU. Основные рабочие подразделения разделены на три сектора: сектор стандартизации связи, ITU-T; сектор радиосвязи, ITU-R; сектор развития электросвязи ITU-D.

ITU-R и ITU-D выполняют отдельные исследовательские, координационные и технические функции (такие как, например, регистрация радиочастот или координация работы космических телекоммуникационных спутников), тогда как Сектор стандартизации связи – ITU-T в большей степени отвечает за решение стратегических задач развития информационных технологий и

инфраструктуры и, в частности, за разработку методик и стандартов, необходимых для всего мирового сообщества.

Основной целью работы ITU-T является разработка универсальных рекомендаций и международных стандартов, относящихся к различным сферам телекоммуникационных технологий и управления телекоммуникациями. Разрабатываемые рекомендации обеспечивают основу для развития рынка услуг связи, создания совместимых технических и организационных систем и др. С точки зрения обеспечения информационной безопасности наиболее значимыми стали рекомендации, относящиеся к серии "X – Сети передачи данных и связь открытых систем" и, в частности, к серии "X.8xx – Безопасность".

В соответствии с Резолюцией 1 Всемирной ассамблеи по стандартизации телекоммуникаций 2000-го года, была введена практика назначения Ведущих исследовательских групп (Lead Study Groups, LSGs) по определенным вопросам, требующим одновременной координации усилий нескольких исследовательских групп, которые работают в различных областях. Начиная с сентября 2001 года функционирует "Исследовательская группа 17: Сети передачи данных и телекоммуникационное программное обеспечение" ("Study Group 17: Data Networks and Telecommunication Software"), образованная на основе существовавших до этого "Исследовательской группы 7" и "Исследовательской группы 10". С момента своего образования она является Ведущей исследовательской группой по вопросам безопасности коммуникационных систем (Communication Systems Security, CSS) и, соответственно, не только работает над обеспечением безопасности технологий, напрямую относящихся к ее компетенции, но и курирует вопросы обеспечения безопасности различных коммуникационных технологий, разрабатываемых другими исследовательскими группами.

Одной из наиболее значимых разработок этой группы в сфере информационной безопасности считается Стандарт X.509, заложивший основы развития инфраструктуры публичных ключей. Наиболее актуальными проблемами, над которыми в настоящее время работает Ведущая исследовательская группа по вопросам безопасности коммуникационных систем, являются: управление безопасностью; безопасность мобильных систем; безопасность систем связи служб реагирования на чрезвычайные ситуации; телебиометрия.

В целом же работа этой исследовательской группы охватывает следующие основные сферы:

– безопасность управления сетями (включает в себя работу над следующими рекомендациями: M.3010 – Принципы сетей управления телекоммуникациями, M.3016 – Обзор безопасности сетей управления телекоммуникациями и некоторые другие);

– аутентификация и службы каталогов (X.500 – Обзор концептуальных моделей и сервисов, X.509 – Основы технологии публичных ключей и сертификатов и некоторые другие);

– управление системами (X.733 – Функция отчета о происшествии, X.740 – Функция проведения аудита безопасности и некоторые другие);

– основы архитектуры безопасности (X.800 – Архитектура безопасности инфраструктуры открытых систем для приложений ITU; X.802 – Модель безопасности нижних уровней, X.803 – Модель безопасности верхних уровней и некоторые другие);

– факсимильная связь (T.36 – Возможности обеспечения безопасности при использовании факсимильных аппаратов третьей группы; T.563 – Характеристики терминалов для использования с факсимильными аппаратами четвертой группы и некоторые другие);

– телевизионные и кабельные системы (J.170 – Спецификация безопасности IPCabelcom и некоторые другие);

– техника обеспечения безопасности (X.841 – Объекты информационной безопасности для контроля доступа и некоторые другие);

– мультимедийные коммуникации (H.233 – Система обеспечения конфиденциальности для аудиовизуальных сервисов, H.234 – Управление ключами шифрования и системой аутентификации в аудиовизуальных сервисах и др.

Помимо разработки рекомендаций и стандартов, одним из важных направлений работы ITU также стало обеспечение информационного обмена в различных формах: распространение методических материалов, касающихся обеспечения информационной безопасности, проведение семинаров и конференций. Одним из наиболее масштабных таких мероприятий является Всемирный саммит по информационному обществу (WSIS: The World Summit On The Information Society).

Institute of Electrical and Electronics Engineers (IEEE) – Институт инженеров по электронике и электротехнике IEEE является одной из наиболее известных профессиональных организаций, существует с 1884 года и в настоящее время насчитывает около 380000 членов из 150 стран мира. В сферу ее интересов входит множество вопросов, связанных с электротехникой, радиоэлек-

троникой, вычислительной техникой, информатикой, а также некоторыми разделами физики и математики. Основные направления работы этой организации: проведение специализированных профессиональных конференций; публикация специализированных изданий; поддержка образовательной деятельности; поддержка инновационных технических и методических разработок в различных сферах; разработка и распространение технических стандартов.

В состав IEEE входят 10 региональных отделений, 38 профессиональных обществ, 4 совета и 1450 студенческих отделений. Текущее управление деятельностью на верхнем уровне осуществляется Советом директоров и Исполнительным комитетом, работу которых возглавляют Президент и Исполнительный директор. Одним из основных подразделений IEEE, специализирующихся на вопросах информационной безопасности, является Технический комитет по безопасности и защите частной информации – "IEEE Computer Society Technical Committee on Security and Privacy"(http://www.ieee-security.org/).В его составе функционируют три подкомитета:

1. Подкомитет по стандартам (Subcommittee on Standards);
2. Подкомитет по академической работе (Subcommittee on Academic Affairs);
3. Подкомитет по специализированным конференциям (Subcommittee on Security Conferences).
4. Основными мероприятиями, которые проводит этот комитет, являются:
5. Ежегодный симпозиум по безопасности и защите частной информации (IEEE CS Symposium on Security and Privacy);
6. Ежегодный семинар по основам информационной безопасности (Computer Security Foundations Workshop).

Также комитет ведет работу по сбору и обобщению актуальной информации о событиях в сообществе специалистов по информационной безопасности: объявления о планируемых конференциях, отчеты о прошедших конференциях и семинарах, обзоры литературы и периодики, ссылки на ресурсы в сети Интернет и др. Специальный информационный бюллетень с этой информацией – "Cipher" – рассылается подписчикам в среднем один раз в два месяца.

Association for Computing Machinery (ACM) – Ассоциация вычислительной техники является одной из старейших организаций, связанных с информационными технологиями – была основана в 1947 году, на заре раз- вития компьютерной техники.

Основные задачи ACM - поддержка образовательных проектов в сфере информационных технологий, организация научно-практических конференций, симпозиумов и семинаров, общественно-политическая работа, связанная с информационными технологиями, публикация периодических изданий и сборников научных трудов, посвященных проблемам современных информационных технологий, поддержка электронного архива таких публикаций, а также другая подобная деятельность. Основным управляющим органом этой организации является Совет ACM, в который входит 16 человек, в том числе президент и вице-президент. Управление текущими делами Ассоциации осуществляют четыре профильных комитета. Штаб-квартира ACM, в которой работают основные исполнительные органы, располагается в Нью-Йорке начиная с 1960 года.

Одной из основ организации работы ACM является разделение всего сообщества членов ассоциации на так называемые группы специальных интересов (Special Interests Group – SIG) – подразделения, специализирующиеся на отдельных относительно узких проблемах развития информационных технологий. Всего ACM объединяет 34 группы, специализирующиеся на различных вопросах разработки и использования программного обеспечения, аппаратных средств и телекоммуникаций. Каждая из групп самостоятельно определяет для себя границы своей деятельности, а их политика и финансовые вопросы координируются одним из комитетов.

Одна из этих групп – Special Interest Group on Security, Audit and Control (SIGSAC, Группа специальных интересов по вопросам безопасности, аудита и контроля, http://www.acm.org/sigs/sigsac/) – специализируется на вопросах информационной безопасности. Основной задачей данной группы является организация работы специализированных научно-практических конференций, таких как: симпозиум по технологиям и моделям управления доступом (SACMAT: ACM Symposium on Access Control Models and Technologies), проводимый ежегодно начиная с 1995 года; конференция по безопасности компьютеров и коммуникаций (CCS: ACM Conference on Computer and Communications Security), проводимая ежегодно начиная с 1993 года. Кроме того, вопросы информационной безопасности прямо или косвенно затрагиваются в работе других специализированных групп Ассоциации, таких как, например, Special Interest Group on Electronic Commerce (Группа по проблемам электронной коммерции).

World Wide Web Consortium (W3C) – Консорциум Всемирной Паутины.

Создание W3C было инициировано в 1989 году с целью разработки единых, согласованных стандартов обмена информацией в глобальных сетях передачи данных, а официально создание консорциума было оформлено в 1994г. Его основными задачами являются:

- обеспечение возможности доступа к сети Интернет для как можно большего числа людей вне зависимости от знания иностранных языков, культурной принадлежности, географического положения и доступных им технических средств и технической инфраструктуры;
- обеспечение возможности подключения к Интернет различных технических устройств;
- обеспечение возможности структурирования и формализации информации, доступной через Интернет, с целью сделать ее как можно более пригодной для автоматизированной обработки;
- обеспечение надежности и безопасности обмена информацией, а также возможности участвовать в информационном обмене с тем уровнем защищенности, который отдельные пользователи считают для себя подходящим.

К настоящему времени консорциум объединяет более четырехсот ведущих технологических и телекоммуникационных компаний, правительственных организаций, исследовательских центров, институтов и университетов по всему миру. Кроме того, в штате консорциума состоят около 70 независимых технических экспертов, обеспечивающих его работу. Финансирование деятельности осуществляется за счет членских взносов, а основные административные функции и повседневная деятельность выполняются на базе трех организаций:

1. Массачусетский технологический институт (США);
2. Европейский консорциум по исследованиям в области информатики и математики (Франция);
3. Университет Кейо (Япония).

Помимо формирования стандартов ("рекомендаций"), эта организация также занимается образовательной деятельностью и предоставляет возможности для обсуждения различных вопросов, связанных с функционированием Интернет. Деятельность консорциума организована в виде групп: Рабочие группы (занимаются проработкой технических вопросов), Группы специальных интересов и Координационные группы (обеспечивают взаимодействие

между другими группами). В каждую группу входят представители организаций-участников консорциума и приглашенные эксперты. Сферы работы консорциума ("домены", Domain), разделены на направления (Activities). Работа по двадцати четырем направлениям выполняется в общей сложности шестьюдесятью группами. Вопросами информационной безопасности занимается сфера "Технология и общество" (Technology and Society Domain) в рамках специального направления "Безопасность" (W3C Security Activity), состоящего из двух рабочих групп. Также до 2006 года в составе Консорциума функционировало направление "Защита частной информации" (Privacy).

К работам консорциума в сфере информационной безопасности относятся: разработка стандарта цифровых подписей для информационных ресурсов (PICS Signed Labels 1.0 Specification); разработка системы электронной подписи для документов XML; разработка стандартов передачи зашифрованных данных с использованием языка XML.

International Organization for Standardization (ISO) – Международная организация по стандартизации. ISO в нынешнем виде была учреждена в 1946г. и представляет собой неправительственное объединение национальных организаций по стандартизации, нацеленное на унификацию стандартов (главным образом, технических) в различных областях производственной деятельности и оказания услуг.

Помимо основных членов (156 стран), непосредственно участвующих в работе, в ISO также входят члены-корреспонденты (Correspondent member) – страны, не имеющие полноценных органов стандартизации, а также члены-подписчики (Subscriber member) – страны с небольшими экономиками, получающие необходимую справочную информацию на льготных условиях.

Главным органом управления ИСО является ежегодная Генеральная Ассамблея, принимающая стратегические решения, касающиеся развития всей организации. Подготовкой материалов для принятия таких решений занимается Совет ИСО, собрания которого проходят два раза в год. Непосредственно разработкой стандартов занимаются технические комитеты и подкомитеты, в работе которых принимают участие представители заинтересованных стран. За разработку каждого документа в подкомитете отвечает специально создаваемая для этого рабочая группа. Проекты международных стандартов, принятые техническими комитетами, рассылаются в национальные организации для голосования; документ приобретает ста- тус международного стандарта,

если за него проголосовало не менее 75% членов, участвовавших в голосовании. Основным подразделением ИСО, занимающимся вопросами информационной безопасности, является Объединенный технический комитет JTC 1 "Информационные технологии", в состав которого входит подкомитет SC 27 "Средства безопасности в информационных технологиях" (IT Security techniques). За время своей работы этот подкомитет разработал более 60 международных стандартов, относящихся к информационной безопасности.

С вопросами информационной безопасности также связана работа подкомитета SC 37 "Биометрическая идентификация" (Biometrics) и подкомитета SC 17 "Карточки и персональная идентификация" (Cards and personal identification).

Классификация и направления работы специализированных международных организаций и объединений в сфере информационной безопасности.

Специализированные организации, имеющие глобальное влияние на управление информационной безопасностью на различных уровнях и общее состояние информационной безопасности, как правило, могут функционировать на базе:

- частных компаний, занимающихся исследованиями, разработками и консультированием в сфере информационной безопасности;
- крупных учебных заведений, специализирующихся на информационных технологиях, а также обладающих существенным авторитетом и финансовыми ресурсами;
- правительственных учреждений, ответственных за обеспечение информационной безопасности в определенных сферах.

Основным направлением организационной работы, осуществляемой в такой форме, становится формирование и поддержание баз данных, содержащих информацию о ставших известными уязвимостях различных программных и аппаратных средств, а также другие формы и направления информационной, консультативной и методической работы в данной сфере. Важными факторами успешности функционирования таких организаций является объединение информации из как можно большего числа источников (в частности, от как можно большего числа специалистов и компаний, занимающихся проблемами информационной безопасности) и как можно более эффективное распространение сведений (знаний) в сообществе пользователей информационных систем.

Ввиду того, что такая форма организационной работы основана на частных компаниях и относительно небольших учре-

ждениях, подходы к организации и управлению обычно не подчиняются каким-либо общим правилам. Также состав таких организаций может со временем меняться: на смену одним исследовательским центрам могут приходить другие – более успешные и эффективные – с теми же функциями. В настоящее время можно выделить следующие наиболее значимые организации, занимающие эту нишу: CERT Coordination Center – Координационный центр CERT; исследовательская группа X-Force компании IBM.

CERT Coordination Center (CERT/CC) – Координационный центр CERT CERTCC, возникшая в 1988 году как Computer security incident response team (Группа реагирования на инциденты, связанные с компьютерной безопасностью), функционирует на базе Института разработки программного обеспечения при Университете Карнеги-Мелон (Software Engineering Institute, Carnegie Mellon University) и финансируется Министерством обороны и Министерством национальной безопасности США. Наряду с проведением независимых исследований и решением различных задач по обеспечению безопасности глобальной информационной инфраструктуры, эта организация обеспечивает централизованный сбор сведений обо всех уязвимостях в различных информационных системах и поддержание актуальной базы знаний об уязвимостях в информационных системах. Сведения о вновь выявляемых уязвимостях, вредоносных программах и способах нарушения информационной безопасности рассылаются по электронной почте: подписчиками этого бюллетеня являются более 161000 специалистов во всем мире. В рамках этой деятельности CERT/CC осуществляет постоянную исследовательскую работу:

- определение характера возможных последствий использования выявленных уязвимостей и вирусов;
- анализ имеющихся средств использования уязвимостей;
- анализ того, насколько активно используются уязвимости и насколько широко распространены вирусы;
- взаимодействие с поставщиками информационных систем с целью более глубокого анализа выявляемых уязвимостей.

На основе проводимого анализа CERT/CC разрабатывает меры по устранению уязвимостей и рекомендации по уменьшению негативных последствий. По результатам этой работы всем подписчикам рассылается информация об угрозах информационной безопасности и возможных способах их устранения. Также на основе этих данных формируется специальная справочная и техническая документация, проводится дальнейшая исследовательская и методическая работа. В част- ности, CERT/CC поддерживает

программу безопасной разработки ПО ("secure coding"), вающуюся на том, что большая часть уязвимостей возникает в следствие относительно небольшого числа ошибок в программном коде информационных систем. Таким образом, CERT/CC на основе накопленных результатов анализа уязвимостей ведет целенаправленную работу по выявлению типичных программных ошибок, выработке стандартов безопасного программирования и распространению этой информации среди разработчиков ПО. Помимо основной информационной работы с уязвимостями CERT также занимается сопутствующими видами деятельности:

- организация учебных курсов по различным направлениям (сетевая безопасность, управление информационными рисками, организация работы групп реагирования);
- сертификация специалистов по реагированию на инциденты в сфере информационной безопасности;
- поддержка фундаментальных научных исследований в различных областях информационной безопасности, таких как методы разработки безопасных приложений, выявление уязвимостей, анализ шпионского ПО, решение вопросов безопасности как составная часть процесса разработки и др.;
- содействие развитию локальных (национальных и корпоративных) групп реагирования на инциденты.

X-Force security intelligence team – Исследовательская группа X-Force. Деятельность этой группы является одним из направлений бизнеса компании Internet Security Systems (ISS) – наиболее авторитетного поставщика комплексных решений в сфере информационной безопасности, клиентами которого являются все без исключения крупнейшие компании США, а также правительственные организации. В конце 2006 года ISS была куплена компанией IBM и интегрирована в нее в качестве самостоятельного подразделения. Одной из задач группы X-Force является поддержание в актуальном состоянии базы данных известных уязвимостей различных программных и аппаратных платформ. База данных, поддерживаемая этой группой, доступна по сети Интернет и постоянно пополняется сведениями о новых уязвимостях (в настоящее время их насчитывается более 40000). Основные причины, по которым данная организация является ведущей в этой области, следующие:

- большое количество крупных компаний-клиентов, от которых постоянно поступает информация о нападениях, уязвимостях и др.;
- наличие собственной научно-исследовательской ба-

зы, на основе которой постоянно осуществляется выявление вых уязвимостей и обобщение сведений об уязвимостях, полученных из различных источников;

– использование специально разработанных универсальных классификаций (в частности, общего словаря наименований уязвимостей – Common Vulnerabilities and Exposures, CVE) для хранения и обработки информации в базах данных известных уязвимостей.

Также одним из направлений справочно-информационной деятельности этой исследовательской группы является оказание услуг по индивидуальному анализу угроз и информированию (X-Force Threat Analysis Service (XFTAS)). Данный комплекс услуг позволяет заказчикам ежедневно получать адаптированную актуальную информацию об угрозах и уязвимостях с учетом особенностей построения их информационных систем (платформ, приложений, сферы ведения бизнеса, географического положения) и включает в себя: информацию об угрозах; экспертный анализ угроз; описание текущего и прогнозного состояния угроз; рекомендуемые способы устранения угроз; количественный анализ атак за последние 30 дней. Еще одной из задач группы является выпуск периодических (ежеквартальных, ежегодных) информационных бюллетеней с обзорами наиболее значимых событий в сфере информационной безопасности.

Альянсы крупных технологических компаний. Совместные альянсы (ассоциации, коалиции, группы) крупных (иногда средних) технологических и консультационно-исследовательских компаний представляют собой временные (заключаемые на краткосрочную или среднесрочную перспективу) или долгосрочные соглашения между несколькими фирмами, направленные на совместное, скоординированное, целенаправленное решение определенных масштабных и ресурсоемких задач развития технологии, формирования рыночного спроса на определенные продукты и организации инфраструктуры информационной безопасности. Высокая значимость такой формы организационной работы в сфере информационной безопасности, как формирование альянсов крупными и средними компаниями, специализирующимися на информационных технологиях, обусловлена тем, что:

– такие альянсы способны осуществить наиболее крупные инвестиции в разработку новых технологий и проведение исследований, которые могут повлиять на все развитие информационных технологий и состояние дел в сфере информационной безопасности;

– компании, входящие в такие альянсы, занимают значительную долю рынка и потому определяют общее направление развития информационных технологий вообще и средств защиты информации в частности;

– такие альянсы компаний способны создать комплексные технологии, продукты и решения, охватывающие различные аспекты функционирования информационных систем и средств защиты информации, и таким образом достичь нового уровня защищенности информации, что практически невозможно при работе компаний (даже самых крупных) по отдельности.

Как правило, каждый такой альянс является уникальным, и участники в каждом конкретном случае определяют условия работы в рамках такой организационной формы. На конкретный подход к организации альянса могут повлиять такие факторы, как:

– характер целей и задач, которые ставятся перед альянсом;

– текущее состояние дел в той области, для работы в которой создается альянс;

– состав участников альянса, их роль и место на рынке информационных технологий;

– наличие возможных конкурентов (например, аналогичных альянсов параллельно создаваемых другими группами компаний);

– ранее сложившиеся взаимоотношения между компаниями – участниками альянса и др.

Задачами формирования альянсов могут быть:

– разработка новых продуктов и услуг, а также базовых технологий, протоколов, алгоритмов и соглашений, на основе которых такие продукты и услуги в будущем могли бы разрабатываться;

– формирование новых рынков сбыта и поддержка существующих;

– влияние на государственные и общественные организации, а также на сообщество пользователей информационных систем с целью обеспечения развития и более широкого использования информационных технологий и средств информационной безопасности;

– влияние на систему профессиональной подготовки специалистов с целью обеспечения качества их обучения.

Основными типичными приемами организационной работы на таком уровне являются:

– скоординированный вы- бор и унификация технических

решений (аппаратных устройств, программных алгоритмов), пользуемых в системах передачи и обработки информации и/или системах защиты информации;

– информационная поддержка как производителей информационных систем и поставщиков решений (входящих в альянс и не входящих в него), так и потребителей и пользователей (потенциальных и настоящих);

– скоординированное разделение функций по разработке отдельных элементов информационной технологии в рамках общей согласованной стратегии развития;

– скоординированная маркетинговая и информационная политика, направленная на обеспечение использования (поддержки, совместимости) создаваемых решений (технологий, протоколов и др.) как можно большим числом потребителей и независимых производителей, а также ее признание правительственными структурами;

– совместное влияние на органы государственной власти (лоббирование) с целью обеспечения государственной поддержки определенных продуктов, проектов, технологий и архитектур информационных систем и систем защиты информации.

Smart Card Alliance (SCA) – Альянс по смарт-картам. SCA (http://www.smartcardalliance.org) занимается вопросами развития технологии смарт-карт – одной из ключевых технологий в сфере информационной безопасности, используемой для идентификации пользователей различных сервисов и информационных систем (таких как мобильные телефонные сети, банковские "электронные кошельки" и др.). Этот долгосрочный (стратегический) альянс был образован в начале 2001 года путем слияния двух организаций: Smart Card Industry Association и Smart Card Forum. В состав альянса входят около сотни различных компаний и правительственных организаций. При этом в составе участников альянса выделяются несколько групп:

1. Руководящий Совет (Leadership Council) – ведущие компании, определяющие основную политику Альянса: Visa USA, Bank of America, IBM, Lockheed Martin, Intel, Mastercard International и некоторые другие (всего более двадцати компаний);

2. основная группа членов Альянса – различные фирмы, так или иначе связанные с вопросами информационной безопасности, поставкой соответствующих продуктов и услуг (такие как Texas Instruments Incorporated, Sun Microsystems и другие) – всего около 70 компаний;

3. члены – правительст- венные организации. В эту

группу входят как федеральные правительственные учреждения США (Государственный департамент, Министерство национальной безопасности и другие), так и местные органы власти (Портовая администрация Нью-Йорка, Транспортная администрация Вашингтона и другие) – всего около 30 членов.

Также в состав Альянса входит один университет и несколько ассоциированных членов. Работу альянса возглавляют Совет директоров во главе с председателем и Исполнительный директор. Деятельность альянса разделена на членские советы (Member Council) по отдельным сферам интересов:

1. Совет по бесконтактным и мобильным платежам.
2. Совет по здравоохранению (специализируется на вопросах использования смарт-карт в сфере здравоохранения).
3. Совет по идентификации.
4. Совет по системам контроля за физическим допуском.
5. Совет по транспорту (специализируется на вопросах продвижения и адаптации смарт-карт в транспортной сфере).

Каждый совет управляется председателем, вице-председателями и управляющим комитетом. Направления работы Альянса включают в себя:

- организацию специализированных ежегодных конференций;
- организацию образовательных программ и системы сертификации специалистов;
- издание различных информационных и справочных материалов как технического, так и управленческого характера;
- ведение централизованной базы данных поставщиков оборудования и услуг в сфере смарт-карт.

Internet Security Alliance (ISA) – Альянс по безопасности сети Интернет. ISA был создан в апреле 2001 года по инициативе двух крупных авторитетных организаций: CERT/CC Университета Карнеги-Меллон и Ассоциации электронной промышленности (Electronic Industries Alliance, EIA). Уже к середине 2004 года в альянс входило около тридцати членов, в числе которых такие крупные компании, как Boeing, NEC, Mitsubishi, Federal Express, AIG, Sony, Symantec и другие. Работой Альянса руководит Совет директоров, в который входят авторитетные представители наиболее известных компаний-членов. Кроме того, в состав альянса входят около тридцати ассоциированных членов. На первоначальном этапе создания альянса его основной задачей было повышение эффективности обмена информацией об уязвимостях, распространяемой CERT/CC. В дальнейшем круг задач альянса

расширялся, и теперь работа ведется по следующим направлениям:

- создание эффективных механизмов обмена информацией об уязвимостях в сети Интернет и найденных решениях проблем безопасности;
- исследование фундаментальных проблем безопасности;
- развитие программ профессиональной подготовки и сертификации специалистов по информационной безопасности;
- взаимодействие и государственными органами законодательной и исполнительной власти.

The International Biometric Industry Association (IBIA) – Международная ассоциация компаний-производителей биометрического оборудования. Ассоциация была создана в 1998 году с целью коллективной поддержки интересов компаний, связанных с производством биометрического оборудования. Основной задачей альянса является взаимодействие с потенциальными заказчиками их продукции (как среди коммерческих компаний, так и в общественном секторе) с целью продвижения средств биометрической идентификации. Членами ассоциации являются около 30 компаний и организаций, среди которых Hitachi, LG Electronics, Panasonic, NEC и другие. Управление текущими делами осуществляет Совет директоров в составе одиннадцати человек, а также исполнительный директор. Деятельность Ассоциации разделена на шесть рабочих групп, среди которых:

- рабочая группа по стандартам и технологиям. Ее основная цель – защищать базовые интересы членов альянса в сфере стандартизации биометрических технологий и систем, использующих биометрию;
- рабочая группа по потребительским приложениям. Занимается ориентацией рынка потребительских систем на более широкое использование биометрических технологий;
- рабочая группа по международным рынкам. Осуществляет контакты с другими биометрическими организациями по всему миру;
- рабочая группа по образованию, маркетингу и информированию. Обеспечивает информационное присутствие компаний-членов ассоциации в различных областях через реализацию маркетинговых мероприятий и образовательных программ;
- рабочая группа по глобальной политике. Проводит информационную работу с представителями правительственных структур по всему миру.

2. Практическая часть.

1) Вопросы по разделу:

1) На какой базе могут функционировать специализированные организации, имеющие глобальное влияние на управление информационной безопасностью на различных уровнях и общее состояние информационной безопасности?

2) Характеристика CERT Coordination Center – координационного центра CERT?

3) Характеристика исследовательской группы X-Force компании IBM?

4) Характеристика технологической компании Smart Card Alliance (SCA) – альянса по смарт-картам?

5) Характеристика технологической компании Internet Security Alliance (ISA) – Альянса по безопасности сети Интернет?

6) Характеристика технологической компании The International Biometric Industry Association (IBIA) – международной ассоциации компаний-производителей биометрического оборудования?

2) Задание.

Разработать презентацию: «Деятельность международных организаций в сфере управления информационной безопасностью»

3) Порядок отчетности и форма контроля выполнения работы.

Контроль выполнения задания производится по окончании занятия и на консультациях в форме защиты выполненной работы, предоставленной в электронном и в бумажном виде в форме «Отчет по лабораторной работе …».

3. Материально-техническое обеспечение.

Специализированная мебель и технические средства для представления учебной информации, включая проекционное оборудование; компьютерный класс с компьютерами AMD 2400 – 12 шт., оснащенными операционной системой Windows XP и пакетом Microsoft Office.

ЛАБОРАТОРНАЯ РАБОТА 4
СИСТЕМА ПРАВ ДОСТУПА

Цель занятия – приобретение обучаемыми необходимого объёма знаний и практических навыков в области системы прав доступа в качестве системы безопасности.

Время – 4 часа.

Учебные вопросы:

1. **Теоретическая часть:**
1) Система прав доступа *Windows XP*.
2) Настройка пользовательской учетной записи.
3) Восстановление забытого пользователем пароля.
4) Выполнение действий над пользователями системы.
5) Работа с пользовательскими группами.
6) Управление входом пользователей в систему.
2. **Практическая часть:**
1) Вопросы по разделу.
2) Порядок отчетности и форма контроля выполнения работы.
3. **Материально-техническое обеспечение.**

1. Теоретическая часть.

1) Система прав доступа *Windows XP*.

При включении компьютера после загрузки операционной системы на экране появляется приветствие, после чего предлагается выбрать режим работы (имя пользователя, учетная запись или аккаунт пользователя) под которым вы войдете в сеанс работы с системой. Если компьютер входит в состав домена с большим количеством пользователей, то вместо экрана «Приветствия» появится экран, где необходимо ввести названия учетной записи в системе и пароль.

Правильно составленный пароль должен иметь не менее восьми символов в длину, должен содержать строчные и прописные символы, цифры и различные метасимволы, чтобы иметь гарантию, что пароль всегда будет уникальным.

Для успешного функционирования операционной системы должна быть введена определенная система безопасности, базирующаяся на системе прав доступа. Ниже приведены стандартные права пользователей, предусмотренные в операционной системе *Windows XP*.

Чтобы каждый раз при создании нового пользователя не указывать комбинации похожих прав пользователей, в системе существует несколько готовых прав для пользователей, пригодных для реального использования системными администраторами и отдельными пользователями, называемых группами. В *Windows XP* существует 10 основных групп пользователей:

– *Администраторы* (*Administrators*) – пользователи имеют полный и неограниченный доступ к компьютеру;

– *Операторы* сохранения и резервирования данных (*Backup Operator*) – пользователи могут заниматься сохранением информации и ее резервированием на будущее;

– *Гости* (*Guests*) – пользователи имеют доступ аналогичный группе *Пользователи*, но несколько более урезанный, по умолчанию группа отключена;

– *Операторы сетевой конфигурации* (*Network Configuration Operators*) – пользователи могут иметь некоторые административные привилегии для управления сетевыми возможностями системы;

– *Опытные пользователи* (*Power Users*) – пользователи, входящие в группу, имеют практически те же права, что и администраторы системы, но только с некоторыми ограничениями;

– *Replicator* – используется для организации работы системы в домене, а именно для репликации файлов в домене;

– *Пользователи* (*Users*) – наиболее популярная группа, в которую входят простые пользователи; все пользователи, которые работают в системе, должны входить в эту группу, т.к. они защищены от случайного уничтожения информации или изменения системы;

– *Пользователи, осуществляющие отладку* (*Debugger Users*) – пользователи имеют право на отладку программ и процессов на данной машине, локально или удаленно;

– *Помощники* (*HelpServicesGroup*) – группы пользователей для помощи и Центра Поддержки.

Если требуется, чтобы у пользователя был набор прав, состоящий из прав по нескольким группам, то можно его сделать членом всех этих групп. Тогда набор прав будет равен сумме прав, входящих в группы, членом которых пользователь является. Например, если обычному пользователю иногда нужно сохранять или резервировать информацию системы, осуществлять отладку программ, то пользователь может быть членом трех групп:

Users, *Backup Operators* и *Debug Users*. Для доступа к программе управления пользователями, необходимо запустить программу *Computer Management*:

Пуск – Панель управления – Администрирование – Управление компьютером – Локальные пользователи и *Группы* (рис. 1) Для выполнения административных действий: смены пароля, изменения свойств пользователя и пр. необходимы права администратора системы.

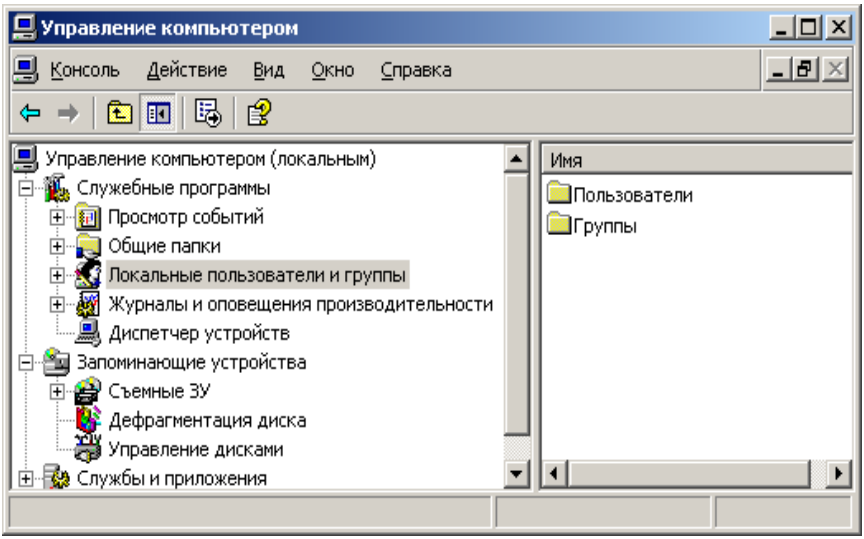


Рис.1. Окно программы Управление компьютером (*Computer Management*).

В зависимости от выполняемой работы, нужно выбрать *Пользователи* (*Users*) или *Группы* (*Groups*).

При выборе строки *Пользователи* в окне настройки пользователей (рис. 2) после выбора двойным щелчком любого из пользователей появится окно свойств пользователя (рис. 3).

После открытия закладок *Членство в группах* и *Профиль* появятся, соответственно, окно принадлежности пользователя группам пользователей (рис.4) и окно его настроек (рис.5).

В окне *Общие свойства пользователя* имеются следующие поля:

Потребовать смену пароля при следующем входе в систему – поле влияет на то, должен ли пользователь при своем следующем входе в систему менять свой пароль. Поле может быть по-

лезно, когда системный администратор при создании пользователя присваивает некоторый пароль по умолчанию. При первом сеансе работы, когда пользователь будет работать со своей информацией, система предложит ему ввести свой пароль, который не будет известен системному администратору, что говорит об уровне и комфорте безопасной работы.

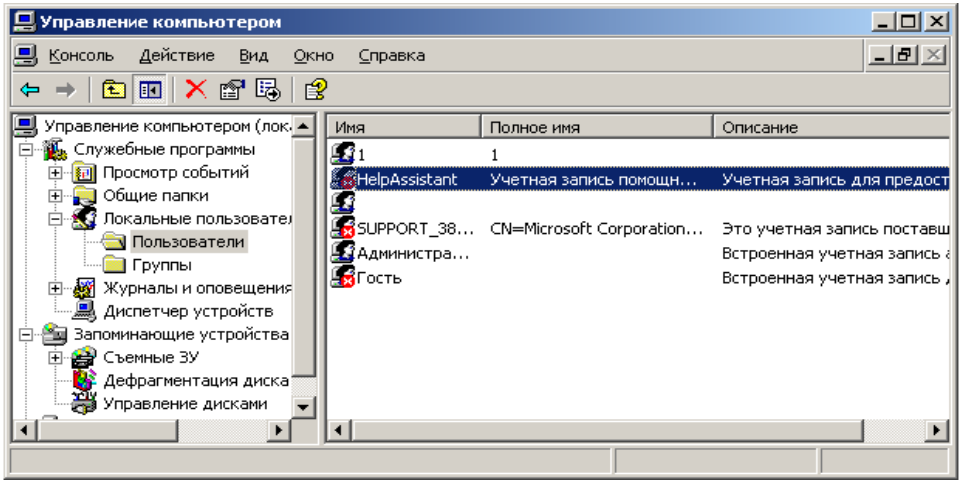


Рис.2. Окно настройки пользователей.

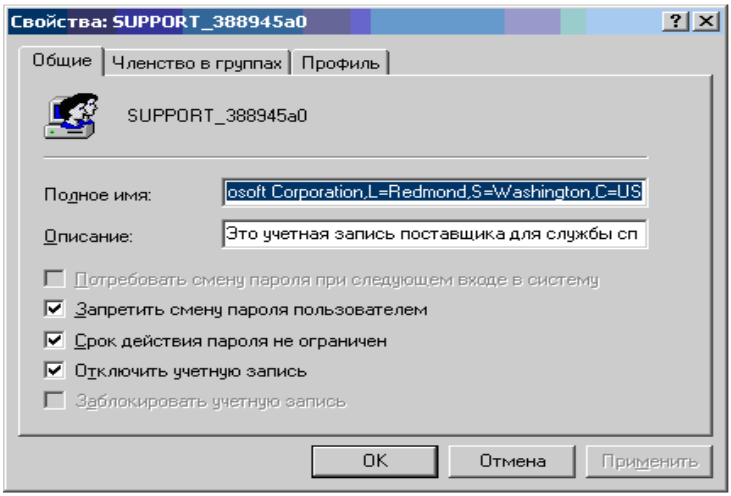


Рис.3. Окно свойств пользователей.

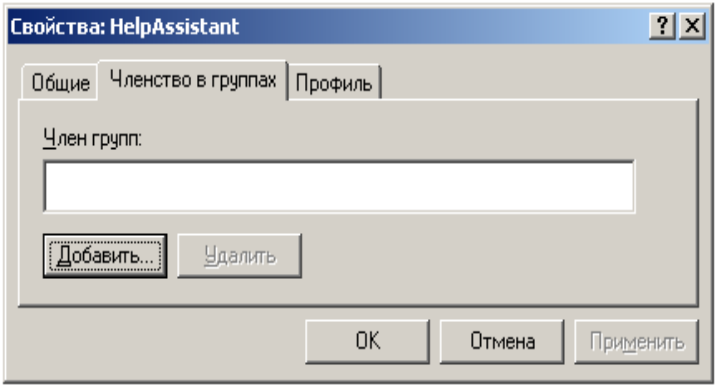


Рис.4. Окно принадлежности пользователя группам пользователей.

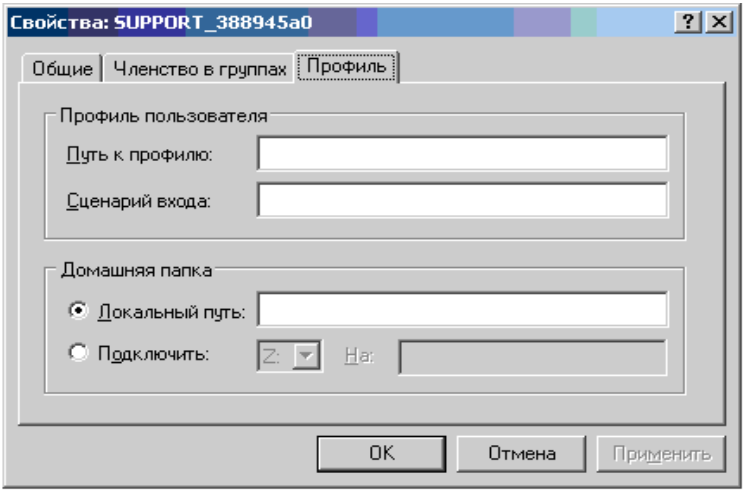


Рис.5. Окно настроек пользователей.

Запретить смену пароля пользователем – поле запрещает пользователю смену своего пароля. Данное свойство может быть полезно, например, когда в системе работает не опытный пользователь, умеющий менять пароли, но забывающий их.

Срок действия пароля не ограничен – поле указывает на то, что срок действия пароля данного пользователя никогда не истекает.

В политике безопасности системы принято, чтобы пользователи с определенной периодичностью, определяемой систем-

ным администратором, меняли свои пароли, что необходимо для целей безопасности сложных, многопользовательских систем, в которых хранятся большие объемы важной информации: финансовой, отчетной, инженерной и прочей. Отказ от этого правила может быть лишь в следующих случаях:

– система имеет только одного пользователя, с относительно малозначимой информацией;

– система имеет одного пользователя с надежным паролем для запоминания и устойчивым к взломам кракеров;

– пользователи обладают настолько малым желанием по обеспечению безопасности системы, что не желают поддержания секретности их паролей на должном уровне.

Отключить учетную запись – поле выполняет функции выключателя учетной записи пользователя. Это один из наиболее часто используемых полей в борьбе с недобросовестными пользователями, а также в целях защиты и настройки системы. Другая причина блокировки учетной записи заключается в том, что не все учетные записи принадлежат реальным пользователям. В системе существуют еще и специальные учетные записи, которые принадлежат виртуальным пользователям или некоторым системным службам, например, *аккаунт Guest*. Учетная запись имеет практически такие же права, за некоторыми исключениями, как и группа *Users*. Смысл *Гостевого входа* в том, что он используется для раздачи *Windows* сетевых ресурсов другим пользователям с удаленных систем: папок, файлов и пр. при работе системы в составе компьютерной сети. И если учетная запись *Гостя* не включена, то может оказаться невозможным вход пользователей из сети в данную систему.

Заблокировать учетную запись – поле обеспечивает работу одного механизма системы безопасности *Windows XP*. Существует ряд причин, когда система может запретить определенному пользователю входить в сеанс работы с системой. Это может быть из-за того, что система безопасности ОС настроена таким образом, что должна запрещать пользователям вход в систему, после определенного количества неправильно введенных паролей, чтобы избежать подбора пароля учетной записи методом подбора. Только системный администратор может вновь разблокировать запись пользователя, убрав флажок из поля *Заблокировать учетную запись*.

В окне *принадлежности пользователя группам пользователей* указывается принадлежности пользователя к определенным группам (рис. 4). Под списком пользователей находятся две

кнопки: *Добавить* и *Удалить*, которые управляют добавлением и удалением новых групп пользователей. Для удаления группы следует ее выделить щелчком мыши и нажать кнопку *Удалить*. Для добавления новых групп пользователей, к которым будет принадлежать выбранный пользователь, следует нажать кнопку *Добавить*. Появится окно выбора групп пользователей (рис.6.).

Окно содержит ряд кнопок и записей. Первая запись показывает тип объектов, по умолчанию стоит запись *Группы* (*Groups*). Вторая запись показывает, в какой системе производится работа, по умолчанию вписывается имя локальной системы.

При добавлении пользователей можно пропускать первые два поля, переходя сразу к нижнему полю, в которое нужно поместить имена объектов для добавления. Для добавления объектов следует нажать кнопку *Добавить*. Появится новое диалоговое окно (рис.7). Нажать кнопку *Поиск*. Появится окно выбора групп пользователей (рис. 8). Щелчком мыши выбираем имя группы пользователей (для выбора ряда групп пользователей используются клавиши *Shift* или *Ctrl*). Нажать кнопку *ОК* или сделать двойной щелчок по выбранной группе пользователей. Выбранные группы пользователей появятся в нижней части окна выбора групп пользователей (рис. 7). После выбора групп нажать кнопку ОК. Появится окно свойств пользователя (рис. 3) с добавленными в него группами.

Далее следует произвести настройку профиля пользователя. Для этого следует выделить группу (группы пользователей) и перейти на вкладку *Профиль* (рис. 5). Поля вкладки используются для работы *Windows XP* в больших сетях, чтобы пользователь имел доступ к другим ПК, подключенным к сети. Настройка данной вкладки гарантирует, что пользователь всегда получит доступ к личной информации, вне зависимости от его места нахождения.

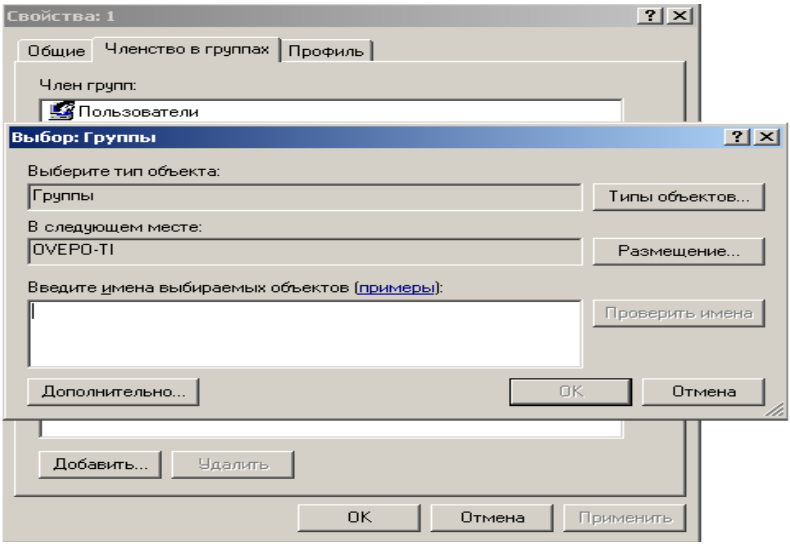


Рис.6. Окно выбора групп пользователей для добавления.

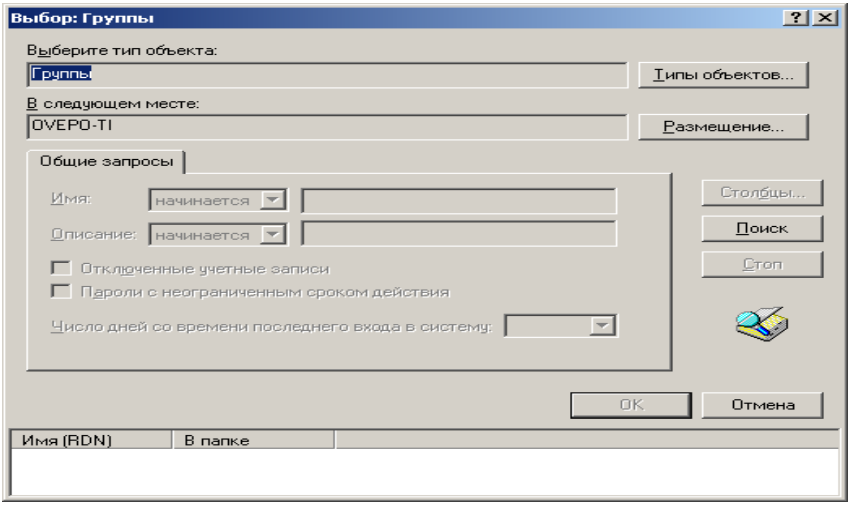


Рис.7. Окно выбора групп пользователей в расширенном варианте.

Имя (RDN)	В папке
Debugger Users	OVEPO-TI
HelpServicesGroup	OVEPO-TI
SQLServer2005MSSQLServerADHelperUser$OVEPO-TI	OVEPO-TI
SQLServer2005MSSQLUser$OVEPO-TI$SQLEXPRESS	OVEPO-TI
SQLServer2005SQLBrowserUser$OVEPO-TI	OVEPO-TI
Администраторы	OVEPO-TI
Гости	OVEPO-TI
Операторы архива	OVEPO-TI
Операторы настройки сети	OVEPO-TI
Опытные пользователи	OVEPO-TI
Пользователи	OVEPO-TI
Пользователи удаленного рабочего стола	OVEPO-TI
Репликатор	OVEPO-TI

Рис.8. Вывод имен доступных групп пользователей.

2) Настройка пользовательской учетной записи.

Для выполнения пользователем функций по настройке своей пользовательской учетной записи следует запустить программу *Учетные записи пользователей*: *Пуск - Панель управления – Учетные записи пользователей*

На экране появится окно, содержащее справа сверху имя пользователя, тип его учетной записи: административная или обычная пользовательская (рис. 9).

В окне отображен список учетных записей пользователя с указанием типа учетной записи: ограниченная учетная запись является обычной пользовательской; защита паролем указывает на то, что учетная запись защищена паролем. В верхней части окна приведен список действий *Выберите задание*, которые можно выполнить с конкретной (выделенной) учетной записью. Выберем учетную запись администратора. Появится новое окно (рис. 10).

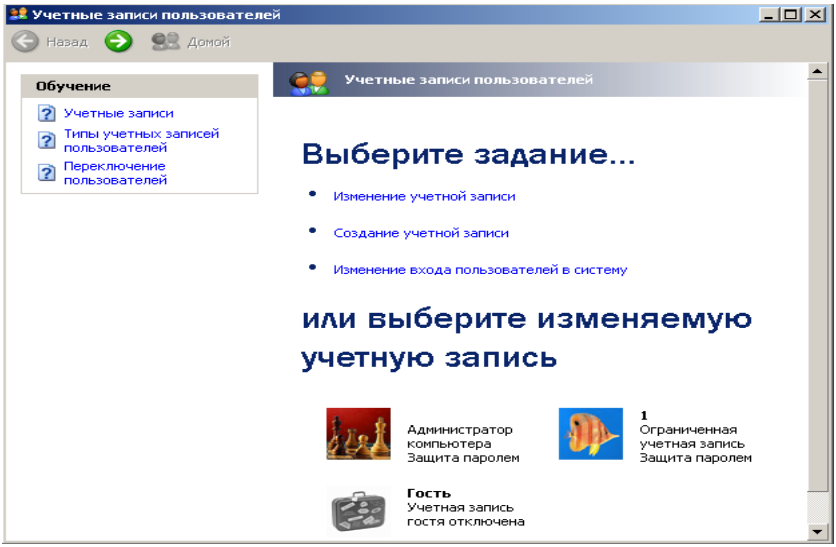


Рис.9. Окно программы *Учетные записи пользователя.*

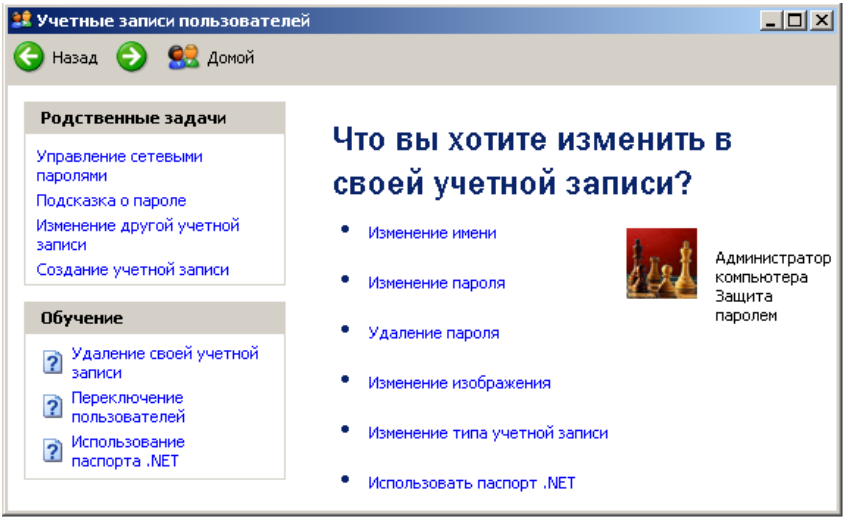


Рис.10. Окно программы *Учетные записи пользователя* конкретного пользователя (администратора).

1. Режим *Изменение имени* позволяет изменить имя пользователя. Для смены имени пользователя следует сделать щелчок по режиму. Появится новое окно (рис. 11). На клавиатуре набрать новое имя пользователя и нажать кнопку *Сменить имя*.

2. Режим *Изменение пароля* позволяет изменить пароль. После щелчка мышью по данному пункту появится окно смены пароля пользователя (рис. 11). В первом поле вводится текущий пароль пользователя, в двух следующих – новый пароль. В последнем поле рекомендуется ввести подсказку, чтобы легче было вспомнить установленный пароль. Для подтверждения нового пароля следует нажать кнопку *Изменить пароль*.

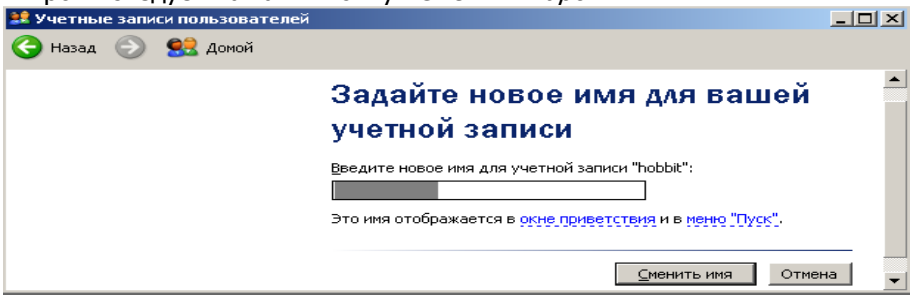


Рис.11. Окно смены имени выбранного пользователя.

3. Режим *Удаление пароля*. При активизации режима система поинтересуется, уверены ли вы в своем решении убрать пароль, т.к. вся информация, которая была доступна под вашим именем, станет доступна всем пользователям данной системы (рис. 12).

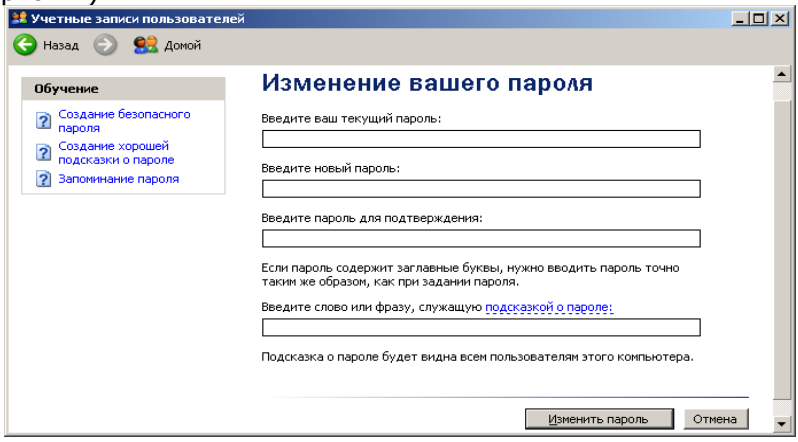


Рис.11. Окно изменения пароля выбранного пользователя.

4. Режим *Изменения изображения*. В *Windows XP* с именем каждого пользователя ассоциированная картинка, использование

которой делает работу с пользователями более наглядной. При активизации режима появится новое окно (рис. 13) со списком рисунков для выбранной учетной записи. Для дополнения списка рисунков используется два режима:

– *Поиск других рисунков* открывает содержимое папки *Мои рисунки* и предлагает сделать выбор нового рисунка;

– *Получение рисунка от камеры или со сканера* предлагает воспользоваться фотографиями, рисунками или другими картинками отсканированными или отснятыми видеокамерой.

Ссылка *Обучение*: *Использование собственного изображения* подсказывает об использовании собственных картинок в качестве идентификатора, сопровождающего выбранную учетную запись.

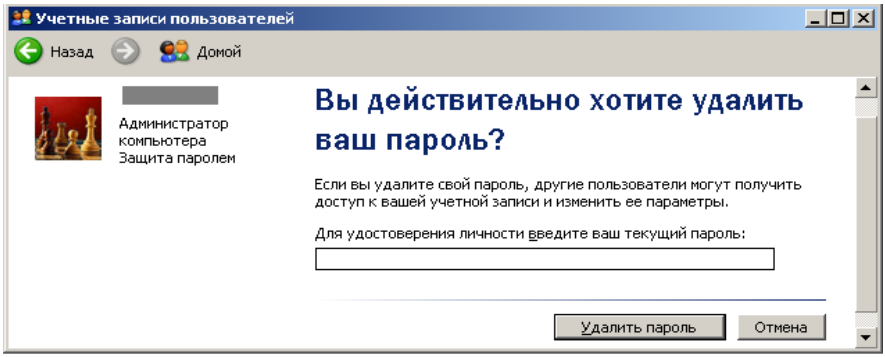


Рис.12. Окно подтверждения удаления пароля.

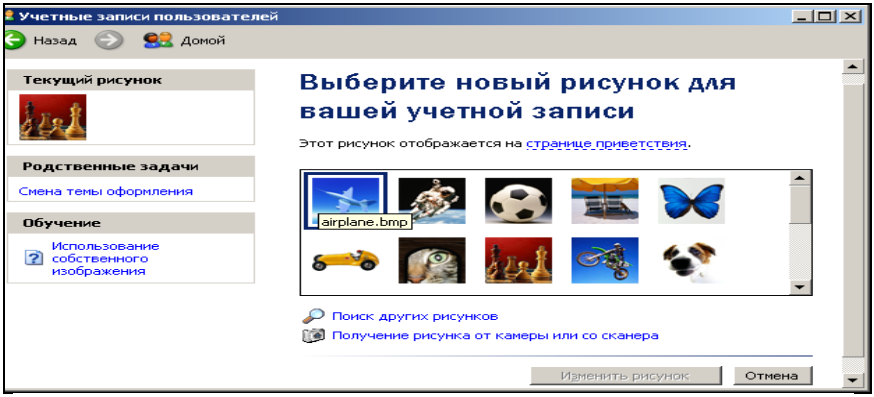


Рис.13. Окно изменения рисунка для выбранной учетной записи.

5. Режим *Использовать паспорт .NET*. занимается тем, что сопоставляет данной пользовательской записи определенный уникальный сертификат – паспорт. При активизации режима появляется окно *Мастера паспорта .Net* (рис. 14). Для продолжения работы следует воспользоваться подсказками мастера, выйти в Интернет и дальнейшая работа выполнится автоматически. Помощь при работе с данным режимом можно получить из раздела *Обучение*: *Использование паспорта .NET*.

6. В разделе *Родственные задачи* режим *Управление сетевыми паролями* активизирует окно *Сохранение имен пользователей и паролей*. В окне указываются личные данные, требуемые для подключения и регистрации в сети или на веб-узлах Интернета. Данные с помощью соответствующих кнопок можно добавлять, удалять изменять (кнопка *Свойства*).

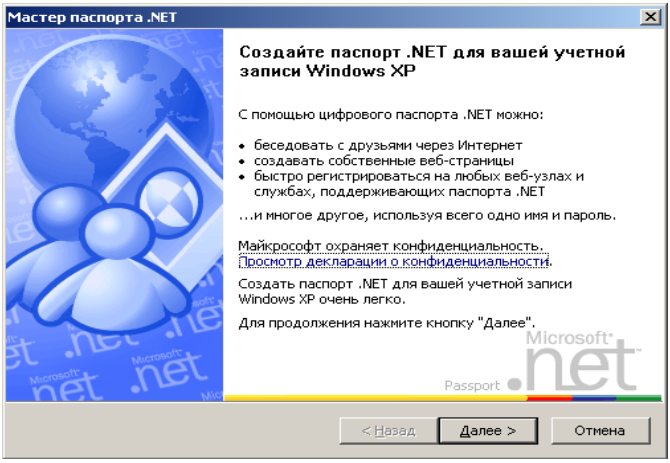


Рис.14. Окно Мастера паспорта *.Net.*

3) Восстановление забытого пользователем пароля.

В разделе *Родственные задачи* режим *Подсказка о пароле* активизирует окно *Мастер забытых паролей* (рис. 15). Мастер позволяет создать дискету «сброса паролей», которую можно использовать для создания нового пароля.

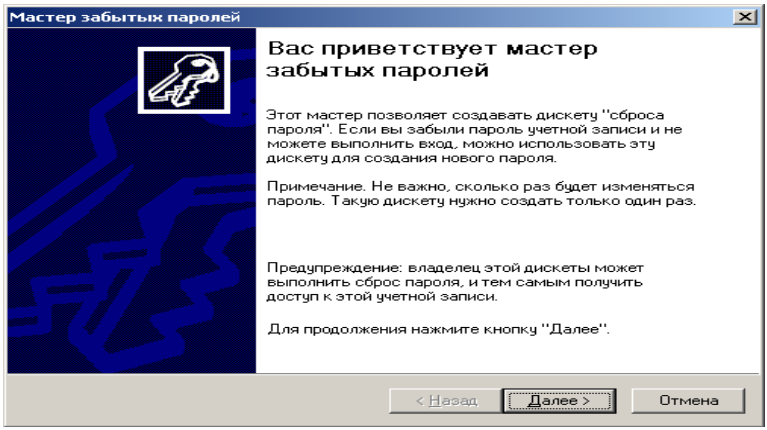


Рис.14. Окно Мастера забытых паролей.

Мастер забытых паролей предлагает начать операцию сброса пароля на дискету, для которой потребуется чистый и форматированный флоппи-диск, который следует вставить в дисковод A:.

Предупреждение: *выполнение данной функции нужно делать только один раз, вне зависимости от частоты смены пароля в системе.*

В процессе выполнения мастера будет создан диск, который позволит, в случае, если пароль будет забыт, создать новый пароль для системы и успешно в нее войти. Такая возможность предоставляется пользователям *Windows XP*, благодаря использованию в ней специальных криптографических алгоритмов, использующих пару ключей. Эти алгоритмы считаются наиболее устойчивыми к взломам. На последующих рисунках (15-16) представлено использование этого мастера.

На вопрос мастера на третьем шаге нужно корректно ввести текущий пароль к системе и дождаться завершения работы мастера.

Диск для дальнейшего использования следует спрятать в надежное и безопасное место, особенно если он сделан с правами администратора системы.

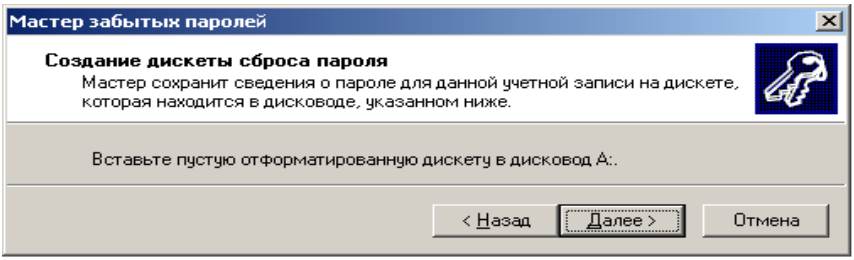


Рис.15. Второй шаг *Мастера забытых паролей*.

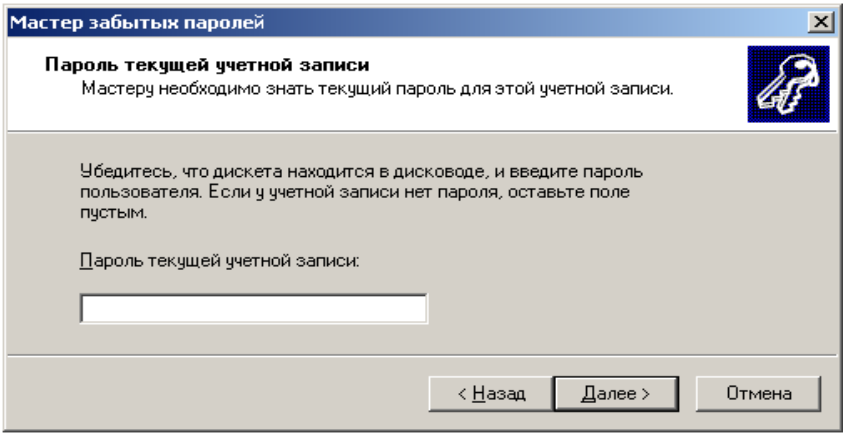


Рис.16. Третий шаг *Мастера забытых паролей.*

4) Выполнение действий над пользователями системы.

Программа *Управление компьютером* (*Computer Management*) позволяет при выборе пользователя производить ряд возможных действий над ними посредством команд контекстного меню (рис. 17). Команды позволяют задавать пароль пользователю, переименовывать и удалять пользователя. При удалении пользователь из системы удаляется, но все его данные, программы, почта, временные файлы Интернета и системные области данных, включая реестр и корзину, остаются неизменными.

Для окончательного удаления пользователя из системы следует:

- войти в каталог: *%SystemRoot%|Documents and Settings* ;
- найти папку с именем удаленной учетной записи;
- удалить или заархивировать папку.

Аналогично следует поступить с корзиной пользователя, в

качестве которой используется его идентификатор. Корзина находится в каталоге *RECYCLER*. Удаление пользователей используется по разным причинам, например, пользователь перешел в другой отдел компании или уволился. Переименование пользователей используется по разным причинам, например, пользователь перешел на другой компьютер или ему пришлось создать еще одну учетную запись. В этих случаях следует:

- создать новую учетную запись для нового пользователя;
- скопировать в нее все данные и файлы пользователя;
- логически удалить старую не нужную учетную запись;
- стереть все файлы старой учетной записи с жестко диска.

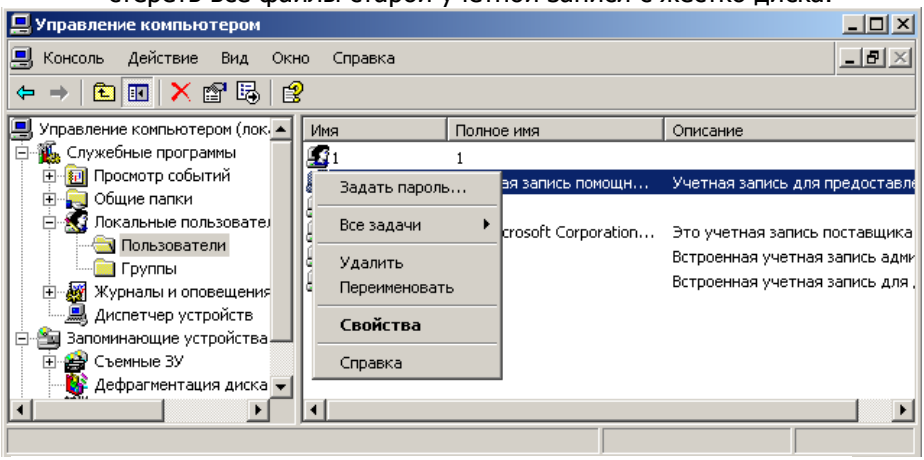


Рис.17. Окно программы *Управление компьютером* с контекстным меню.

Существует еще одна особенность переименования учетных записей, связанная с возможностью серьезной утраты информации. Например, работающим на компьютере пользователям пришлось обменяться пользовательскими учетными записями. Наиболее логичным решением, в этом случае, является взаимное изменение имен учетных записей. Однако если удалить одного пользователя, то можно удалить с жесткого диска совпадающий по имени с учетной записью каталог, который может принадлежать другой учетной записи. Итог: оба пользователя будут удалены. Поэтому здесь следует быть особенно внимательным.

5) Работа с пользовательскими группами.

В программе *Управление компьютером* после выбора раздела групп пользователей (рис. 2) можно выполнить ряд

возможных над ними действий (рис. 18).

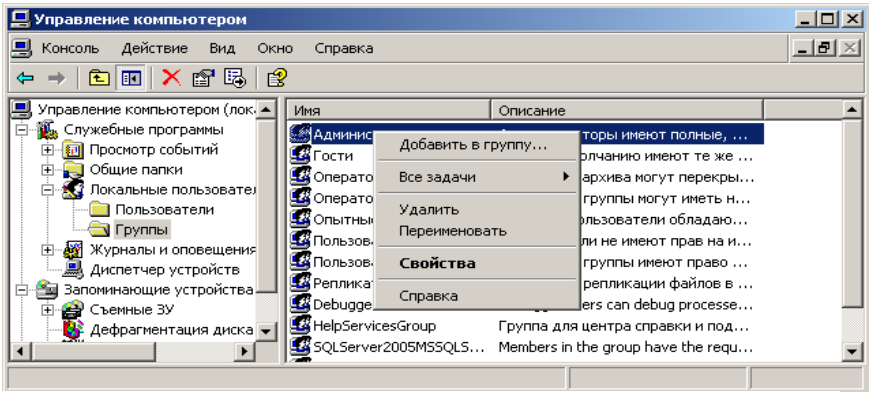


Рис.18. Окно программы *Управление компьютером*, раздел *Группы.*

Команда *Добавить в группу* позволяет добавить в группу определенных пользователей или даже их группы, процесс аналогичен представленному ранее (рис. 6 – 8).

Команда *Все задачи* содержит в себе тот же пункт меню: Добавить в группу.

Команды *Удалить* и *Переименовать* позволяют, соответственно, удалять и переименовывать группы пользователей, аналогично одному пользователю, но с одним исключением: после удаления группы пользователей нет необходимости удаления дополнительной информации, так как группа не имеет своего представления в пользовательских папках.

Команда *Свойства* показывает членов группы, позволяя добавить к ней другие группы и пользователей, как и с помощью команды *Добавить в группу*.

При щелчке правой кнопки мыши на пустом месте появится другое контекстное меню (рис. 18).

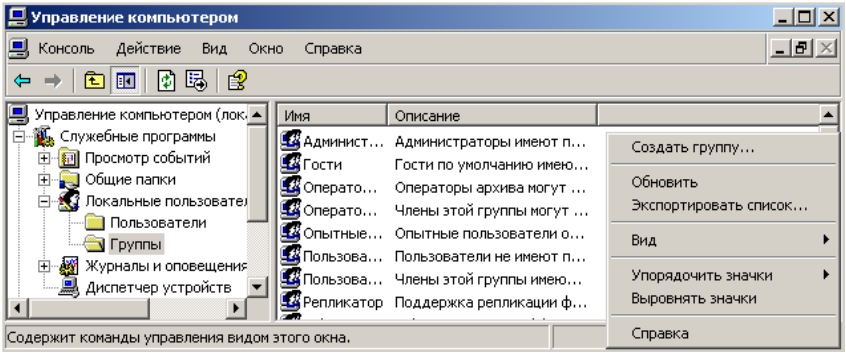


Рис.18. Окно программы *Управление компьютером*, раздел *Группы*, с контекстным меню, вызванным в свободной области окна.

Новой возможностью данного меню является команда *Создать группу*. После ее выбора на экране появится диалоговое окно создания новой группы пользователей (рис. 19).

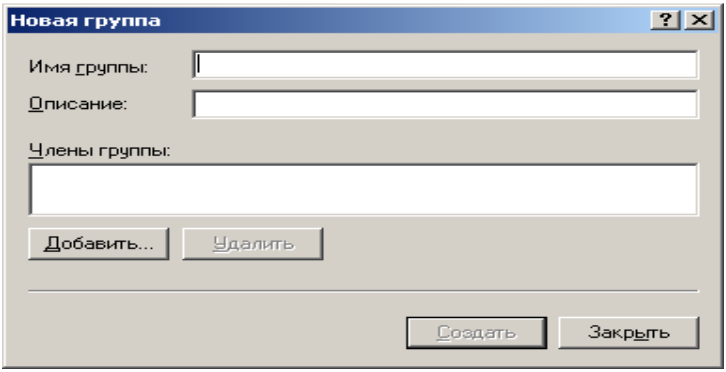


Рис.19. Диалоговое окно *Новая группа.*

В первом поле диалогового окна предлагается ввести имя создаваемой группы пользователей. В следующей строке – ее краткое описание. Рекомендуется создавать простое, наглядное и емкое описание группы, что значительно упростит администрирование системы при возрастающей нагрузке и числе пользователей.

В поле *Члены группы* с помощью кнопки *Добавить* можно поместить пользователей, которые будут входить в ее состав, затем нажать кнопку *Создать*.

6) Управление входом пользователей в систему.

Все введенные пользовательские учетные записи на экране «Приветствие» при входе в систему будут показаны. Для входа в систему под одним из них нужно его выбрать мышью и ввести пароль. После чего нажать клавишу *Enter* или стрелку рядом с паролем учетной записи и системой произведется вход в настройки выбранного пользователя и активизация его сеанса работы. Однако использование экрана «Приветствие» бывает удобно далеко не всегда, например, наличие большого количества пользователей или желание системного администратора скрыть их количество и имена, прописанных в системе.

Для того чтобы запретить экран «Приветствие», сделав вход в систему более безопасным и походящим на классический экран входа пользователей, в *Windows XP* необходимо под учетной записью, имеющей права администратора, войти в программу *Учетные записи пользователей* (рис. 9).

Рядом с каждой учетной записью отображается ассоциированная с ней картинка. Для изменения учетной записи выбранного пользователя следует выбрать в верхней части окна режим *Изменение входа пользователя в систему* (рис. 20).

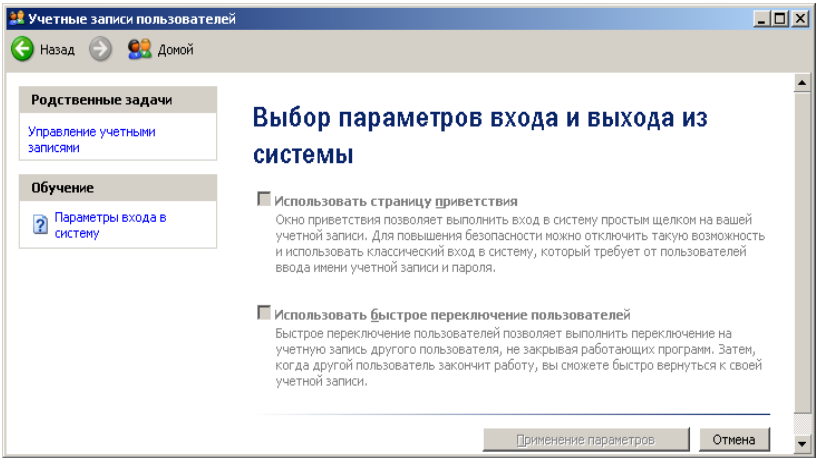


Рис.20. Окно *Выбор параметров входа и выхода из системы.*

Режим *Использовать страницу приветствия* – управляет использованием экрана «Приветствие» при входе в систему. Если

флажок в режиме установлен, то экран будет использован, в ином случае будет произведен классический вход в систему, как в Windows NT, которое предложит для входа в систему ввести имя учетной записи пользователя и ее пароль.

Режим *Использовать быстрое переключение пользователей* управляет переключением пользователей. Это связано с тем, что ОС *Windows NT* многозадачная и многопользовательская и в процессе ее работы можно переключаться между пользователями, которые работают в данной системе. При этом все настройки пользователей и их программы продолжат свое выполнение, даже если будет производиться переключение между учетными записями пользователей, работающих в данное время в системе. В случае если флажок не установлен, то переключение пользователей становится невозможным.

Переключение пользователей производится путем выбора: *Пуск|Выход из системы|Смена пользователя*. После выполнения команды появится экран «Приветствие» или классический вход *Windows NT* в зависимости от настройки системы.

2. Практическая часть.

1) Вопросы по разделу:

1) Что происходит при включении компьютера после загрузки операционной системы?

2) Что происходит при включении компьютера после загрузки операционной системы, если компьютер входит в состав домена с большим количеством пользователей?

3) Какой вид должен иметь правильно составленный пароль?

4) На чем базируется система безопасности в операционной системе *Windows XP*?

5) Перечислите основные группы пользователей в операционной системе *Windows XP*?

6) Что нужно сделать, если требуется, чтобы у пользователя был набор прав, состоящий из прав по нескольким группам?

7) Какую программу нужно запустить для доступа к программе управления пользователями?

8) Для выполнения административных действий: смены пароля, изменения свойств пользователя и пр. необходимы права администратора системы.

9) Какие правила используются в политике безопасности системы для целей безопасности сложных, многопользовательских систем, в которых хранятся большие объемы важ-

ной информации?

10) Перечислить случаи отказа от правил, используемых в политике безопасности системы для целей безопасности сложных, многопользовательских систем?

11) Перечислите причины отключения (блокирования) учетной записи.

12) Как определить к каким группам относится пользователь?

13) Как произвести добавление новых групп пользователю?

14) Как произвести добавление пользователей?

15) Как произвести вывод на экран доступных имен всех групп пользователей?

16) Как произвести вывод на экран списка учетных записей пользователя с указанием типа учетной записи?

17) Как произвести настройку учетной записи пользователя?

18) Как произвести изменение имени пользователя?

19) Как произвести изменение пароля пользователя?

20) Как произвести изменение рисунка учетной записи пользователя?

21) Что означает режим «Использование паспорта *.NET*?

22) Какие задачи решаются в разделе *Родственные задачи* режима *Управление сетевыми паролями*?

23) Как восстановить забытый пользователем пароль?

24) Какое предупреждение *Мастера забытых паролей* необходимо знать при восстановлении забытого пароля?

25) Какие действия производит над пользователями программа *Computer Management*?

26) Какие действия нужно произвести для окончательного удаления пользователя из системы?

27) Для каких целей используется переименование учетной записи пользователя?

28) Перечислите возможные действия при работе с пользовательскими группами в программе *Computer Management*?

29) Каким образом производится управление входом пользователя в систему?

30) Как произвести переключение пользователя во время сеанса работы?

2) Порядок отчетности и форма контроля выполнения работы.

Контроль выполнения задания производится по окон-

чании занятия и на консультациях в форме защиты выполненной работы, предоставленной в электронном и в бумажном виде в форме «Отчет по лабораторной работе …».

3. Материально-техническое обеспечение.

Специализированная мебель и технические средства для представления учебной информации, включая проекционное оборудование; компьютерный класс с компьютерами AMD 2400 – 12 шт., оснащенными операционной системой Windows XP и пакетом Microsoft Office.

ЛАБОРАТОРНАЯ РАБОТА 5
ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ОС ОТ АТАК ПО КОМПЬЮТЕРНЫМ СЕТЯМ

Цель занятия – приобретение обучаемыми необходимого объёма знаний и практических навыков в обеспечении защиты ОС от атак по компьютерным сетям.

Время – 4 часа.

Учебные вопросы:

1. **Теоретическая часть:**
1) Сетевая защита и брандмауэр.
2) Настройка брандмауэра.
3) Дополнительные параметры брандмауэра.
4) Удаленные сеансы пользователей.
5) Удаленные пользователи.
2. **Практическая часть:**
1) Вопросы по разделу.
2) Задание.
3) Порядок отчетности и форма контроля выполнения работы.
3. **Материально-техническое обеспечение.**

1.Теоретическая часть.

1) Сетевая защита и брандмауэр.

Как бы ни была безопасна система, всегда есть риск, что кто-то извне по компьютерной сети будет пытаться ее взломать. Единственным решением, которое позволяет в большинстве случаев решить эту проблему является своевременное обновление версий программного обеспечения. Но и в этом случае можно найти какую-то особенность в функционировании программного обеспечения и использовать ее для взлома системы. Например: использование пользователем демонстрационной версии программного продукта или используемая версия программного обеспечения больше не поддерживается разработчиком. В этих ситуациях, если не использовать каких-либо дополнительных мер, пользователь может оказаться беззащитным от атак извне.

Понимая опасность таких ситуаций, многие исследовательские центры и частные компании занимались решением этой проблемы. Разработчики рассудили: раз сетевой взломщик не должен взломать компьютер пользователя, то он просто не должен полу-

чить к нему доступ, т.е. необходимо гарантированно закрыть доступ к компьютеру несанкционированным пользователям. Разработанный метод защиты похож на стену, окружающую со всех сторон компьютер, поэтому он и получил название *Firewall* (пожарная стена), иначе сетевой экран или фильтр, который отфильтровывает запросы сетевых пользователей к системе. В официальной русской версии *Windows XP* он переведен как *брандмауэр*.

Брандмауэр – это специальное программное обеспечение, поставляемое вместе с операционной системой или устанавливаемое пользователем, которое позволяет запретить любой доступ нежелательных пользователей из сети к системе. *Брандмауэр* помогает повысить безопасность компьютера. Он ограничивает информацию, поступающую на компьютер с других компьютеров, позволяя лучше контролировать данные на компьютере и обеспечивая линию обороны компьютера от людей или программ (включая вирусы и «черви»), которые несанкционированно пытаются подключиться к компьютеру. *Брандмауэр* – это пограничный пост, на котором проверяется информация (трафик), приходящая из Интернета или по локальной сети. В ходе проверки *брандмауэр* отклоняет или пропускает информацию на компьютер в соответствии с установленными параметрами.

В состав *Windows XP* входит встроенная версия *брандмауэра* (в пакет обновления *SP2* для *Microsoft Windows XP брандмауэр* включен по умолчанию), основной алгоритм работы которого обеспечивает защиту от несанкционированных пользователей. Практически невозможно найти уязвимость, которая бы обеспечивала проникновение взломщика на защищенную сетевым экраном систему. Функции, выполняемые *брандмауэром*:

- блокировка доступа на компьютер вирусам и «червям»;
- запрос пользователя о выборе блокировки или разрешения для определенных запросов на подключение;
- ведение журнала безопасности и по желанию пользователя запись разрешенных и заблокированных попыток подключения к компьютеру, журнал может оказаться полезным для диагностики неполадок.

Идея атак взломщиков основывается на работе низкоуровневых алгоритмов обработки сетевых запросов, в некоторых старых версиях программного обеспечения их можно было пытаться использовать для возможного проникновения через сетевой экран. В современных версиях *брандмауэра*, если грамотно его настроить, можно избежать любых атак взломщиков.

Когда на компьютер по- ступает непредусмотренный

запрос (кто-то пытается подключиться из Интернета или по локальной сети), *брандмауэр* блокирует подключение. Если на компьютере используются программы передачи мгновенных сообщений или сетевые игры, которым требуется принимать информацию из Интернета или локальной сети, *брандмауэр* запрашивает пользователя о блокировании или разрешении подключения. Если пользователь разрешает подключение, *брандмауэр* создает исключение, чтобы в будущем не тревожить пользователя запросами по поводу поступления информации для этой программы. Предусмотрена так же возможность отключения *брандмауэра* для отдельных подключений к Интернету или локальной сети, но это повышает вероятность нарушения безопасности компьютера.

2) Настройка брандмауэра.

Если *брандмауэр* подключен, то для его настройки следует:

– войти в систему под учетной записью системного администратора;

– открыть папку, в которой находятся сетевые подключения:

Пуск|*Настройка*|*Панель управления*|*Сетевые подключения* (рис. 1);

– выбрать строку, например, *Подключение по локальной сети* (рис.2);

– во вкладке *Общие* сделать щелчок по кнопке *Свойства* (рис. 2);

– появится дополнительное окно *Свойства*, в котором выбрать вкладку *Дополнительно* (рис. 2);

– во вкладке *Дополнительно* нажать кнопку *Параметры* (рис. 3);

– появится окно программы *Брандмауэр Windows* (рис. 3).

Аналогичное окно появится при выборе программы *Брандмауэр Windows* из списка программ в *Панели управления*:

Пуск – Настройки – Панель управления – Брандмауэр Windows (рис. 4)

Для получения подробной информации в окне программы *Брандмауэр Windows* следует сделать щелчок по ссылке *Подробнее о Брандмауэре Windows*. Появится окно *Центр справки и поддержки,* в котором будет приведена вся информация о назначении и использовании *брандмауэра*.

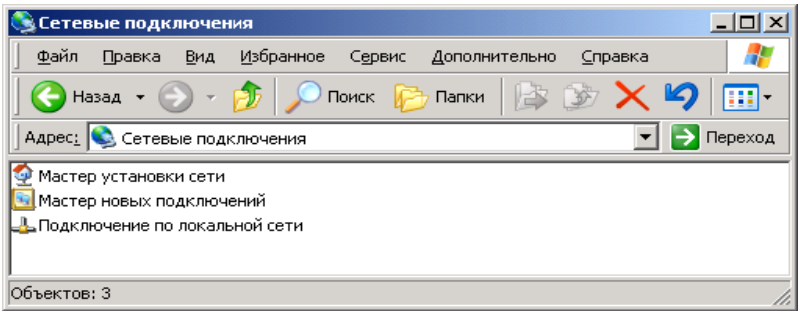


Рис. 1. Окно программы *Сетевые подключения.*

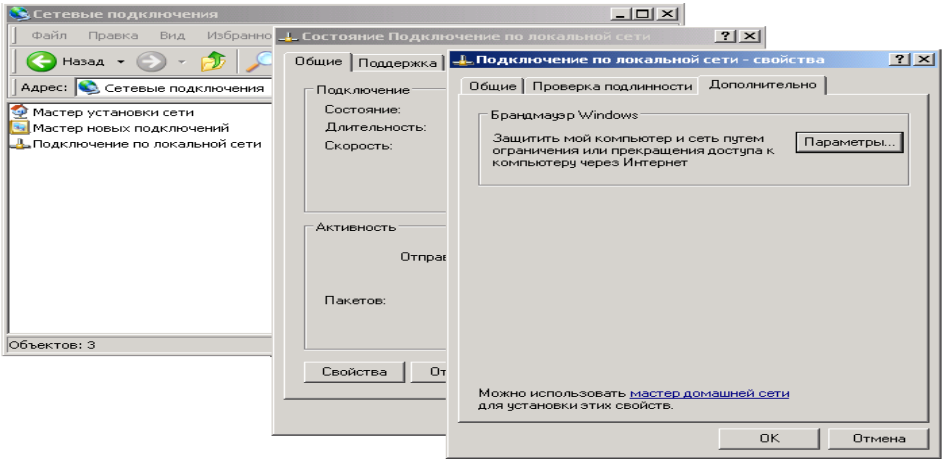


Рис. 2. Окна программы *Подключение по локальной сети.*

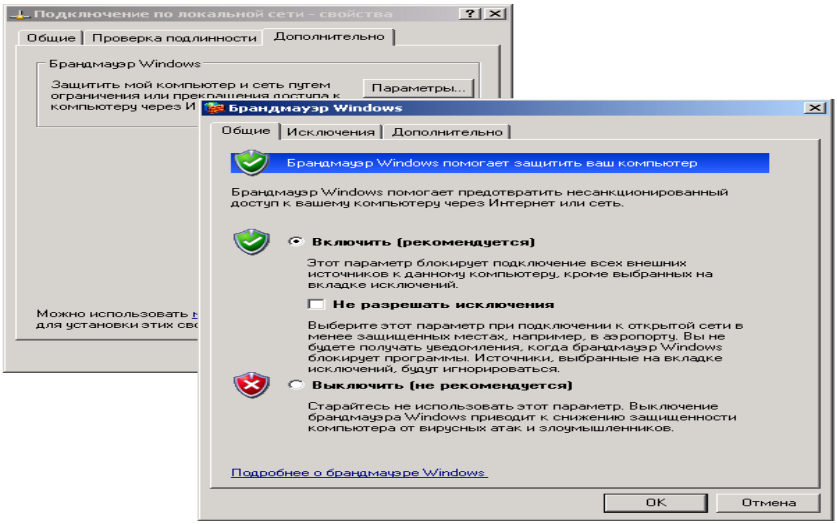


Рис. 3. Окно вкладки *Дополнительно* и окно программы *Брандмауэр.*

Закладка *Общие* окна настроек *брандмауэра* является главной, по умолчанию *брандмауэр* включен (рис. 4). Закладка содержит ряд опций.

Опция *Включить (рекомендуется)* включает *брандмауэр*. Опция *Не разрешать исключения* может использоваться только вместе с опцией *Включить (рекомендуется)*. Она позволяет повысить уровень безопасности системы в случае ее использования в публичных местах, таких как аэропорты, кафе, кинотеатры и пр., оборудованные доступом в Интернет. Уровень безопасности будет увеличен за счет запрета работы программ, к которым разрешается получать доступ из сети, прегражденной сетевым фильтром. Сообщения об отказе доступа пользователям к таким приложениям система генерировать не будет.

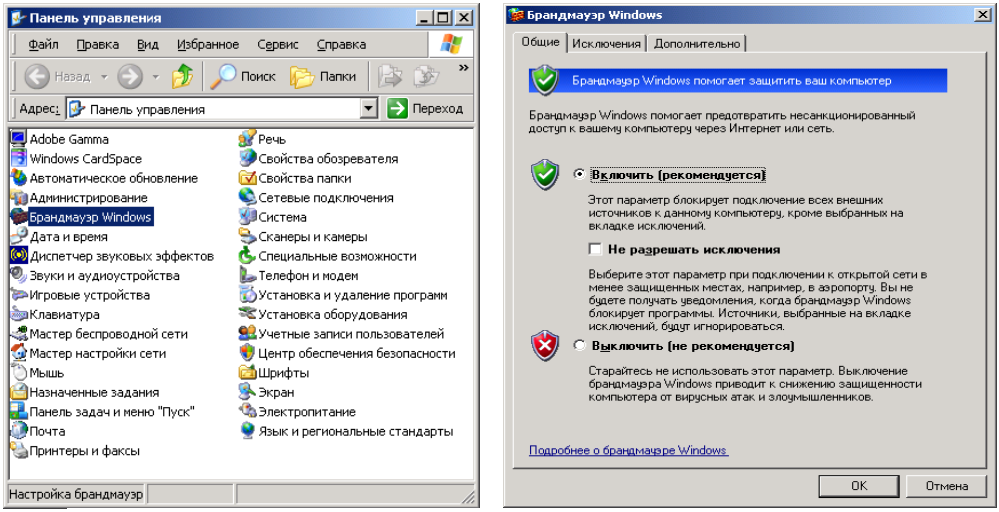


Рис. 4. Окно *Панель управления* и окно программы *Брандмауэр Windows.*

Опция *Выключить (не рекомендуется)* полностью выключает *брандмауэр*. В этом случае система оказывается совершенно незащищенной от атак извне. Единственный случай, когда это может быть оправдано, это когда нужно кратковременно протестировать работу какого-либо приложения, которое не хочет работать с активным сетевым экраном.

Брандмауэр Windows блокирует входящие сетевые подключения, исключая программы и службы, выбранные пользователем. Добавление исключений улучшает работу некоторых программ, но повышает риск безопасности. Закладка *Исключения* позволяет указать программы и сервисы, к которым могут быть осуществлены соединения пользователей со стороны Интернета (рис. 5). Фактически, для этих программных продуктов сетевой фильтр работать не будет, пропуская все запросы к ним через себя.

Закладка *Исключения* представляет собой список программ и сервисов, к которым можно разрешить доступ со стороны Интернета, посредством установки рядом с ними флажка. Опция *Отображать уведомление, когда брандмауэр блокирует программу*, в случае ее активизации, заставляет *Windows* выдавать сообщение о попытке доступа из сети. По умолчанию опция включена, т.к. она помогает лучше понять процессы, происходящие внутри системы. Если на закладке *Общие* установлена опция *Не разре-*

шать исключения сообщение выдаваться не будет.

Для удаления программы или сервиса из списка разрешенных объектов к обращению из сети Интернет следует выделить объект из списка окна и нажать кнопку *Удалить*. Данную операцию стоит проводить с программами или сервисами, которые больше не должны быть доступны для пользователей из Интернета.

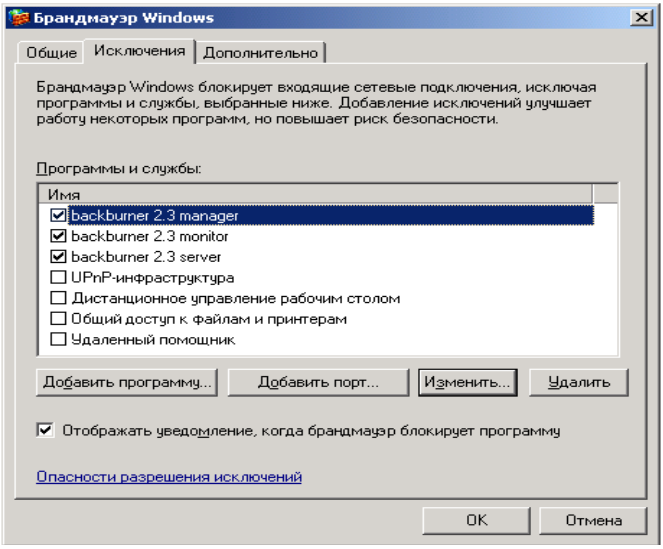


Рис. 5. Закладка *Исключения.*

Для редактирования определенного объекта из списка программ и сервисов, разрешенных к обращению из Интернета следует выделить редактируемый объект и нажать кнопку *Изменить*, появится окно *Изменение программы* (рис. 6). Диалоговое окно содержит имя редактируемой программы и путь к ее исполняемому файлу. Кнопка *Изменить область* позволяет указать, каким именно сетевым компьютерам будет доступна выбранная программа или сервис. В данном окне можно указать три режима, в соответствии с которыми будет осуществляться доступ из сети к программе или сервису, расположенному в системе.

Режим *Любой компьютер (включая из Интернета)* (рис. 7) указывает, что доступ к данной программе будет возможен со всех сетевых компьютеров, включая расположенные в Интернете. Не рекомендуется выбирать режим без особой необходимости, т.к. будет предоставлена воз- можность любому пользовате-

лю извне пробовать подключаться к определенному му обеспечению. А в случае наличия в нем уязвимостей, ватель может получить доступ к системе или нарушить ее нормальное функционирование.

Режим *Только локальная сеть (подсеть)* (рис. 7) позволяет сделать возможным доступ к программному обеспечению только из сети, в которой находится система, что значительно снижает риск взлома даже при наличии уязвимостей в программном обеспечении. Если нужно разрешить доступ только с некоторых сетевых компьютеров, рекомендуется использовать третью опциею.

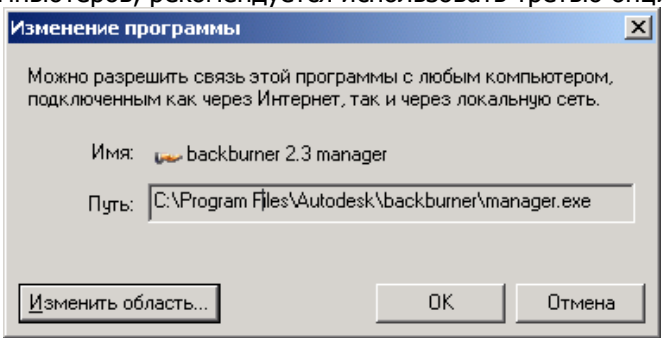


Рис. 6. Диалоговое окно *Изменение программы.*

Режим *Особый список* позволяет указать в нижележащем поле ввода список *IP-адресов* (сетевой адрес вида *a.b.c.d*) компьютеров, которым будет разрешен доступ к выбранному сервису или программе. Это наиболее удобный и безопасный способ осуществления разрешения на доступ из сети, так как в этом случае всегда можно контролировать компьютеры, которые его получают, и быть уверенными в том, что система надежно защищена от атак. Рекомендуется использовать данный режим (если позволяет ситуация), как самый оптимальный из всех. Кнопка *ОК* сохраняет внесенные изменения в окне, кнопка *Отмена* – их отменяет.

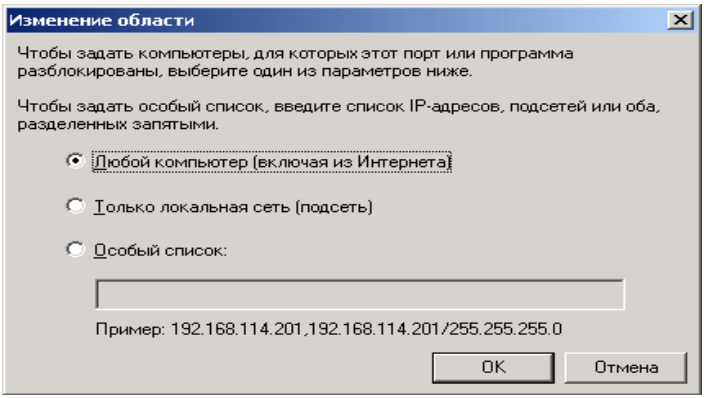


Рис. 7. Диалоговое окно *Изменение области.*

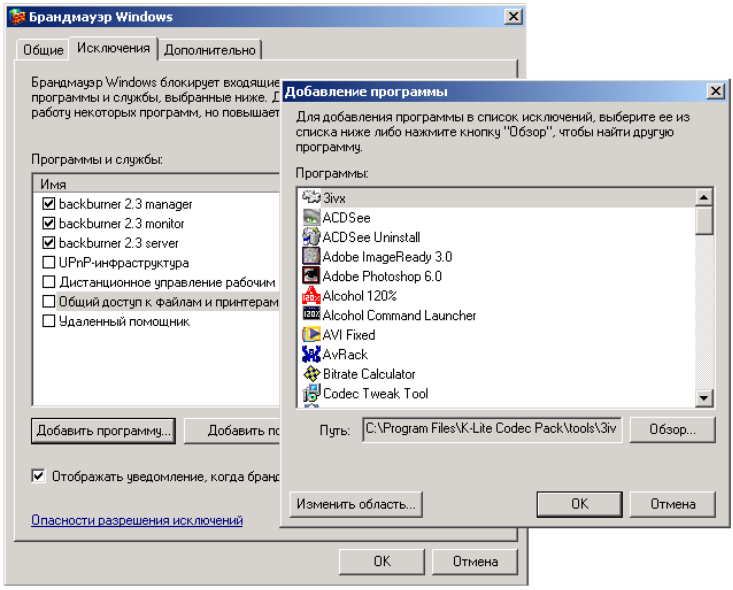


Рис. 8. Диалоговое окно *Добавление программы.*

В закладке *Исключения* кнопка *Добавить программу* позволяет добавить программы, к которым следует разрешить доступ со стороны сети (рис. 8). Из предлагаемого списка требуется выбрать нужное приложение или воспользоваться кнопкой *Обзор* и указать его исполняемый файл в файловой системе компьютера. С помощью кнопки *Изменить область* можно указать с каких сетевых компьютеров будет возможен доступ к данному приложе-

нию. Кнопка *ОК* сохраняет внесенные изменения, закрывая окно добавления программы, кнопка *Отмена* приводит к отмене всех дополнений сделанных в окне.

В закладке *Исключения* нажатие кнопки *Добавить порт* выводит диалоговое окно *Добавление порта* (рис. 9). Номер порта представляет собой канал, выраженный целочисленным десятичным числом, по которому приложения могут обмениваться информацией. Если используемому приложению требуется открыть определенный канал, то в поле *Имя* следует ввести имя приложения, в поле *Номер порта* – номер порта, сообщенный приложением. Флажковые опции *TCP* и *UDP* позволяют указать, какой порт требуется приложению. Если необходимо создать два порта с одинаковыми номерами, но разными типами (*TCP* или *UDP*), то следует дважды воспользоваться функцией дополнения порта (кнопкой *Добавить порт*) (рис. 9), и с помощью кнопки *Изменить область* указать с каких сетевых компьютеров будет возможен доступ к данному порту. Кнопка *ОК* сохраняет внесенные изменения, кнопка *Отмена* приводит к отмене всех дополнений сделанных в окне.

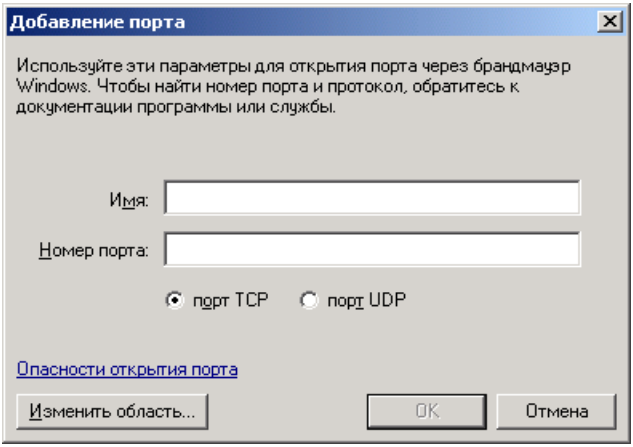


Рис. 9. Диалоговое окно *Добавление порта.*

3) Дополнительные параметры брандмауэра.

В окне настроек брандмауэра в закладке *Дополнительно* находятся некоторые важные настройки (рис. 10).

Первая группа элементов управления *Параметры сетевого подключения* позволяют избирательно использовать *брандмауэр* для сетевых интерфейсов системы. Сетевой фильтр включен только для интерфейсов, отмеченных флажками в списке *Службы*

(рис. 10). Кнопка *Параметры* вызывает окно для настройки доступа сетевых пользователей к *сетевым сервисам* для выбранного сетевого соединения. *Сетевыми сервисами* называют программное обеспечение, запросы на обработку к которому поступают по сети. В этом случае компьютеры, от которых поступают запросы, называются *клиентами*, а компьютеры, которые их обрабатывают – *серверами*.

По умолчанию в окне представлено несколько наиболее часто используемых в Интернете сервисов. В случае их использования можно разрешить к ним доступ сетевых пользователей. Например, если используется в системе *FTP-* или *Web-сервер*, то можно разрешить к ним доступ пользователей из сети. Для этого необходимо установить флажки в режимах, соответственно, *с FTP-сервер* и *Веб-сервер* (*HTTP*) (рис. 10).

После установки флажка в любом из пунктов появится диалоговое окно, в котором система поинтересуется, на каком компьютере установлен сервис, к которому нужно разрешить доступ. По умолчанию предлагается адрес системы, на которой осуществляется настройка *брандмауэра* (рис. 11).

В поле ввода *Имя или IP-адрес компьютера вашей сети, на котором располагается эта служба (например, 192.168.0.12)* нужно ввести адрес компьютера, на котором расположен сервис (если он отличается от адреса системы с настраиваемым *брандмауэром*). Нажатие кнопки *ОК* приводит к закрытию окна *Параметры службы*, а в окне *Дополнительные параметры* (рис. 10) рядом с соответствующим пунктом появляется флажок. Кнопки *Добавить* и *Изменить* в окне *Дополнительные параметры* (рис. 10) приводят, соответственно к добавлению или редактированию существующего сервиса (рис. 11).

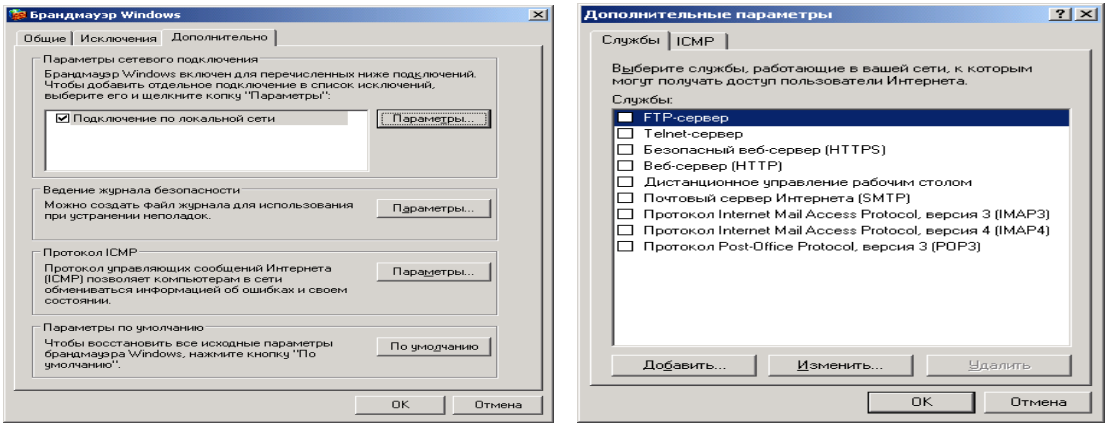


Рис. 10. Закладка *Дополнительно* и окно выбора дополнительных параметров сетевого подключения.

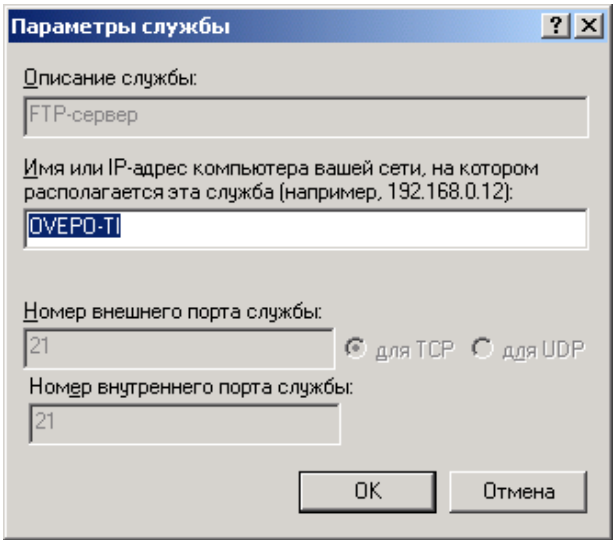


Рис. 11. Установка адреса системы, на которой расположен сервис, доступ, к которому открывается для сетевых пользователей.

Закладка *ICMP* окна *Дополнительные параметры* позволяет установить доступность сетевых сервисов, выполняющих служебные функции (рис. 12). *ICMP* (*Internet Control and Message Protocol*) означает отношение приведенных в окне *Дополнительные параметры – закладка ICMP* сервисов к протоколу обмена

контрольной информацией в Интернете. Данный протокол предназначен для технических целей и поддерживает корректную работу компьютерной сети, а также может использоваться при поиске неисправности, неизбежно возникающих в сложных сетевых вычислительных структурах. Он реализован с помощью ряда программных сервисов, которые перечислены в списке данного окна.

Вышеперечисленные сервисы предназначены для решения только технических задач. Но существует, как минимум, два пути нарушения нормальной работы системы или причинения ей значительного вреда, если указанные сервисы не будут установлены.

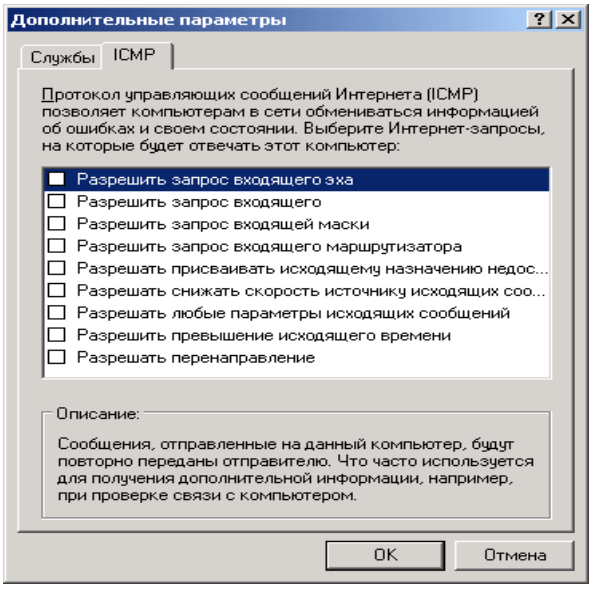


Рис. 12. Закладка *ICMP.*

Во-первых, возможен запрос взломщиков со стороны сети на выполнение системой различных действий для достижения определенных технических целей. Например, они могут послать системе запрос о ее существовании на определенный сетевой адрес. Если система находится по указанному адресу и функционирует нормально, то она может ответить на запрос. Взломщики могут послать множество таких запросов. Система будет отвечать на них, в результате чего ее производительность для полезных задач резко упадет, т.о. достигается атака *Отказ в обслуживании* (*DoS, Denied of Service*).

Также существуют мето- ды посылки специфических

просов, которые будут вынуждать ОС расточительно использовать свои системные ресурсы, вследствие чего наступит момент, когда система перестанет функционировать и ее придется перезагружать.

Во-вторых, возможна атака, целью которой является получение контроля над системой. Она может иметь самые различные алгоритмы. Наиболее вероятным сценарием взлома является посылка специфического запроса системе, который не может быть корректно обработан и вызовет запуск определенной программы, содержащейся в нем (запросе). Эта программа может что-нибудь уничтожить в системе или открыть к ней доступ из Интернета для взломщиков.

Вышеприведенные ситуации говорят о том, что нужно очень осторожно относиться ко всей информации, приходящей из сети, даже если она содержится в служебных запросах. Поэтому все служебные сервисы *по умолчанию* заблокированы сетевым экраном.

Второй раздел элемента управления *Ведение журнала безопасности* вкладки *Дополнительно* (рис. 12) позволяет задавать настройки, позволяющие отслеживать и сохранять в файле состояние сетевого экрана. При нажатии кнопки *Параметры* появится окно настроек протоколирования работы *брандмауэра* (рис. 13).

Режим *Записывать пропущенные пакеты* в случае установки флажка позволяет системе сохранять в файле *C:|WINDOWS|pfirewall.log* все пакеты, отклоненные системой, что необходимо для просмотра возможных атак из сети или запрещенных адресов.

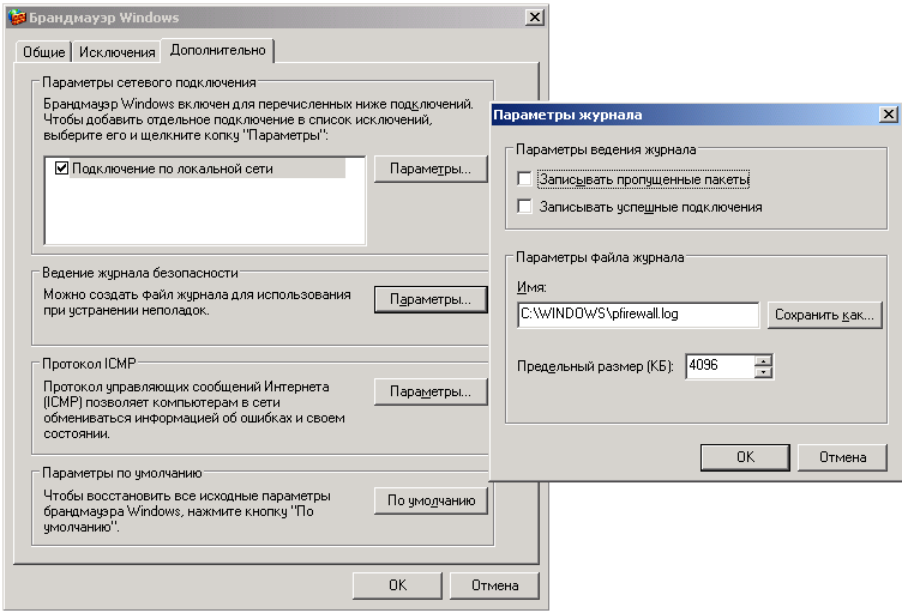


Рис. 13. Окно настроек протоколирования работы сетевого экрана.

Режим *Записывать успешные подключения* в случае установки флажка, позволяет производить запись всех удачных соединений, произведенных с системой.

В разделе *Параметры файла журнала* находятся опции, в которых указывается имя файла для протоколирования действий *брандмауэра* и его максимальный размер. При указании пути и имени этого файла в поле ввода *Имя* следует учесть, чтобы данный файл не был доступен простым пользователям, которые могут использовать его по своему усмотрению. Поле *Предельный размер (КБ)* позволяет указать максимальный размер этого файла в килобайтах, по умолчанию установлен размер четыре мегабайта. Нажатие кнопки *ОК* сохраняет внесенные изменения и приводит к закрытию окна.

Третий раздел элемента управления *Протокол ICMP* (рис. 13) задает настройки, позволяющие отслеживать обработку системой *ICMP-запросов* сети. При нажатии кнопки *Параметры* появится диалоговое окно *Параметры ICMP*. Рекомендуется разрешать работу для сетевых пользователей только необходимых сервисов. По умолчанию разработчиками системы заданы настройки, подходящие для большинства пользователей.

Для восстановления принятых по умолчанию параметров *брандмауэра* предлагается нажать кнопку *По умолчанию* (рис. 13).

4) Удаленные сеансы пользователей.

Пользователям, у которых возникают вопросы по работе с системой, *Windows XP* предлагает помощь в виде развитой системы файлов помощи и в виде интерактивной помощи, одним из видов которой является помощь пользователей друг другу. Специальный механизм *Удаленные сеансы* позволяет пользователям помогать друг другу: *Пуск|Программы|Удаленный помощник* (рис. 14).

Настройка входа в систему удаленных пользователей: войти в систему под учетной записью администратора; в *Панели управления* выбрать программу *Система*: *Пуск|Настройка|Панель управления|Система* (рис. 15) в появившемся окне *Свойства системы* выбрать закладку *Удаленные сеансы* (рис. 16).

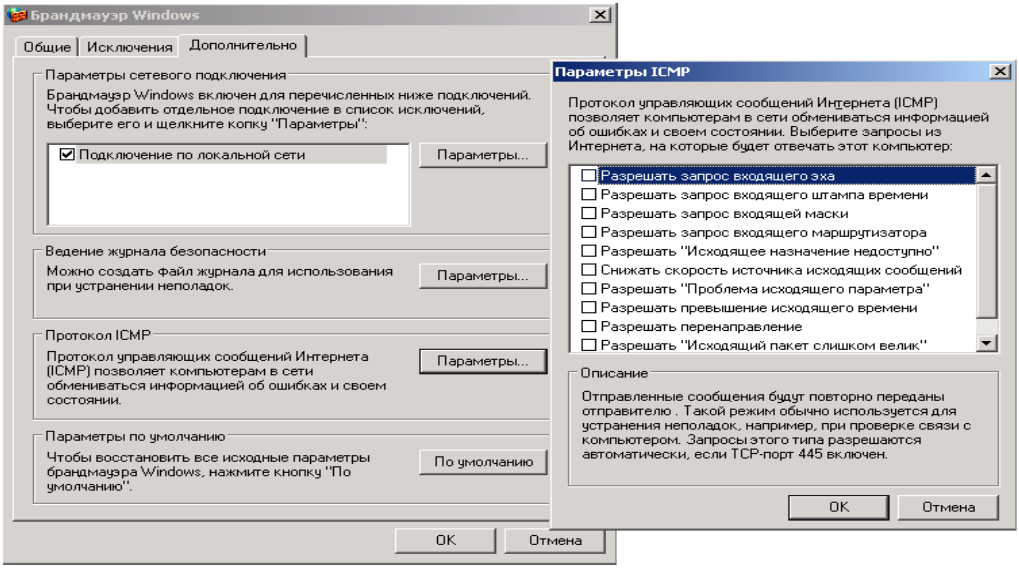


Рис. 13. Окно настроек *Протокола ICMP.*

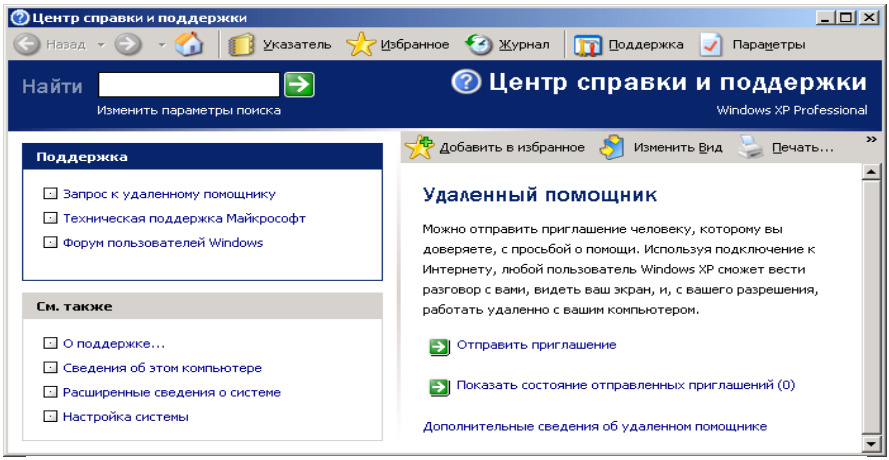


Рис. 14. Окно программы *Удаленный помощник.*

Для дезактивации механизма удаленной помощи нужно убрать флажок в режиме *Разрешить отправку приглашений удаленному помощнику*, для использования механизма удаленной помощи нужно поставить флажок в данном режиме и нажать кнопку *Дополнительно* (рис. 16). Для осуществления полноценной процедуры поддержки пользователем (к которому нужно обратиться за помощью), следует установить флажок в режиме *Разрешить удаленное управление этим компьютером*. Следует осторожно относиться к данному режиму, т.к. он дает возможность выбранному пользователю управлять компьютером удаленно, поэтому, если намерения пользователя не ясны, то лучше этого не делать.

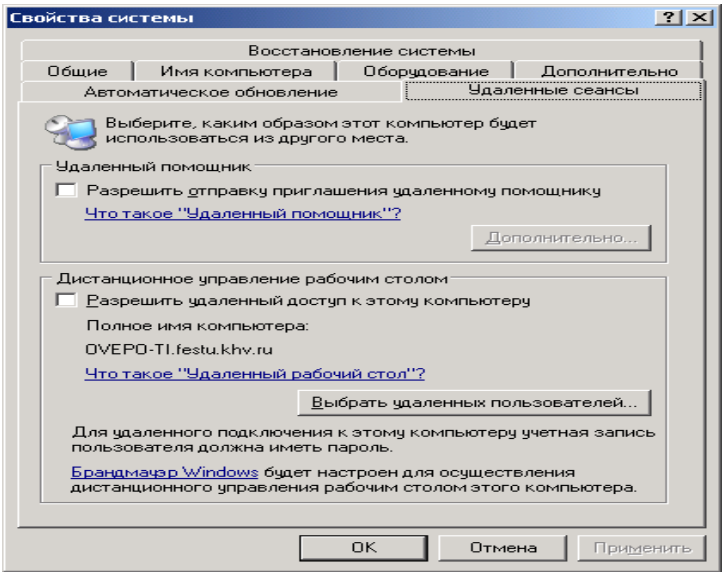


Рис. 15. Закладка *Удаленные сеансы* программы *Система.*

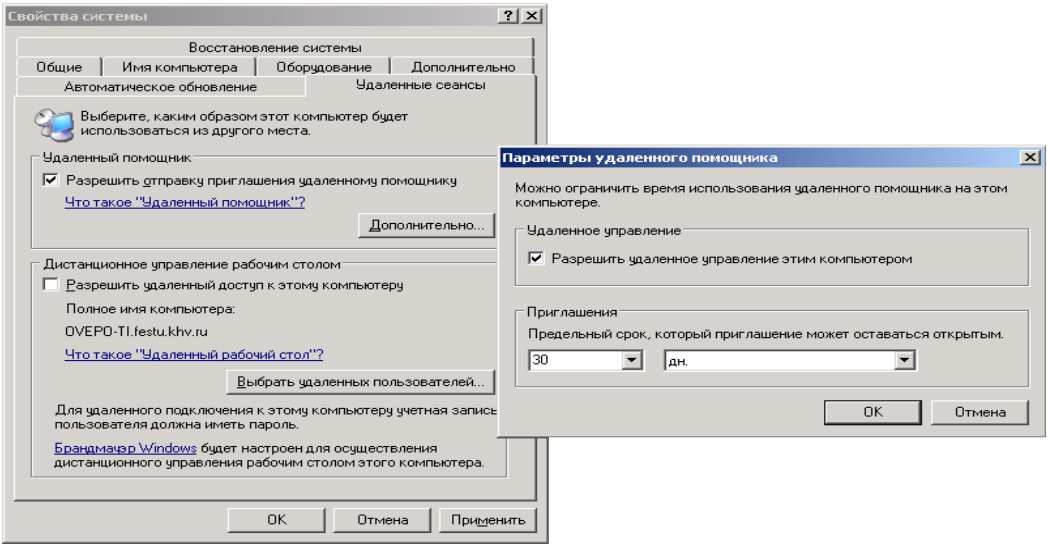


Рис. 16. Окно настройки удаленной помощи.

Последний режим определяет интервал времени, в течение которого запрос о помощи остается в силе для других пользова-

телей. Нажатие кнопки *ОК* приводит к активизации выбранных настроек.

В целях безопасности рекомендуется запрещать механизм удаленной помощи, лучше обратиться в техническую поддержку *Microsoft*.

5) Удаленные пользователи.

Если необходимо временно разрешить удаленный вход в систему сетевых пользователей с получением полного доступа следует:

– войти в систему под учетной записью администратора;

– в *Панели управления* выбрать программу *Система*: *Пуск*|*Настройка*|*Панель управления*|*Система* (рис. 15);

– в появившемся окне *Свойства системы* выбрать закладку *Удаленные сеансы* (рис. 16);

– в поле *Дистанционной управление рабочим столом* поставить флажок в режиме *Разрешить удаленный доступ к этому компьютеру* (рис. 17);

– для уточнения пользователей, которым разрешен доступ сделать щелчок по кнопке *Выбрать удаленных пользователей* (рис. 17);

– появится диалоговое окно *Пользователи удаленного рабочего стола,* в котором с помощью кнопок *Добавить* и *Удалить* можно, соответственно, добавлять и удалять пользователей;

– для добавления пользователей сделать щелчок по кнопке *Добавить*;

– в появившемся диалоговом окне *Выбор: Пользователи* сделать щелчок по кнопке *Дополнительно* (рис. 18);

– появится дополнительное окно со списком пользователей, которым разрешен доступ;

– щелчком выбрать имя пользователя, после чего окно закроется;

– для сохранения установленных настроек нажать кнопку *ОК*, для отмены – кнопку *Отмена*;

– после возврата к окну *Пользователи удаленного доступа* нажатие кнопки *ОК* приведет к тому, что все пользователи, отображенные в списке, получат возможность удаленно входить в систему и пользоваться ее интерфейсом, приложениями и документами, соответствующими учетной записи, под которой они входят в систему; все они должны быть локально прописанными в системе.

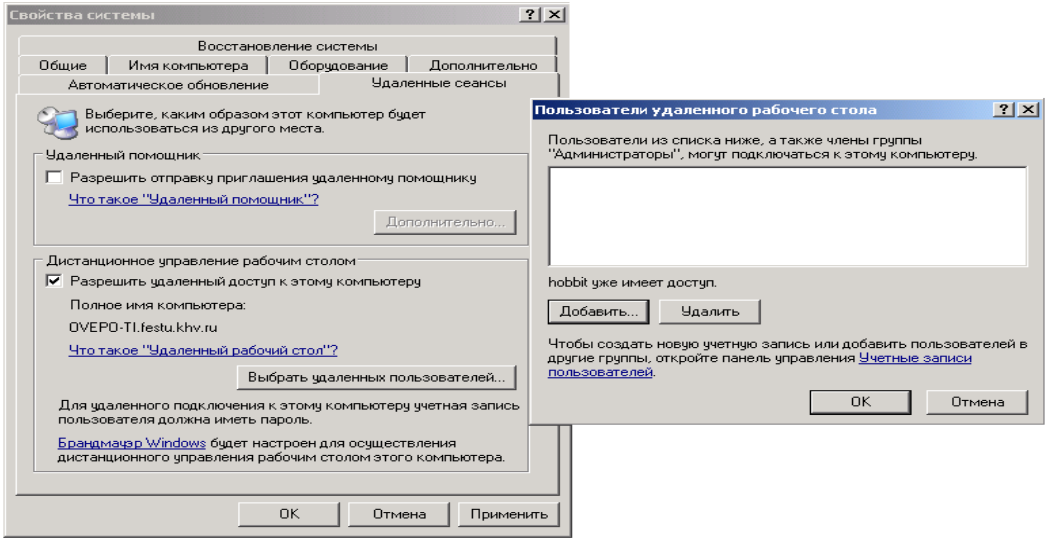


Рис. 17. Окно определения пользователей, имеющих права работать удаленно.

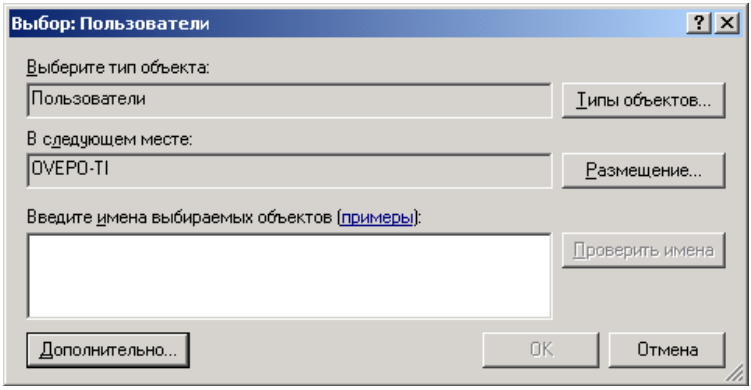


Рис. 18. Выбор пользователей.

2. Практическая часть

1) Вопросы по разделу:

1) Определите назначение программы *Брандмауэр*.

2) Перечислите функции, выполняемые программой *Брандмауэр*.

3) На работе каких алгоритмов основывается работа взломщиков?

4) Опишите работу программы *Брандмауэр*.

5) Как настроить программу *Брандмауэр*?

6) Какие опции рекомендуется включать, а какие выключать в программе *Брандмауэр*?

7) Каким образом исключить программу или сервис из списка с запрещенным доступом в программе *Брандмауэр*?

8) В каком случае активизация опции *Отображать уведомление, когда брандмауэр блокирует программу* не даст результата в программе *Брандмауэр*?

9) Определите назначение режима *Только локальная сеть (подсеть)* в программе *Брандмауэр*.

10) Определите назначение режима *Особый список* в программе *Брандмауэр*.

11) Перечислите дополнительные параметры настройки *Брандмауэра*.

12) Определите назначение механизма *Windows XP* «*Удаленные сеансы».*

13) Как настроить механизм *Удаленные сеансы* в *Windows XP*?

14) Определите назначение механизма *Windows XP*«*Удаленные пользователи».*

15) Как настроить механизм *Удаленные пользователи* в *Windows XP*?

2) Задание.

1) Произвести настройку *Брандмауэра* на своем ПК.

2) Произвести настройку механизма *Windows XP* «*Удаленные сеансы»* на своем ПК.

3) Произвести настройку механизма *Windows XP* «*Удаленные пользователи»* на своем ПК.

3) Порядок отчетности и форма контроля выполнения работы.

Контроль выполнения задания производится по окончании занятия и на консультациях в форме защиты выполненной работы, предоставленной в электронном и в бумажном виде в форме «Отчет по лабораторной работе …».

3. Материально-техническое обеспечение.

Специализированная мебель и технические средства для представления учебной информации, включая проекционное оборудование; компьютерный класс с компьютерами AMD 2400 – 12 шт., оснащенными операционной системой Windows XP и пакетом Microsoft Office.

ЛАБОРАТОРНАЯ РАБОТА 6
ПОЛИТИКА БЕЗОПАСНОСТИ

Цель занятия – приобретение обучаемыми необходимого объёма знаний и практических навыков в области политики безопасности.

Время – 4 часа.

Учебные вопросы:

1. **Теоретическая часть:**
   1) Политика безопасности, права пользователей.
   2) Глобальные параметры безопасности системы.
   3) Политика обновления.
2. **Практическая часть:**
   1) Вопросы по разделу.
   2) Задание.
   3) Порядок отчетности и форма контроля выполнения работы.
3. **Материально-техническое обеспечение.**

1. Теоретическая часть.

1) Политика безопасности, права пользователей.

Политика безопасности системы является одной из важнейших составляющих в обеспечении надежной и защищенной работы *Windows XP*. Настройка политики безопасности осуществляется в программе *Local Security Settings*: *Пуск|Панель управления|Администрирование|Локальная политика безопасности|Назначение прав пользователя*

После запуска программы *Назначение прав пользователя* появится окно *Локальные параметры безопасности* (рис. 1)

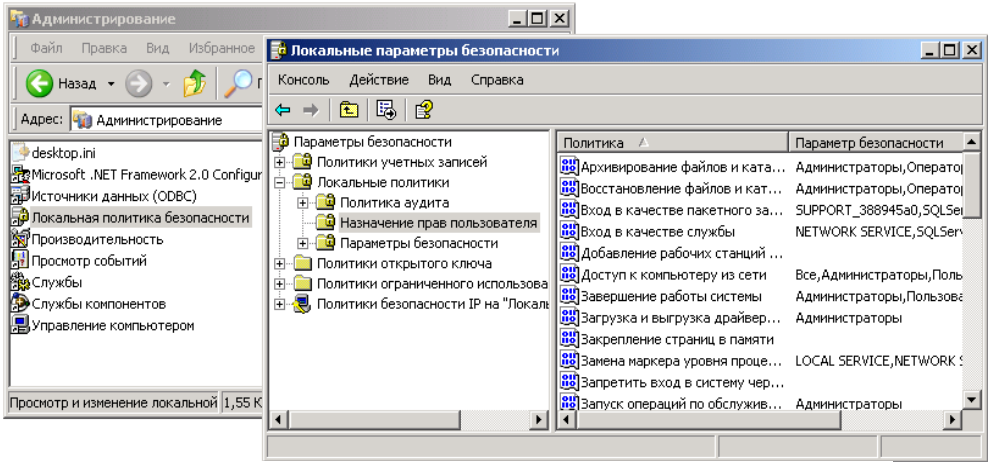


Рис. 1. Окно Локальные параметры безопасности.

Основные пункты политики безопасности.

1. Пункт *Доступ к компьютеру из сети* – определяет, какие именно пользователи и группы пользователей могут получать доступ к данному компьютеру по компьютерной сети. Если компьютер не подключен к локальной сети, рекомендуется запретить доступ пользователей извне, это позволит избежать атак взломщиков и их проникновение в систему при работе в Интернете. Для запрета доступа сетевых пользователей к компьютеру следует:

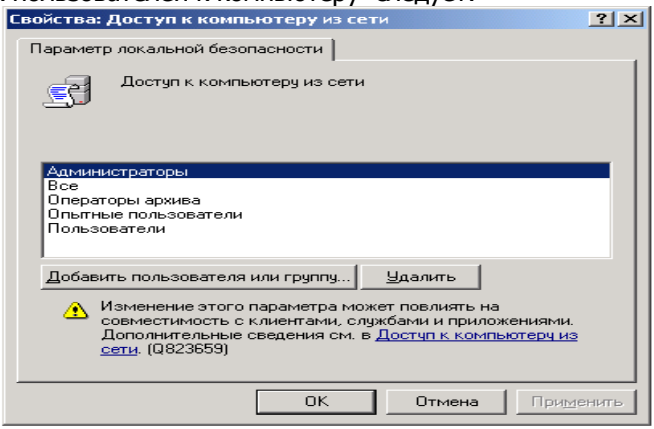


Рис. 2. Окно Параметр локальной безопасности.

–в окне *Политика* программы *Назначение прав пользователя* щелчком мыши выбрать политику *Доступ к компьютеру из сети*;

–появится окно *Параметр локальной безопасности Доступ к компьютеру из сети* (рис. 2);

–выделить всех пользователей (или лишних пользователей) при помощи указателя мыши и клавиши *Shift*;

–сделать щелчок по кнопке *Удалить*;

–нажать кнопку *ОК*.

Пользователи, которым разрешен доступ к компьютеру, должны быть отображены в данном пункте политики безопасности, иначе они не смогут войти в систему. Если пользователи в списке окна отсутствуют, то их следует добавить при помощи кнопки *Добавить пользователя или группу.* Для этого следует:

–сделать щелчок по кнопке *Добавить пользователя или группу*;

–в появившемся диалоговом окне сделать щелчок по кнопке *Дополнительно*;

–в окне *Пользователи* или группы нажать кнопку *Поиск*;

–в нижней части окна появится список всех пользователей и групп;

–щелчком выбрать нужную строку нажать кнопку *ОК*;

–в появившемся диалоговом окне в поле *Введите имена выбираемых объектов,* появится выбранный пользователь (группа), нажать кнопку *ОК*;

–выбранный пользователь (группа) будет отображен в окне *Доступ к компьютеру из сети*.

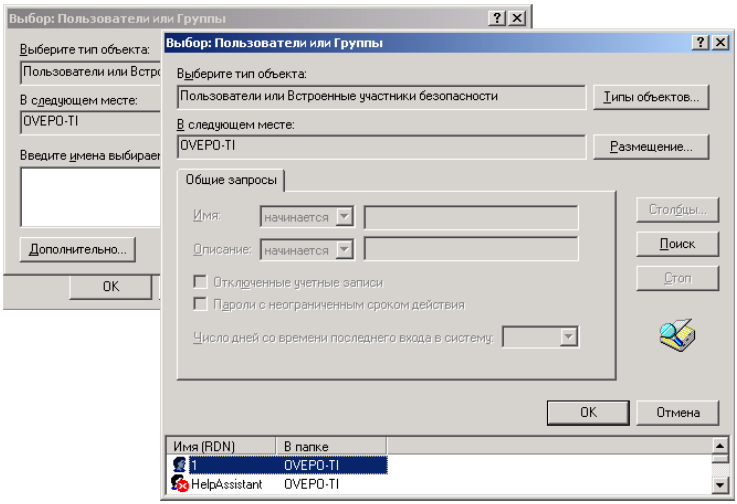


Рис. 3. Добавление пользователей или групп.

2. Пункт *Разрешать вход в систему через службу терминалов* является аналогичным предыдущему, но вход пользователей в систему осуществляется в качестве клиентов терминал-сервера. Если данный сервис не используется, то рекомендуется аналогичным методом запретить вход в систему всех пользователей, убрав их из значения данного пункта как клиентов терминал-сервера. В случае необходимости всегда можно добавить нужных пользователей и их группы при помощи кнопки *Добавить пользователя или группу* (рис. 4).

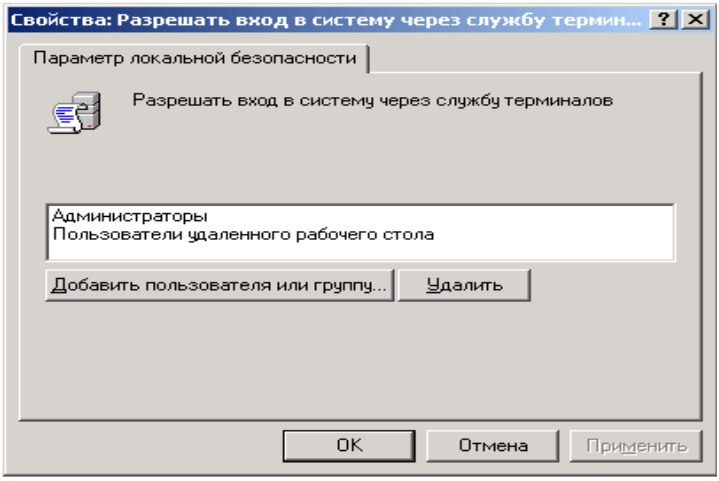


Рис. 4. Окно *Разрешить вход в систему через службу терминалов.*

3. Пункт *Изменение системного времени*, позволяющий пользователям, перечисленным в нем, менять системное время, а также просматривать календарь, появляющийся на экране при двойном щелчке по текущему времени на панели задач. По умолчанию данной возможностью обычные пользователи не смогут воспользоваться. Для разрешения пользователям выполнять такое действие следует их внести в список данного пункта политики безопасности при помощи кнопки *Добавить пользователя или группу* (рис. 5).

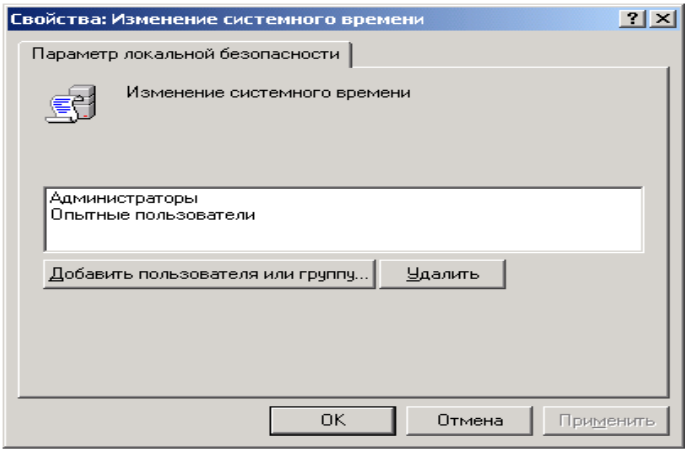


Рис. 5. Окно *Изменение системного времени.*

4. Пункт *Отладка программ* позволяет указать пользователей, которые смогут подсоединять свой отладчик к процессам и производить их отладку. Следует включать в этот пункт только тех пользователей, которым это действительно нужно, например, *системный администратор* и *системные программисты*. Не следует давать это право другим пользователям, так как этой возможностью могут воспользоваться вирусы для заражения системы, запущенные под одной из пользовательских записей, имеющей право на отладку процессов.

5. Пункт *Отказ в доступе к компьютеру из сети* содержит пользователей и их группы, которым запрещен вход в систему по компьютерной сети. При необходимости можно добавить пользователей, которым запрещен доступ к компьютеру с помощью кнопки *Добавить пользователя или группу* (рис. 6).

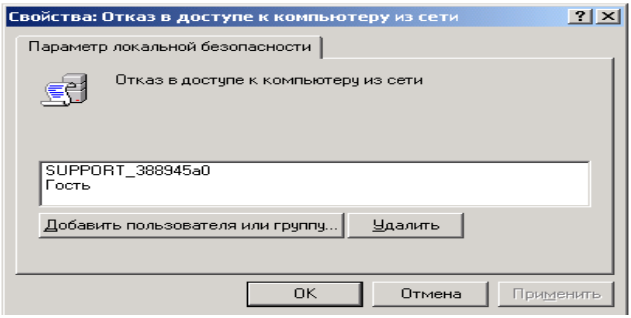


Рис. 6. Окно *Отказ в доступе к компьютеру из сети.*

6. Пункт *Отклонить локальный вход* содержит пользователей и их группы, которым запрещен локальный вход в систему. При необходимости можно добавить пользователей, которым запрещен доступ к компьютеру с помощью кнопки *Добавить пользователя или группу* (рис. 7).

7. Пункт *Запретить вход через службу терминалов* также содержит пользователей и их группы, которым запрещен вход в систему как клиентов терминал-сервера. При необходимости можно добавить пользователей, которым запрещен доступ к компьютеру с помощью кнопки *Добавить пользователя или группу* (рис. 8).

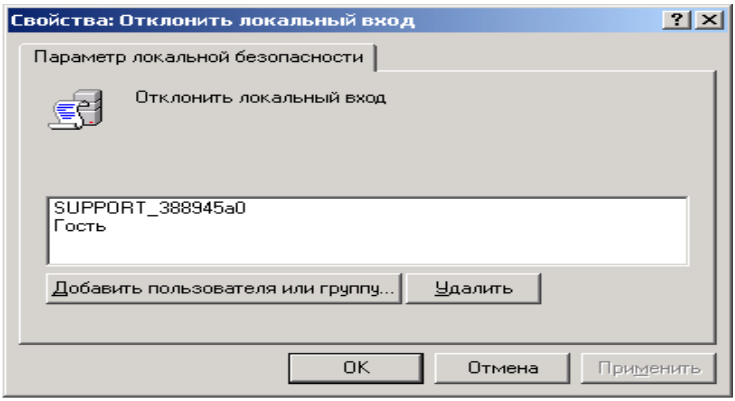


Рис. 7. Окно. О*тклонить локальный вход.*

С помощью трех перечисленных выше опций локальной политики безопасности можно запретить пользователям, которые по структуре организации не должны получать доступа, вход в систему. Этим можно предотвратить внутренние коллизии организации и защитить данные от их искажения или разрушения пользователями, которые удаленно пытаются ими воспользоваться.

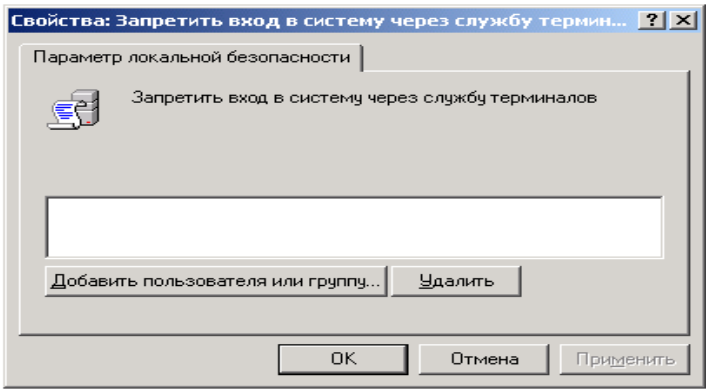


Рис. 8. Окно *Запретить вход в систему через службу терминалов*

8. Пункт *Принудительное удаленное завершение* является очень важным в настройке локальной политики безопасности, так как если его не настроить соответствующим образом, то система может получить команду на выключение или перезагрузку от удаленно пользователя. Поэтому в данном пункте следует указывать только пользователей, которым действительно может потребоваться с машин, находящихся в локальной сети, выключить или перезапустить систему.

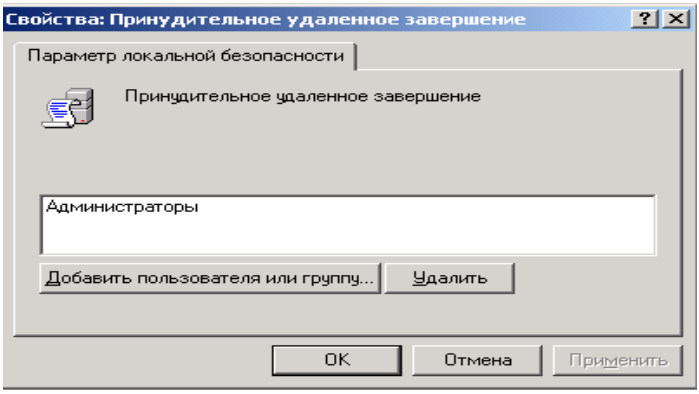


Рис. 9. Окно *Принудительное удаленное завершение*

9. Пункт *Загрузка и выгрузка драйверов устройств* позволяет указать, кто из пользователей может динамически устанавливать и выгружать драйвера устройств. Это право необходимо для установки драйверов уст- ройств, имеющих специфика-

цию *Plug and Play*.

10. Пункт *Локальный вход в систему* является очень важным и определяет, какие пользователи и их группы могут локально входить в систему.

11. Пункт *Управление аудитом и журналом безопасности* относится к механизму аудита системы и определяет, какие пользователи и их группы могут устанавливать аудит доступа к определенным объектам, таким как файлы, ключи реестра и пр. По умолчанию в данном пункте перечислена лишь одна группа локальных системных администраторов.

12. Пункт *Изменение параметров среды оборудования* определяет пользователей, которые будут иметь право в *Windows XP* менять значения системных переменных. По умолчанию на это имеют право только пользователи, принадлежащие локальной группе администраторов.

13. Пункт *Запуск операций по обслуживанию тома* позволяет указать пользователей и их группы, которые будут иметь право выполнять задачи по поддержанию работы накопителей, такие как очистка диска или его дефрагментация. Выполнение данных задач, по умолчанию, доверяется только пользователям из группы системных администраторов.

14. Пункт *Восстановление файлов и каталогов* позволяет указывать пользователей и их группы, которые могут выполнять операцию восстановления файлов и директорий из сохраненных копий, а также ставить им необходимые права доступа. По умолчанию в системе такими пользователями являются члены группы системных администраторов, а также операторы сохранения данных.

15. Пункт *Завершение работы системы* указывает, кто из локальных пользователей, имеющих учетные записи в системе, имеет право на ее выключение или перезагрузку. По умолчанию на это имеют право все пользователи. Однако, в ряде случаев, может потребоваться запретить выполнять данные функции некоторым пользователям. Например, если нужно, чтобы компьютеры работали в то время, когда некоторые пользователи их пытаются отключить. В этом случае нужно убрать этих пользователей из данного пункта. Особенно это может быть полезно, если определенные пользователи пытаются выключить компьютер, на котором находится информация, используемая удаленно другими пользователями.

16. Пункт *Овладение файлами или иными объектами* отвечает за возможность поль- зователей, перечисленных в

нем, брать на себя право становиться владельцами файлов и ектов. Этими объектами могут быть структуры *Active Directory*, ключи реестра, принтеры и процессы. По умолчанию на это имеют право только пользователи группы системных администраторов. Добавление к этому пункту пользователей означает предоставление им всех прав по доступу к различным объектам.

2) Глобальные параметры безопасности системы.

Глобальные параметры безопасности устанавливаются в разделе локальной политики безопасности *Параметры безопасности* (рис. 10). *Пуск|Панель управления|Администрирование|Локальная политика безопасности|Параметры безопасности*

Рассмотрим наиболее важные пункты.

1. Пункт *Учетные записи*: *Состояние учетной записи 'Администратор'* предоставляет возможность выбора: будет ли учетная запись администратора системы включена или отключена, при нормальном функционировании системы. В случае использования системы в безопасном режиме запись администратора будет включена, независимо от значения данного пункта. Для изменения значения этого пункта следует его выбрать двойным щелчком мыши и в появившемся окне поставить флажок в соответствующем режиме (рис.11).

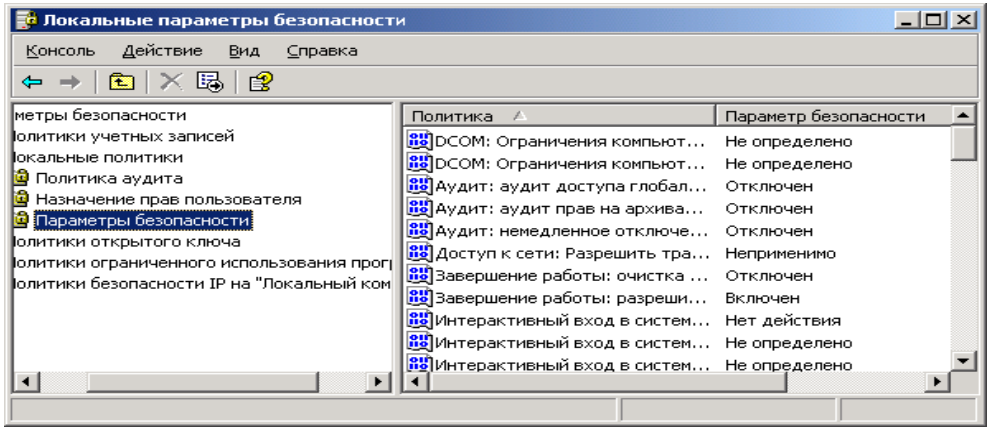


Рис. 10. Окно *Параметры безопасности*

Отключение учетной записи системного администратора может быть полезно, т.к. это дает гарантированную защиту от атак взломщиков на эту учетную запись. Если необходимо вклю-

чить учетную запись системного администратора, то это можно сделать под учетной записью другого пользователя, принадлежащего к группе системных администраторов, или в защищенном режиме работы операционной системы.

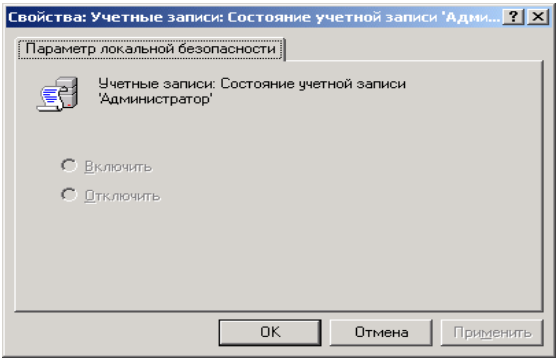


Рис. 11. Окно *Состояние учетной записи 'Администратор'*

Пункт *Учетные записи: Состояние учетной записи 'Гость'* позволяет отключать учетную запись гостя, т.к. для входа под данной учетной записью не требуется пароль, что может нарушить политику прав доступа пользователями. Учетная запись *Гость* по умолчанию отключена.

Пункт *Accounts: Limit local account use of blank passwords to console logon only*, в случае включения позволяет ограничить доступ к незащищенным паролями консольным учетным записям локальных пользователей со стороны различных сетевых сервисов, например: терминал-сервера, *Telnet* и *FTP*. По умолчанию, в целях защиты системы от сетевых атак, данный пункт включен.

Пункт Accounts: Rename administrator account позволяет переименовать встроенную учетную запись администратора системы. Это делается в целях защиты от атаки методом подбора паролей. Чтобы изменить имя учетной записи администратора, нужно дважды щелкнуть мышью по имени этого пункта и в появившемся окне ввести новое имя этой учетной записи.

Пункт *Audit: Audit the use of Backup and Restore privilege* позволяет контролировать выполнение всех операций сохранения и восстановления данных. Система будет сохранять сообщения обо всех резервируемых и восстанавливаемых файлах и папках. Это очень удобно для проведения контроля за операциями резервирования и восстановления дан- ных. Для работы данного пунк-

та необходимо включение в политике аудита опции *Аудит зования привилегий*. По умолчанию данный пункт локальной литики безопасности отключен.

Пункт *Audit: Shut down system immediately if unable to log security audits* является очень полезным и позволяет после своего включения, в случае обнаружения операционной системой невозможности производить запись событий аудита, произвести автоматическое выключение системы. Невозможность записи аудита событий системы обычно связана с переполнением хранилища этих сообщений. Для продолжения нормальной работы системы необходимо войти в нее под учетной записью администратора и произвести в программе:

Пуск|Панель управления|Администрирование|Просмотр событий

очистку всех этих сообщений, возможно, предварительно их сохранив. Это является гарантией того, что все действия системы или пользователей будут контролироваться администратором.

Пункт *Devices*: *Prevent users from installing printer drivers* – позволяет запретить пользователям устанавливать драйвера принтеров под их учетными записями.

Пункт *Devices: Restrict CD-ROM access to locally logged-on user only* позволяет ограничить доступ сетевых пользователей к локальному *CD-ROM*-приводу системы. Это может быть полезно, когда нужно чтобы сетевые пользователи имели доступ только к тем ресурсам, к которым они должны его иметь.

Пункт *Devices: Restrict floppy access to locally logged-on user only* позволяет ограничить доступ сетевых пользователей к локальному *CD-ROM*-приводу системы. Это может быть полезно, когда вы хотите, чтобы сетевые пользователи имели доступ только к тем ресурсам, к которым они должны его иметь. Это позволит локальным пользователям приватно работать с их личными носителями.

Пункт *Devices: Unsigned driver installation behavior* позволяет указать поведение системе, при попытке пользователей установить драйвер, не прошедший процедуру сертификации *Microsoft*. Он может иметь три значения:

– *Silent succeed* – происходит инсталляция этого драйвера и никаких сообщений не выдается;

– *Warn but allow installation* – происходит предупреждение пользователя о том, что драйвер не прошел сертификацию, но инсталляция продолжается. Данный пункт используется по

умолчанию;

– *Do not allow installation* – накладывается запрет на установку драйверов системы, не прошедших сертификацию.

Пункт *Interactive logon: Do not display last user name*, в случае своего включения, запрещает показ системе имени пользователя, который в ней работал последним. Это удобно в тех случаях, когда нужно избежать подбора паролей взломщиками к учетным записям пользователей системы, т.к. если у них не будет не только пароля, но и имени учетной записи пользователя, то их задача может стать в два раза сложнее. Данный пункт работает только в том случае, если отключен экран приветствия системы.

Пункт *Interactive logon: Do not require CTRL+ALT+DEL,* в случае его выключения, производит отображение на экране таблички, требующей от пользователя нажатия комбинации клавиш *CTRL+ALT+DEL* для входа в систему. В случае включения этого пункта данное сообщение системы появляться не будет. Данный пункт работает только в том случае, если отключен экран приветствия. Смысл ввода этой комбинации клавиш для входа в систему заключается в том, что она обрабатывается только системой. И это гарантирует то, что в операционную систему входит человек, а не программа по подбору паролей пользователей. Таким образом, данное сообщение может быть дополнительным барьером, охраняющим систему от взломщиков.

Пункт *Interactive logon: Prompt user to change password before expiration* устанавливает количество дней до конца срока действия пароля пользователя, когда система будет предупреждать пользователя об этом. Данный пункт имеет смысл только в том случае, если пароли пользователей имеют определенный срок действия.

Пункт *Recovery console: Allow automatic administrative logon* устанавливает автоматический вход системного администратора в консоль восстановления системы. Это удобно тем, что не требует ввода пароля администратора, но по той же причине, создает большие проблемы с безопасностью, так как консолью восстановления с администраторскими правами сможет воспользоваться любой желающий.

Пункт Recovery console: *Allow floppy copy and access to all drives and all folders*, в случае его включения, позволяет вам использовать команду *SET* консоли восстановления, которая может помочь установить следующие значения переменных:

– *AllowWildCards* – переменная включает поддержку масок у команд, например, *DEL*;

– *AllowAllPath* – переменная позволяет получить доступ ко всем файлам и папкам системы.

– *AllowRemovableMedia* – переменная позволяет копировать файлы на сменные носители, например, гибкие диски;

– *NoCopyPrompt* – переменная запрещает системе выдавать дополнительные сообщения при перезаписи существующего файла.

С помощью данного пункта можно скопировать или удалить информацию с жесткого диска системы. Поэтому не рекомендуется совмещать его использование с включенным предыдущим пунктом, позволяющим вход в консоль восстановления системы без администраторского пароля, т.к. можно лишиться всей информации.

Пункт *Shutdown: Allow system to be shut down without having to log on* позволяет, в случае его включения, производить выключение операционной системы до непосредственного входа в нее пользователями. Если вы не хотите, чтобы пользователи, не имеющие на это прав, выключали систему, установите данный пункт в положение Отключен.

Пункт *Shutdown: Clear virtual memory pagefile* является чрезвычайно важным в обеспечении безопасности вашей системы. При выключении системы в ее файле подкачки остаются данные, которые использовались в работе различными пользовательскими приложениями. Среди этих данных могут быть, частично или полностью, ваши документы, с которыми вы работали в течение сеанса работы с системой. Впоследствии, во время вашего отсутствия, эти данные могут быть кем-либо извлечены из файла подкачки. Таким образом, возможна утечка информации. И чтобы этого не случилось, системе может потребоваться очищать свой файл подкачки. Это можно сделать, включив данный пункт. Однако учтите, время очистки файла займет некоторое дополнительное время, и система будет выключаться чуть дольше.

3) Политика обновления.

Любое программное обеспечение содержит ошибки (баги), т.к. на этапе проектирования приложений и систем невозможно все предусмотреть. Поэтому в любом приложении появляются места кода, которые работают не так, как рассчитывали разработчики, что может привести к нештатной работе программного обеспечения, а также появлению новых ошибок или уязвимостей при его работе.

Для выявления ошибок все компании-разработчики

стараются тестировать свое программное обеспечение, т.е. проверять работу программного обеспечения в шоковых для него условиях, когда его ограничивают в размере доступной памяти, дискового пространства, скорости работы центрального процессора и пр. На этом этапе вылавливаются ошибки и вносятся исправления в код программного обеспечения, улучшающие его стабильность (робастность) или отказоустойчивость. Однако эти меры лишь частично позволяют избавиться от наиболее явных ошибок, которые проявили себя в тестировании. В н.в. не существует аппаратных или математических методов, позволяющих избавиться от ошибок в программном обеспечении на этапе его разработки.

После долгих поисков компании-разработчики нашли простой метод, который позволяет практически со стопроцентной вероятностью избавиться от ошибок в конечных продуктах, находящихся у пользователей. Этим методом является *периодическое обновление программных продуктов*. Компании разработчики решили, что в идеале программное обеспечение должно работать двадцать четыре часа в сутки, семь дней в неделю и в его работе не должно быть никаких нештатных ситуаций, вызванных ошибками. Это можно достигнуть с помощью грамотной *политики обновления*, которая используется практически в любом современном программном продукте, т.е. система периодически выходит в Интернет и проверяет сайт компании-разработчика на появление обновлений к программному обеспечению.

Компания-разработчик для программного продукта периодически помещает на своем сайте исправления, обновления и дополнения. Исправления – это специальные заплатки для программного обеспечения, которые исправляют существующие в нем ошибки, замеченные пользователями или специалистами компании. Обновления включают различные обновления программного продукта и заплатки от обнаруженных в нем ошибок. Дополнения добавляют программному продукту определенную функциональность.

Обновления для пользователей *Windows XP* позволяют не только избежать ошибок ОС, проявляющихся при ее использовании, но и практически гарантированно защитить ее от взломщиков и вирусов, т.к. исправляются все замеченные ошибки в системе безопасности. Алгоритм работы системы обновления *Windows XP* настроен на периодическую проверку сайта компании *Microsoft* на наличие различных обновлений и скачивание или предупреждение пользователя, в зависи- мости от его настроек. Все на-

стройки политики безопасности Windows XP находятся в ме *Система*: *Пуск*|*Настройка*|*Панель управления*|*Система*

Все операции настройки политики обновления ОС, а также выполнения процедуры обновления и получения от нее различных сообщений возможны только под учетной записью администратора системы. После запуска прогарммы появится окно, в котором нужно выбрать закладку *Автоматическое обновление* (*Automatic Updates*) (рис. 12). На закладке можно установить один из четырех параметров, которые будут определять частоту обновления системы:

1. *Автоматически (рекомендуется), Automatic (recommended)* – параметр устанавливается операционной системой *Windows XP* по умолчанию и означает регулярное обновление системы, заданное в двух нижерасположенных параметрах: частоты обновления и времени обновления. По умолчанию *Windows XP* будет обновляться каждый день в три часа (рис. 12). Скачивание обновлений операционной системы может происходить параллельно с работой в Интернете, т.к. операционной системой резервируется двадцать процентов пропускной способности канала связи с Интернетом, что позволяет быстро и незаметно скачивать системные обновления с сайта *Microsoft*.

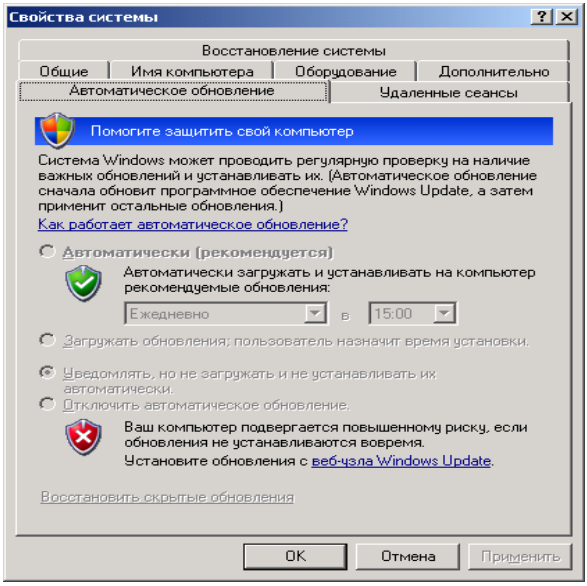


Рис. 12. Закладка *Автоматическое обновление* программы *Система.*

Если пользователь работает на домашнем компьютере, достаточно производить обновления системы раз в неделю. Если система является корпоративной или часто находится в Интернете, рекомендуется проводить каждодневное обновление, чтобы надежно защититься от сетевых взломщиков. Если система скачает обновления, и они будут готовы к инсталляции, система сообщит об этом. Если же за время выхода в Интернет система не успеет скачать все обновления, они будут скачаны в следующий раз. Все скачанные и установленные обновления можно удалить, воспользовавшись для этого программой *Установка и удаление программ*: *Пуск|Панель управлениях Установка и удаление программ*.

2. *Загружать обновления, пользователь назначит время установки*, *Download updates for me, but let me choose when to install them* опция позволяет операционной системе самостоятельно скачивать обновления, но для их установки она должна спросить разрешения у пользователя.

3. *Уведомлять, но не загружать и не устанавливать их автоматически, Notify me but don't automatically download or install them* опция позволяет операционной системе проверять наличие обновлений, но запрещает их непосредственное скачивание или установку. Эта опция полезна, если пользователь сам устанавливаете обновления, например с компакт-диска, также она позволяет сэкономить на интернет-трафике.

4. *Отключить автоматическое обновление*, *Turn off Automatic Updates* опция запрещает работу системы обновления *Windows XP*.

2.Практическая часть.

1) Вопросы по разделу:

1)Определите назначение *политики безопасности* системы.

2)Где производится настройка *политики безопасности* системы?

3)Как запретить доступ сетевых пользователей к компьютеру?

4)Как разрешить доступ сетевым пользователям, которым разрешено работать в системе к компьютеру?

5)Определите назначения пункта политики безопасности *Разрешать вход в систему через службу терминалов*.

6)Как предоставить определенной группе пользователей вносить изменения в системное время?

7)Определите назначе- ние пункта политики

ности *Отладка программ*.

8)Каким образом запретить вход определенной группе пользователей в систему по локальной сети?

9)Определите назначение пункта политики безопасности *Принудительное удаленное завершение*.

10) Как установить пользователей и их группы, которые могут локально входить в систему?

11) Как запретить определенной группе пользователей завершать работу системы, и в каких случаях это актуально?

12) В каком разделе производится настройка глобальных параметров безопасности?

13) Определите назначение *политики обновления*.

14) Как произвести настройку *политики обновления*?

2) Задание.

1)Произвести настройку *Политики безопасности* на своем ПК.

2)Произвести настройку *Параметров безопасности* на своем ПК.

3)Произвести настройку *Политики обновления* на своем ПК.

3) Порядок отчетности и форма контроля выполнения работы.

Контроль выполнения задания производится по окончании занятия и на консультациях в форме защиты выполненной работы, предоставленной в электронном и в бумажном виде в форме «Отчет по лабораторной работе …».

3.Материально-техническое обеспечение.

Специализированная мебель и технические средства для представления учебной информации, включая проекционное оборудование; компьютерный класс с компьютерами AMD 2400 – 12 шт., оснащенными операционной системой Windows XP и пакетом Microsoft Office.

ЛАБОРАТОРНАЯ РАБОТА 7
АУДИТ ЛОКАЛЬНОЙ СИСТЕМЫ

Цель занятия – приобретение обучаемыми необходимого объёма знаний и практических навыков в области аудита локальной системы**.**

Время – 4 часа.

Учебные вопросы:

1.Теоретическая часть: получение информации о процессах, происходящих в системе.

1)Аудит событий. Настройка аудита событий.

2)Просмотр событий.

3)Диспетчер задач и внутренние параметры системы.

4) Закладка *Приложения.*

5)Закладка *Процессы.*

6)Закладка *Быстродействие.*

7)Закладка *Сеть.*

8)Закладка *Пользователи.*

9)Просмотр дополнительных внутренних параметров системы.

2.Практическая часть:

1)Вопросы по разделу.

2)Задание.

3)Порядок отчетности и форма контроля выполнения работы.

3.Материально-техническое обеспечение.

1.Теоретическая часть: получение информации о процессах, происходящих в системе.

1) Аудит событий. Настройка аудита событий.

Практически все события системы, отражающие процессы, происходящие на уровне ядра ОС и выше и представляющие интерес для пользователя любого уровня, могут быть определены и сохранены в файле благодаря специальному механизму *Windows XP*, называемому *аудитом системы*. Просмотр сохраненных событий осуществляется специальной программой *Просмотр событий*.

Этот механизм является очень гибким в настройке и позволяет вести аудит различных событий, происходящих в системе, как по их классу принадлежности, так и по тому, удачно или неудачно было завершено событие. Например, можно заставить

систему контролировать все успешные попытки пользователей и приложений получения доступа к реестру. Или можно контролировать все попытки входа пользователей в систему, которые закончились неудачно.

Настройки аудита локальной системы находятся в программе *Локальная политика безопасности* (*Local Security Settings*):

Пуск|Все программы|Панель управления|Администрирование| Локальная политика безопасности

Для настройки аудита событий следует:

- запустить программу *Локальная политика безопасности*;
- выбрать пункт *Локальные политики* (рис. 1);
- выбирать пункт *Политика аудита*;
- появятся настройки политики аудита (рис. 2).
- Настройки аудита событий представляют собой список контролируемых событий, а также признак того, когда будет осуществляться запись этого события: при его успешном исходе, отказе или в обоих случаях. Факт успешности завершения события определяется по его коду завершения, существующему внутри системы. Для определения того, когда будет происходить запись того или иного события, определенного соответствующей строкой списка политики аудита, следует по ней сделать двойной щелчок мышью, после чего на экране появится окно настройки политики аудита (рис. 3).

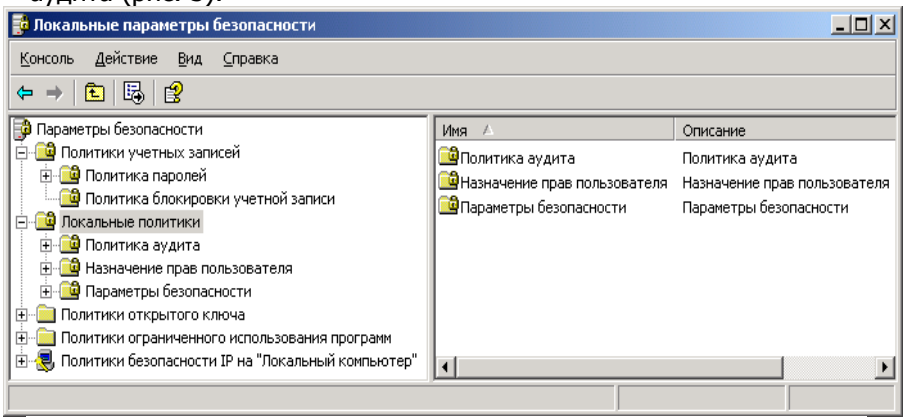


Рис. 1. Окно программы *Локальные параметры безопасности.*

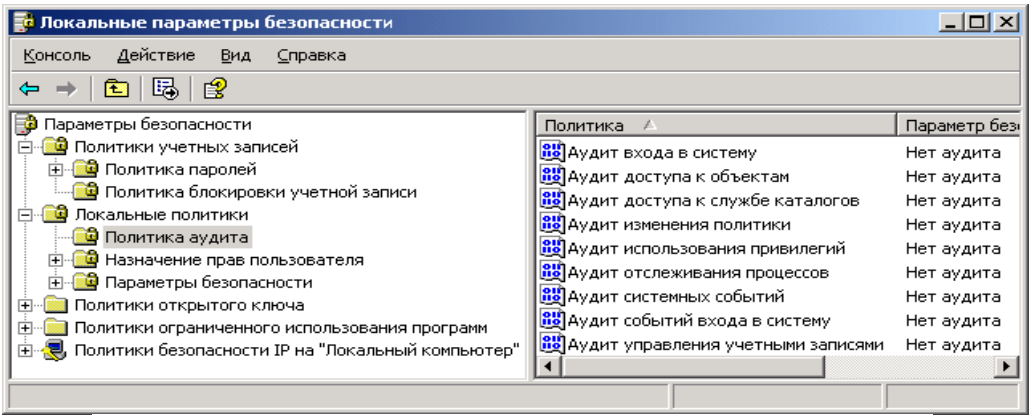


Рис. 2. Окно настройки аудита.

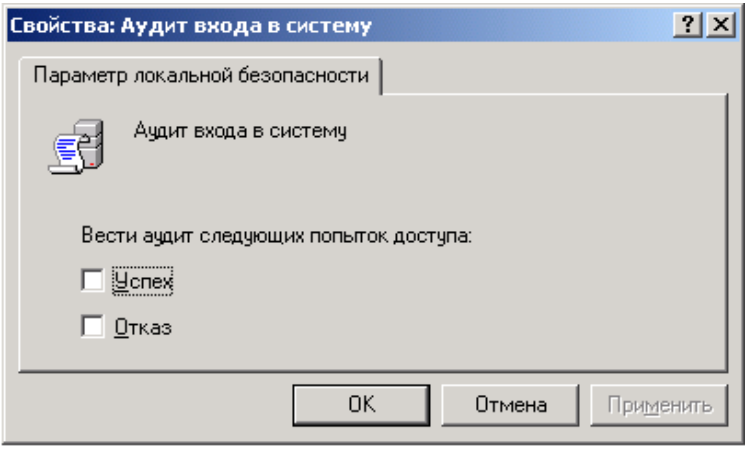


Рис. 3. Диалоговое окно ввода значений опций, определяющих, когда будет производиться аудит определенного события.

Данное окно позволяет пользователю выбрать вид аудита события для просмотра: при успешном завершении события, в случае его сбоя или в любом случае, настройки достигаются установкой флажка в соответствующих режимах: *Успех*, *Отказ* или в обоих режимах. Каждая из политик аудита обладает своими характерными особенностями:

1. Политика аудита *Аудит событий входа в систему* ответственна за запись событий, генерируемых операционной системой

при входе и выходе пользователей на других сетевых компьютерах, при условии, что данный компьютер используется для проверки подлинности учетной записи. При установке опции *Успех*, будет производиться запись событий, в результате которых пользователи успешно вошли в систему, в случае установки опции *Отказ*, будет производиться запись событий, в результате которых пользователи не смогли войти в систему. В случае установки обеих опций будет производиться запись всех попыток входа пользователей в систему, как удачных, так и нет.

2. В больших системах используется полное протоколирование входа пользователей в систему, которое достигается установкой обоих опций. Для небольших организаций и домашних систем достаточно вести протоколирование входа пользователей только по критерию *Отказ*, чтобы всегда можно было обнаружить случаи подбора паролей или попытки вторжения взломщиков, которые не увенчались успехом, и принять соответствующие меры. Так же будет получена информация о возможном источнике проблеем и пользователях, которые постоянно забывают свой пароль, и, вероятно, пытаются его где-то записывать.

3. Политика аудита *Аудит управления учетными записями* ответственна за запись событий, возникающих при работе с учетными записями пользователей: создание, изменение или удаление группы пользователей; переименование учетной записи пользователя, ее выключение, включение; установка иди смена пароля. Во всех случаях системой, в соответствии с установленными опциями *Успех* и *Отказ* будет производиться запись событий. Рекомендуется поставить политику на запись события в случае неудачного завершения операции доступа к объектам этой службы, что предохранит от возможных атак, которые могут проводиться в сетевых структурах.

4. Политика аудита *Аудит доступа к службе каталогов* ответственна за протоколирование доступа к объектам службы *Active Directory*, которая представляет собой, специальную сетевую файловую систему, элементами которой могут быть не только файлы и папки. Рекомендуется ее поставить на запись события в случае неудачного завершения операции доступа к объектам этой службы, что предохранит от возможных атак, которые могут проводиться в сетевых структурах.

5. Политика аудита *Аудит входа в систему* ответственна за запись событий, генерируемых операционной системой при входе и выходе пользователей на данном компьютере. При установке опции *Успех* будет произво- диться запись событий, в ре-

зультате которых пользователи успешно вошли в систему. В чае установки опции *Отказ* будет производиться запись событий, в результате которых пользователи по каким-либо причинам не смогли войти в систему. В случае установки обеих опций можно производить запись всех попыток входа пользователей.

6. Политики аудита *Аудит доступа к объектам* и *Аудит изменения политики* ответственны, соответственно, за аудит доступа к различным объектам системы, которые контролируются с помощью прав доступа, и за аудит работ с правами пользователей и политики аудита. В большинстве случаев достаточно будет производить аудит по отказу для этих двух событий. Данные записи могут пригодиться в случае, если в системе будет происходить что-то странное и необходимо выяснить причины возникших ситуаций.

7. Политика аудита *Аудит использований привилегий* производит запись событий, в случае использования пользователями специфических системных привилегий. Рекомендуется установить ее на запись событий в случае отказа для их получения пользователям. Данная информация может помочь специалистам по компьютерной безопасности в выяснении того, что произошло с системой.

8. Политика аудита *Аудит отслеживания процессов* позволяет вести аудит по таким событиями процесса, как запуск программы, выход из нее, а также другим важным системным событиям. Установка аудита данных событий по отказу может помочь понять, что происходит в системе и, возможно, где ей требуется помощь.

9. Политика аудита *Аудит системных событий* позволяет проводить аудит таких системных событий как перезагрузка или выключение компьютера, а также других важных сообщений, касающихся безопасности системы. Рекомендуется всегда устанавливать данную политику аудита, как минимум, на запись события, в случае его отказа.

Особенности аудита системы:

1. Чем больше событий в различных ситуациях протоколируется, тем больше сообщений аудита системы будете получено, следовательно, тем больше информации будет о процессах, происходящих внутри системы, инициируемые пользователями или различным программным обеспечением.

2. Чем больше сообщений системы будет получено, тем медленнее будет работать система и возможно слишком быстрое переполнение внутреннего ло- га безопасности операционной

системы. В результате чего придется достаточно часто производить его очистку в программе *Просмотр событий*.

2) Просмотр событий.

Программа *Просмотр событий* (*Event Viewer*) представляет специальную системную программу, входящую в состав *Windows XP*, которая позволяет видеть все сообщения, записанные в лог-файлы различными приложениями и самой ОС. Программа *Event Viewer* (рис. 4) находится:

Пуск|Панель управления|Администрирование|Просмотр событий

В данном окне содержится три пункта: *Приложение*, *Безопасность*, *Система* (*Application*, *Security*, *System*), иначе их называют *логами*, *лог-файлами* или, соответственно, *журналом приложений*, *журналом безопасности* и *журналом системы*. Информация, содержащаяся в них, является сообщениями, записанными приложениями системной безопасности ОС и системными компонентами *Windows XP*. Предполагается, что информация, содержащаяся в этих разделах важна для пользователя, и он должен периодически с ней знакомиться.

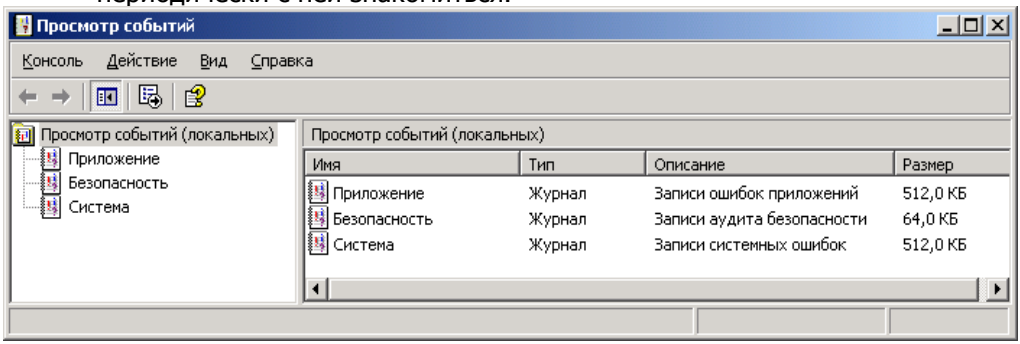


Рис. 4. Стартовое окно программы *Просмотр событий.*

Типы протоколируемых системой событий в логах:

– *ошибка* – данное сообщение сообщает об ошибке, такой как возможная утеря данных или нарушение функционирования программного обеспечения, например, невозможность старта одного из системных сервисов или ошибка при завершении приложения;

– *предупреждение* – сообщение не обязательно является чем-то важным, но может говорить об ошибке, которая может возникнуть впоследствии, например, нежелание какой-либо про-

граммы или сервиса во время выключения машины корректно завершаться;

– *уведомление* – сообщение, что описываемое событие успешно завершилось в приложении, драйвере или сервисе, например, успешный старт какого-либо системного сервиса или его остановка;

– *аудит успехов* – сообщение о том, что контролируемое событие в политике аудита и системой безопасности успешно завершилось, например, был произведен корректный вход одного из пользователей в систему;

– *аудит отказов* – класс событий, который будет сообщать о том, что контролируемое в политике аудита и системой безопасности событие завершилось с ошибкой, например, сообщение, сгенерированное при ошибке доступа к какому-либо объекту системы, или сообщение при регистрации пользователя, если он ошибся паролем.

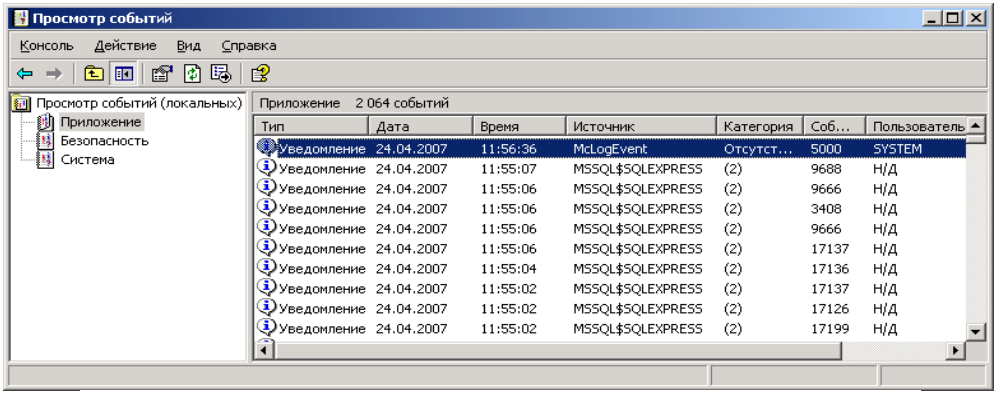


Рис. 5. Содержимое раздела *Приложение* программы *Просмотр событий.*

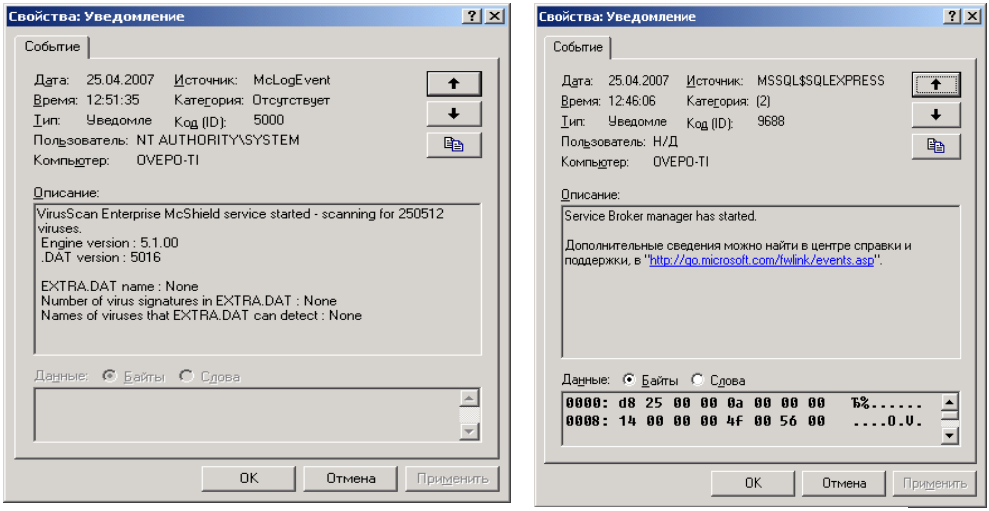


Рис. 6. Типичное сообщение, содержащееся в одном логе системы.

За запись сообщений в лог системы ответственен сервис *Event Log*, который стартует при загрузке *Windows XP*. Вход в раздел *Security* имеют только пользователи, входящие в состав группы локальных администраторов. По умолчанию в этот раздел система не пишет никаких сообщений. Для активации записи сообщений необходимо установить требуемую политику аудита системы (п.1.1.).

Для просмотра свойств конкретного уведомления следует сделать щелчок правой кнопкой мыши на событии. В появившемся контекстном меню выбрать команду *Свойства*. Появится окно *Свойства: Уведомление*. В верхней части окна (рис. 6) содержится типичная информация. В средней и нижней его части содержится информация, различная для каждого из сообщений. Информационные поля в описании события *Even* (формат протоколируемых событий):

– *дата* – поле определяет дату, когда данное событие произошло;

– *время* – поле определяет локальное время, когда это событие наступило;

– *пользователь* – поле определяет пользователя, от имени которого произошло событие (описание пользователя помещено в *Event Log*); поле может содержать имя клиента, вызвавшего событие, при обработке его запроса в программе-сервере, «*N/A*»

определяет принадлежность данного события к операционной системе.

– *компьютер* – поле содержит имя компьютера, на котором произошло данное событие;

– *код (ID)* – поле содержит идентификатор события, который вместе с полем *Источник* используются для анализа ситуации разработчиками программного обеспечения, вызвавшего данную запись в логе; при обращении в службу поддержки по их требованию нужно сообщить эти значения полей интересующих их событий системы;

– *источник* – поле содержит имя программного обеспечения, драйвера или компонента системы, вызвавшего запись события; этот идентификатор, а также поле *Event ID* используются для анализа ситуации разработчиками программного обеспечения, вызвавшего данную запись в логе;

– *тип* – поле содержит один из пяти типов сообщений, которым оно является;

– *категория* – поле классифицирует событие в программном обеспечении, которое его вызвало; данная информация наиболее часто используется в логе событий системы безопасности как идентификатор того, какой именно тип контролируемого события в политике аудита был при записи сообщения.

– *описание* – поле используется для вывода дополнительной информации, которая может лучше понять природу произошедшего в системе события.

В процессе запуска, работы и выключения системы скапливается большое количество событий, на изучение и просмотр которых требуется много времени. Поэтому свое внимание следует сконцентрировать на событиях, имеющих тип: *Ошибка*, *Предупреждение*, *Аудит отказов*. Первые два типа обычно появляются в разделах *System* и *Application* и сообщают о том, на что следует обратить внимание в работе системы и приложения, например, проблемы в работе жестких дисков, системных программ или самой операционной системы. Следует внимательно относиться к таким сообщениям, если их пропускать, то может случиться, что в будущем система перестанет корректно функционировать, а данные могут оказаться потерянными, если не производилось их регулярное резервирование.

Сообщения системы безопасности *Аудит отказов* могут быть связаны с тем, что на систему осуществлялась какая-либо атака извне или кто-то из пользователей забыл свой пароль. Частое появление таких сообщений может означать, что кто-то

подбирает пароль к определенным учетным записям системы. В данных случаях следует быть особенно внимательными, так как таких записей в *Event Log* бывает не много.

При переполнении разделов лог-файла системы следует:

– войти в систему под правами системного администратора;

– загрузить программу *Просмотр событий* (*Event Viewer*);

– выбрать раздел;

– раскрыть пункт операционного меню *Действия* или сделать щелчок правой кнопкой мыши на разделе и в появившемся контекстном меню выбрать пункт *Стереть все события* (рис. 7);

– на экране появится диалоговое окно, в котором будет предложено сохранить события, которые будут удалены, в отдельном файле (рис. 8).

Рекомендуется иметь историю совершенных событий, что может помочь при решении возникших проблем, т.к. при сохранении событий всегда можно проследить их начало и принять соответствующее решение. Поэтому следует нажать кнопку *Да* (рис. 8) и выбрать место и имя для сохраняемого файла, содержащего удаляемые сообщения из части *Events Log*.

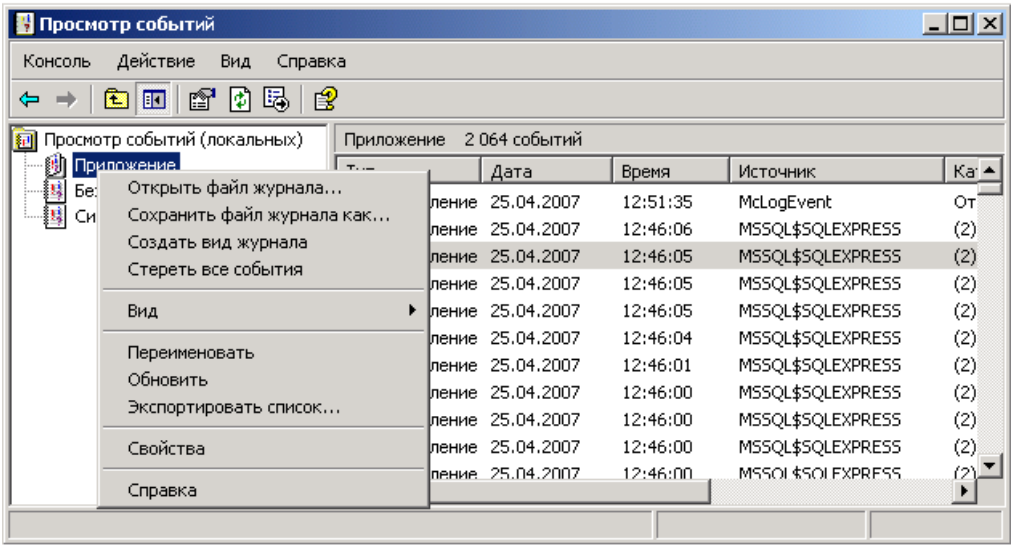


Рис. 7. Меню для очистки выбранного раздела лог-файла системы.

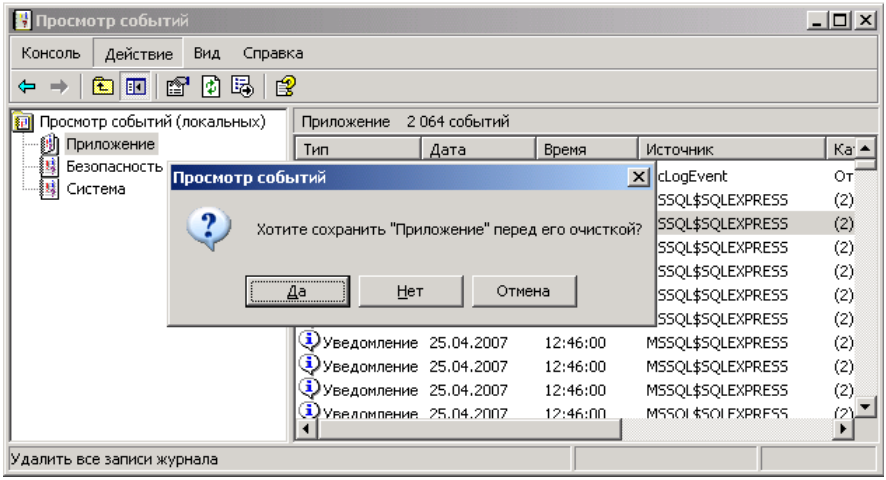


Рис. 8. Предложение системы о сохранении стираемых событий.

Если впоследствии придется просмотреть сохраненные события, то следует в программе *Просмотр событий* раскрыть пункт операционного меню *Действия* и выбрать команду *Открыть файл журнала* (рис. 7), события, находящиеся в файле, отобразятся на экране. Для выполнения операций очистки разделов *Events Log*, а также сохранения и загрузки файлов, содержащих сообщения из этих разделов, требуются права системного администратора.

3) Диспетчер задач и внутренние параметры системы.

Диспетчер задач является встроенным в операционную систему приложением, которое позволяет просматривать и анализировать работающие в данный момент в системе приложения и процессы, а также производить управление ими, независимо от того, в каком состоянии они находятся (рис. 9). *Диспетчер задач* позволяет:

– анализировать текущие параметры производительности операционной системы и параметры, которые были в ее недавнем прошлом, что позволяет наиболее удобно и достоверно настраивать производительность системы в соответствии с предъявляемыми требованиями;

– отображает состояние сетевых соединений и степень их загруженности, что позволит проводить наглядный мониторинг сетевых соединений, если они присутствуют в системе, также

можно обнаружить программы, тайно пересылающие информацию с компьютера в сеть.

– показывает информацию о пользователях (если в системе включена опция быстрого переключения пользователей), работающих с системой в данный момент времени: имя пользователя, его учетная запись, идентификатор входа, статус, имя компьютера, с которого пришел пользователь (если он использовал удаленный вход);

– позволяет проводить некоторые операции над пользователями;

– может помочь запустить приложение;

– может перейти в какое-то определенное окно приложения;

– может осуществить выход из системы.

Основные команды пунктов операционного меню *Диспетчера задач*.

Меню *Файл* команда *Новая задача* (*Выполнить*) запускает новое приложение.

Меню *Вид* содержит команды, ответственные за вывод на экран различной информации, отображаемой в окне *Диспетчера задач* и команды ответственные за частоту обновления информации, отображаемой приложением (рис. 10). Если *Диспетчер задач* будет постоянно обновлять информацию во всех своих окнах, прикрепленным к соответствующим закладкам, то на это потратится много времени работы центрального процессора и производительность системы понизится. Чтобы этого не случилось, разработчики пошли на компромисс, и теперь информация в окнах данной программы обновляется через определенные промежутки времени. Таким образом, любая информация, отображаемая в окне *Диспетчера задач*, является, фактически, всегда той, которая была на момент обновления информации в окне, а сейчас уже стала историей. Но поскольку интервалы обновления информации в окне весьма малы, то можно с большой вероятностью считать, что данная информация отображает текущее состояние системы.

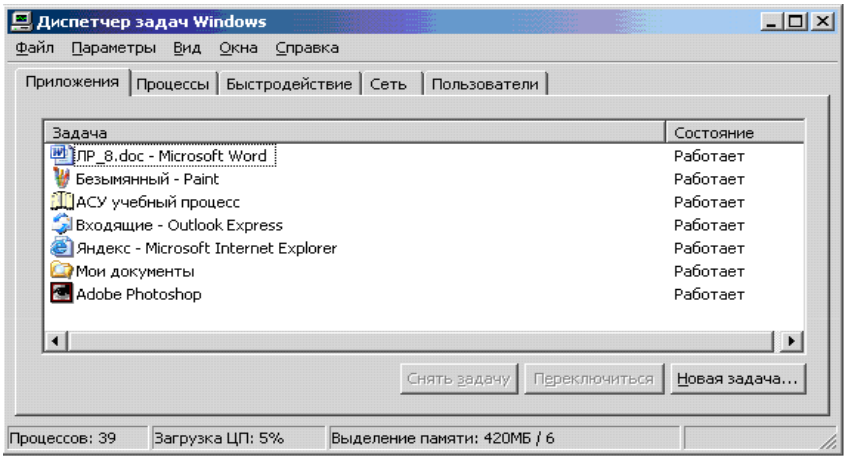


Рис. 9. Окно *Диспетчера задач.*

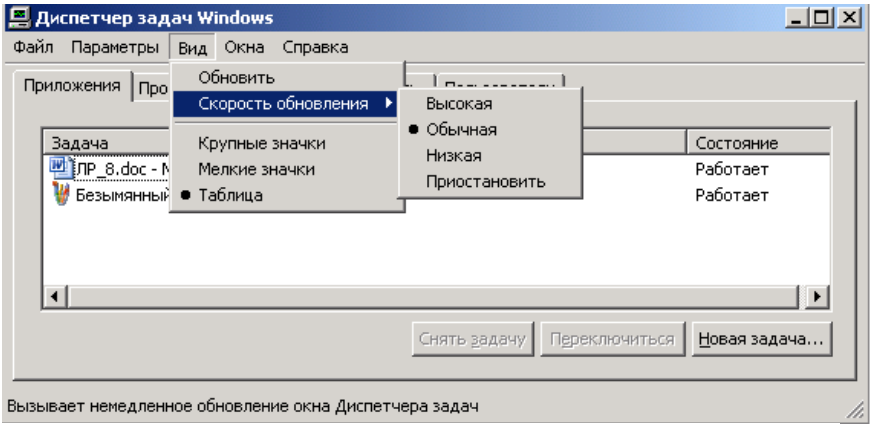


Рис. 10. Меню Вид *Диспетчера задач.*

Команда *Обновить* (рис. 10) предназначена для обновления всех окон диспетчера задач, с целью показа текущего состояния системы.

Команда *Скорость обновления* (рис. 10) позволяет установить, как относительно часто будет обновляться информация во всех окнах *Диспетчера задач*, для этого установлены следующие режимы:

– режим *Высокая* – предназначен для максимально быстрого обновления информации;

– режим *Обычная* – предназначен для обновления информации со скоростью, которая считается достаточной

разработчиками ОС (используется по умолчанию);

– режим *Низкая* – предназначен для редкого обновления информации;

– режим *Приостановить* – предназначен для запрещения обновления информации; означает паузу, которую стоит выбирать, когда нужно обдумать значения параметров, полученных от системы (фактически будет сохраняться информационный слепок системы, который существовал на момент остановки сбора информации).

Команда *Завершение работы* позволяет перевести компьютер в ждущий или спящий режимы, выключить или перезапустить его, завершить сеанс текущего пользователя или переключиться на другого пользователя системы. В ждущем режиме все запущенные программы остаются в оперативной памяти, подача энергии к которой сохраняется. В случае спящего режима все программы записываются на жесткий диск и система полностью обесточивается. Режим энергосбережения и гибернации (*лат*. *hibernatio* – спячка) будет корректно работать только тогда, когда оборудование и программное обеспечение поддерживают его и настроены соответствующим образом. При выборе пункта меню, которое перезапускает или выключает компьютер все пользователи, работающие в системе, будут отключены и все работающие программы остановлены.

Диспетчер задач содержит следующие закладки: *Приложения*, *Процессы*, *Быстродействие*, *Пользователи*.

4) Закладка *Приложения.*

Закладка *Приложения* отображает в системе все работающие в данный момент приложения (рис. 9). Внизу окна под списком активных приложений находятся кнопки, позволяющие завершить приложения, переключиться на приложение и запустить новое приложение. Кнопка *Снять задачу* завершит любое приложение. Если приложение не отвечает на запросы системы, когда она пытается его закрыть, то *Windows* спросит, действительно ли пользователь хочет его завершить, так как есть риск потери несохраненной информации. Нажатие кнопки *Завершить сейчас*, расположенной в этом окне, аварийно завершит приложение. При аварийном закрытии приложений все несохраненные в них данные могут быть безвозвратно потеряны.

Если часто приходится иметь дело с зависшими задачами, последовательное нажатие на кнопку *Завершить сейчас* в открываемых системой окнах с вопросами о завершении выбранного приложения является достаточно утомительным делом. Для избежания данной процедуры можно отредактировать значение ключа *HungAppTimeout*

в реестре по адресу: *HKEY_CURRENT_USER|Control Panel| Desktop*

Ключ определяет время в миллисекундах, через которое *Windows* будет считать приложение зависшим. По умолчанию это значение равно 5000 (пять секунд). Если через этот интервал времени приложение не будет реагировать на запросы системы, оно будет считаться зависшим. В этой же ветви реестра содержится ключ *WaitToKillApplicatioiiTimeout,* который задает время перед закрытием зависшего приложения. По умолчанию это значение равно 20000 (двадцать секунд). В итоге, после того как система в течение пяти секунд убедится, что приложение зависло, она будет ждать его завершения в течение еще двадцати секунд. Итого, суммарное время ожидания системы, перед закрытием зависшего приложения равно 25 секундам.

Для того чтобы зависшие приложения закрывались автоматически, в той же ветке реестра имеется ключ *AutoEnd-Tasks*. При установке его значения равное единице, система автоматически будет уничтожать зависшие приложения. Однако слишком малые значения переменных, определяющих ожидание системы, могут привести к тому, что нормально работающие, но долго думающие процессы будут считаться системой повисшими и могут быть закрыты, что приведет к нестабильной работе системы. Автоматическое уничтожение зависших процессов может оказаться полезной функцией. Если в системе существует большая загрузка приложениями и сервисами, то всегда есть достаточная вероятность появления зависших по каким-то причинам программ, которые тратят системные ресурсы, включая наиболее важные из них: системную память и время работа процессора, то их закрытие может быть жизненно важным для успешного продолжения функционирования системы.

Клавиша *Переключиться* (рис. 9) предназначена для переключение на выбранное приложение в списке приложений. После нажатия этой кнопки оно появится на экране поверх всех других приложений.

5) Закладка *Процессы.*

Любое приложение есть процесс, но не любой процесс есть приложение. Количество процессов и приложений в системе может сильно отличаться. В закладке *Процессы* (рис. 11) под списком процессов находится опция *Отображать процессы всех пользователей* в случае включения которой, при наличии соответствующих прав системного администратора, системой будут отображаться все процессы, которые запущены всеми пользователями системы в данный момент времени. С помощью кнопки *Завершить процесс,* можно уничтожить выбранный процесс (если достаточно прав). В информационной

строке выводится общее количество процессов, текущая загрузка ими процессора системы, а также память, выделенная процессам и операционной системе, и ее суммарная емкость, включая файл подкачки.

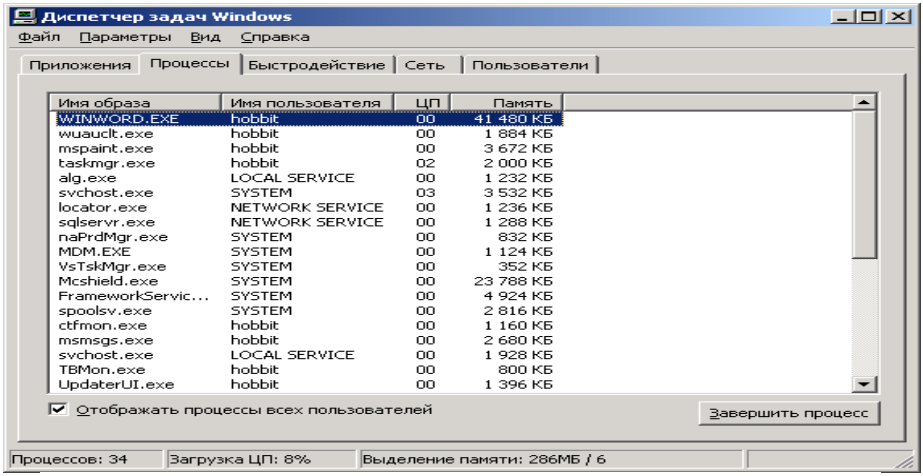


Рис. 11. Закладка *Процессы.*

По умолчанию для каждого процесса *Диспетчер задач* показывает имя исполняемого файла, на основе которого был создан процесс, или функцию процесса, если он принадлежит системе и не находится в отдельном исполняемом файле из которого мог бы быть запущен. После имени образа исполняемого файла следует имя пользователя, под которым был запущен каждый конкретный процесс. Если же процесс принадлежит системе, то в этом поле может содержаться информация о том, к какому типу сервиса системы он относится. Если же процесс является частью системы, то об этом будет сказано словом *SYSTEM*.

В поле *Загрузка ЦП* отображается информация о загруженности процессом центрального микропроцессора системы. В случае если в системе нет процессов требующих выполнения, то будет выполняться специальный процесс, называемый «Бездействие системы», принадлежащий ОС, о чем говорит строчка *SYSTEM*. Следующее информационное поле отображает количество памяти, потребляемой процессом.

Данные характеристики процессов, приведенные в *Диспетчере задач* по умолчанию, являются важнейшими. Имена исполняемых образов позволят в любой момент времени контролировать исполняющиеся процессы. Несмотря на то, что существует

методы скрытия имени исполняемого процесса от показа в *Диспетчере задач*, большинство процессов в нем отображаются. Поэтому всегда можно убедиться в том, что в системе исполняются только те процессы, которые должны исполняться в соответствии с поставленными требованиями.

Поле *Имя пользователя* позволит определить от учетной записи, какого пользователя запущен соответствующий процесс, что удобно для выяснения его механизма запуска. Если процесс запущен под правами какого-либо пользователя, то за его запуск ответственен прямо или косвенно этот пользователь. Если процесс работает от имени системы или администратора, то, если это вирус или шпионская программа, она уже достаточно глубоко проникла в систему и ее автозапуск нужно искать под учетной записью администратора системы в автозапуске или среди программ или в соответствующих местах в реестре, ответственных за автозапуск программ.

Уровень использования микропроцессора процессом определяет то, как много он «думает». Если процесс практически не потребляет процессорного времени, то он, вероятно, находится в состоянии *ожидание*. Если процесс грузит процессор работой, то он находится в состоянии *исполнение* или, возможно, завис.

Количество потребляемой оперативной памяти определяет степень ее использования процессом. Если процесс потребляет слишком много памяти под свои нужды, например, до половины всей доступной памяти, то это может негативно сказаться на работоспособности системы и привести к ее перезагрузке или остановке. Также существуют атаки взломщиков, основанные на потреблении всей доступной оперативной памяти системы с целью ее остановки или нарушения нормального функционирования. Поэтому если в системе странно себя ведет процесс, который не был запущен пользователями системы, то следует его исследовать, предварительно найдя исполняемый образ этого процесса.

Наряду с отображаемыми по умолчанию параметрами процесса (рис. 11) *Диспетчер задач* может по требованию пользователя показывать и другие параметры, задаваемые в пункте меню *Вид* режимом *Выбрать столбцы*. При выборе этого режима появится окно *Выбор столбцов* (рис. 12).

Помимо параметров *Загрузка ЦП*, *Имя пользователя* и *Память* (используемых по умолчанию) интересны параметры *Идентиф. процесса* (*PID*), *Время ЦП*, *Объем виртуальной памяти*, *Базовый приоритет*, *Счетчик дескрипторов* и *Счетчик потоков*. Данные параметры вызывают отобра- жение в *Диспетчере задач*,

соответственно, идентификатора процесса (*PID, Process ID*), мени работы на центральном процессоре, размера используемой виртуальной памяти, количества используемых процессом дескрипторов, а также числа нитей у процесса. После выхода из *Диспетчера задач* все его параметры настройки будут сохранены и при его повторном вызове будут учтены системой. Описание параметров.

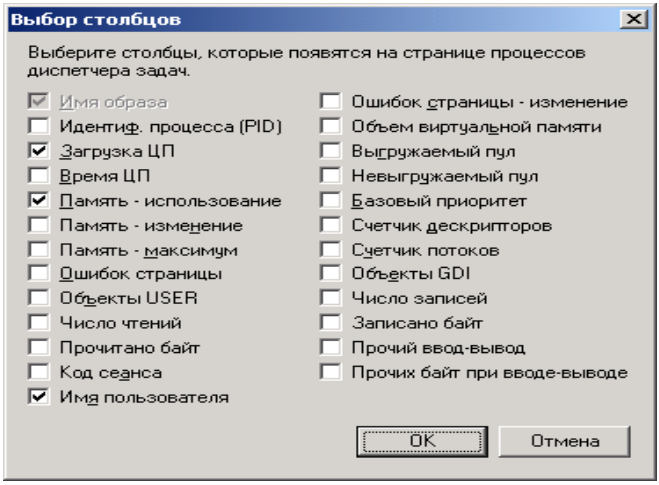


Рис. 12. Окно пункта меню *Вид* режима *Выбрать столбцы.*

1. Поле *Идентификатора процесса* (*PID, Process ID*) является важнейшим параметром, по которому можно найти нужный процесс в системе и продолжить его исследование другими методами, например, специальными отладчиками или сохранив на диске интерактивными дизассемблерами.

2. Поле *Время ЦП* определяет степень использования процессом центрального процессора, чем выше его загруженность, тем активнее работает соответствующее приложение. Если же загруженность процессора приложением незначительна или равна нулю, то это приложение большую часть времени проводит в состоянии покоя. Данное поле дает информацию о том, что происходит внутри системы и какие приложения проявляют ту или иную активность. Многие вирусы и троянские программы могут проводить большую часть времени своей жизни, находясь в состоянии ожидания, минимально используя время работы микропроцессора. Если какой-то неизвестный процесс производит значительную активность в

системе, то это также является предупредительным сигналом. Поэтому при необходимости всегда можно определить когда, кем и как был запущен процесс, что даст возможность предотвратить его повторный запуск.

3. Поле *Объем виртуальной памяти* определяет степень использования виртуальной памяти процессом. Большие запросы к виртуальной памяти могу означать также и ошибки в процессе или его нацеливание на разрушение системы путем захвата всей доступной виртуальной памяти.

4. Поле *Базовый приоритет* определяет значение приоритета, под которым запущен данный процесс. Уровень приоритета *Средний* имеет подавляющее большинство процессов пользователя; некоторые процессы, требующие больших вычислительных ресурсов компьютера, могут иметь приоритеты *Выше среднего* или *Высокий*. Существуют и другие значения приоритетов процессов, но они используются редко.

Исключением является процесс *Idle.exe*, который не учитывается системой как процесс, требующий выполнения и поэтому не имеет приоритета. Он выполняется лишь в случае, когда в текущий момент времени в системе нет других процессов, которые необходимо было бы выполнять на процессоре. В среднем процессы, имеющие больший приоритет, выполняются в операционной системе быстрее, так как им для их выполнения операционной системой предоставляется больше времени работы микропроцессора.

Большое количество пользовательских процессов с приоритетами выше *Средний* могут сильно тормозить работу системы, сделать ее нестабильной, или привести к перезагрузке. Поэтому если неизвестный процесс имеет приоритет выше приоритета *Средний*, то следует определить, что это за процесс и откуда он взялся в системе.

5. Поле *Счетчик дескрипторов* определяет количество используемых процессом дескрипторов – идентификаторов, которые определяют используемые процессом системные ресурсы, например, файлы. Чем больше дескрипторов использует процесс, тем большей активностью он обладает.

Данная ситуация может служить косвенной информацией о внутренней деятельности процесса. Например, если неизвестный процесс, занимающий сравнительно мало оперативной памяти и ресурсов центрального процессора, имеет число дескрипторов за тысячу, то это повод задуматься над тем, зачем все они ему нужны. Вероятно, что он пытается тайно анализировать содержи-

мое файлов системы, заразить или разрушить их содержимое. Существует и другой вариант: многие сетевые атаки на систему основываются на построении к ней избыточного количества запросов, которые она не может обслужить и, как следствие, прекращает нормальное функционирование. Наличие большого количества дескрипторов или постоянное увеличение их числа у процесса, говорит в пользу такого предположения и требует немедленного вмешательства. Если неизвестный процесс имеет очень мало открытых дескрипторов, то он так же является кандидатом на исследование или уничтожение.

6. Поле *Счетчик потоков* определяет число нитей у процесса. *Нитями* называются, процессы, которые выполняются в рамках одного процесса, являющимся для них материнским. Многие процессы имеют несколько нитей, это значительно упрощает их разработку для программиста. Однако большое число потоков у одного процесса (более сотни) является подозрительным и может указывать на применение против системы атаки отказа в обслуживании (как в случае с числом дескрипторов у процесса). В атаке отказа в обслуживании процесс, который перегружает систему запросами на ресурсы, может являться обычной программой, но другая программа или взломщик удаленно по сети делают так, что она начинает все больше и больше запрашивать у системы вычислительных ресурсов.

Единственной возможностью предотвратить такие атаки является периодическое обновление версий используемого программного обеспечения. В целях профилактики или поиска причин возникновения таких атак следует периодически проводить проверку работающих процессов операционной системы посредством *Диспетчера задач, Far Manager* или других средств.

Рекомендуется соблюдать следующее правило: если в *Диспетчере задач* находится неизвестный процесс и его поведение является странным, хотя бы по одному из вышеприведенных параметров, то, если нет других идей, следует его завершить с помощью кнопки *Завершить процесс* или сообщить о процессе системному администратору (если недостаточно прав).

6) Закладка *Быстродействие.*

Закладка *Быстродействие* отображает параметры производительности системы (рис.13).

На индикаторах *Загрузка ЦП* и *Хронология загрузки ЦП* выводится информация, соответственно, о текущей загруженности микропроцессора и о его ис- пользовании в прошлом. В

идеале, в случае бездействия системы, загруженность должна быть в диапазоне от нуля до одного или двух процентов. Это не исключает периодические резкие повышения нагрузки на процессор, вплоть до ста процентов, например, в случае операций с внешними устройствами (жестким диском или принтером).

Если же средняя загрузка системы составляет более пяти процентов, то это значит, что в ней постоянно выполняется какой-то процесс, имеющий сравнительно большую нагрузку на систему. Для выяснения этого процесса следует обратиться к закладке *Процессы* или к закладке *Сеть*, чтобы убедиться в том, что этот процесс ничего не делает в локальной сети или Интернете. Многие сетевые вирусы и черви имеют тенденцию находиться постоянно в системе, выполняя некоторую внутреннюю работу, периодически работая с сетью. И если это так, постоянная небольшая загрузка системы и использование достаточно большого количества памяти, а также сетевой трафик будут их демаскировать.

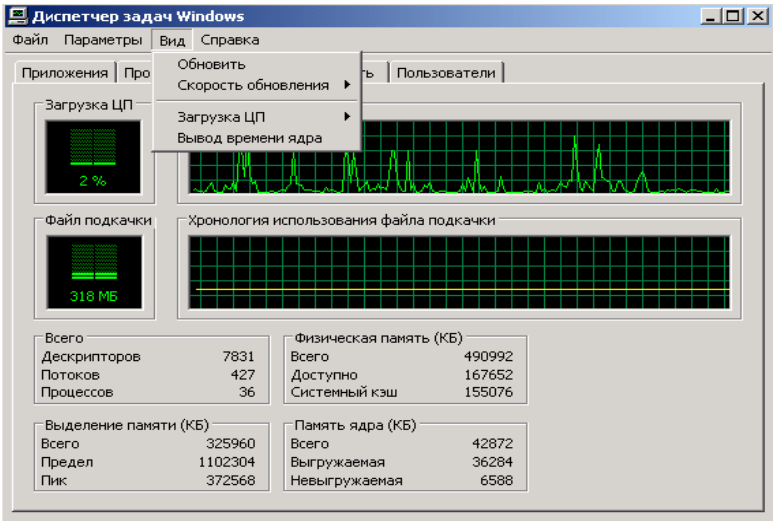


Рис. 13. Вкладка *Быстродействие*.

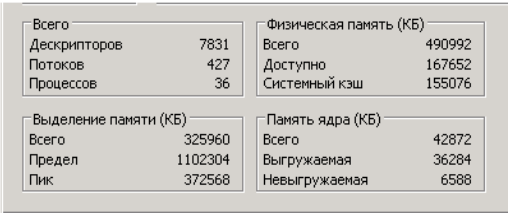
Если в системе имеется более одного микропроцессора, то для каждого из этих процессоров на *Диспетчере задач* появятся свои индикаторы *Загрузка ЦП* и *Хронология загрузки ЦП*.

С помощью пункта меню *Вид* | *Вывод времени ядра* (рис. 13) можно конкретизировать какая именно производительность отражается на индикаторах *Диспетчера задач*: суммарная загрузка системы или отдельная информация по загрузке микропроцес-

сора операционной системой и пользовательскими программами. Этот режим позволяет получить дополнительную информацию о том, где именно происходит повышенная загрузка микропроцессора.

Индикаторы *Файл подкачки* и *Хронология использования файла подкачки* показывают, соответственно, текущее использование файла подкачки и его использование системой в прошлом. Это очень важный показатель. Если файл подкачки используется больше чем на половину при условии, что не были запущены большие программы (текстовые или графические редакторы, компиляторы, плееры и пр.), то это верный признак того, что в системе что-то наладится. Это может быть ошибка в программном обеспечении или атака типа отказа в обслуживании. Для выяснений причин происходящего следует обратиться к закладке *Процессы*, обращая особое внимание на то, как процессы используют память. Также стоит обратить внимание на закладку *Сеть*, чтобы убедиться в том, что процессы ничего не делают в локальной сети или Интернете.

Параметры системы *Всего* отображают общее число дескрипторов (в строке *Дескрипторов*), нитей (в строке *Потоков*) и процессов (в строке *Процессов*). Если количество дескрипторов, потоков и процессов будет слишком большим, то возможно, что кто-то против системы использует сетевую или локальную атаку отказа в обслуживании. Система может стать нестабильной или перестанет функционировать нормально, а вся информация, содержащаяся в пользовательских программах, будет утеряна. Следует срочно найти процесс, который использует большое количество ресурсов и его закрыть. После чего произвести поиск локальной или удаленной причины, вызвавшей данную атаку.



В группе параметров производительности системы *Физическая память (КБ)* отражается суммарный объем оперативной памяти (строка *Всего*), доступной памяти (строка *Доступно*) и объем памяти, занятой под кэш (строка *Системный кэш*). Все объемы приведены в килобайтах. Если обнаружено, что в системе без запуска каких-либо программ слишком мало доступной памяти (меньше сотни мегабайт), то следует установить дополнительную оперативную память или разо- браться с процессами, которые

ее потребляют.

Группа параметров *Выделение памяти (КБ)* определяет использование памяти приложениями в системе:

– строка *Всего* описывается текущее использование памяти;

– строка *Предел* показывает максимальную емкость памяти, которая может быть использована приложениями (сумма емкостей файла подкачки и оперативной памяти);

– строка *Пик* показывает максимальный объем памяти, который использовался приложениями в системе.

Если значение *Пик* или *Всего* приближается к значению *Предел*, то при условии, что в системе не загружены большие приложения, возможно, происходит локальная или удаленная атака.

Группа параметров *Память ядра (КБ)* показывает объем памяти, используемой ядром операционной системы *Windows XP*:

– строка *Всего* показывает суммарный объем памяти, доступный ядру;

– строка *Выгружаемая* показывает размер памяти, который может быть вытеснен в файл подкачки специальными средствами ОС;

– строка *Невыгружаемая* показывает размер памяти, используемой ядром системы, которая не может быть вытеснена в файл подкачки и находится постоянно в оперативной памяти.

В зависимости от текущей ситуации в работе операционной системы, эти значения могут меняться в ту или иную сторону. Если эти значения меняются резко, например, в два раза, то это признак того, что в системе что-то не так. Поэтому следует выяснить причину вызывающую такие колебания в памяти, используемой ядром операционной системы. Рекомендуется перезагрузить систему т.к. в некоторых случаях это объясняется ошибками в операционной системе, которые исчезнут после перезагрузки.

Для диагностики системы можно использовать внешние антивирусные программы, внешние программы проверки системы или встроенные средства ОС. Например, для проверки идентичности файлов можно использовать программу установки *Windows XP* с соответствующим ключом. Справку о ключах можно получить, запустив файл *WinNT32.exe* с ключом *"/?"*, который находится в дистрибутиве операционной системы, в папке 1386.

7) Закладка *Сеть*.

В закладке *Сеть* отображается мониторинг сетевых или модемных соединений (рис. 14).

Если нет сетевых подключений, то на экране появится окно идентичное левому окну, изображенному на рис. 14. Если же компьютер подключен к компьютерной сети и был произведен выход в Интернет либо была загружена сетевая программа, то на экране появится окно идентичное правому окну, изображенному на рис. 14.

В верхней части окна отображается графическое представление загрузки сетевого соединения. Загрузка измеряется от нуля до ста процентов. В нижней части окна указывается для каждого сетевого адаптера системы его имя, текущая сетевая загрузка, скорость соединения и состояние соединения.

Можно дополнить отображаемые характеристики сетевых соединений (рис. 15):

Меню *Вид* \ *Выбрать столбцы*

В целях повышения информированности о процессах, происходящих в сетевых соединениях, можно установить ряд дополнительных опций:

– опция *Описание адаптера* позволяет посмотреть описание адаптеров, которые используются в системе;

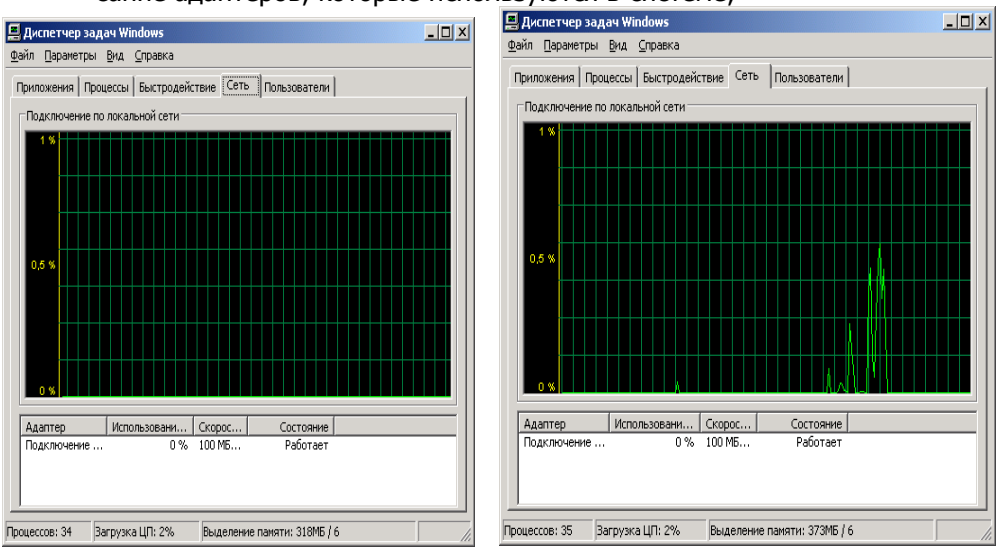


Рис. 14. Закладка *Сеть.*

– опции *Пропускная способность отправки* и *Пропускная*

способность получения позволяют, соответственно, определить количество в процентах передаваемых и получаемых байт, которые проходят через сетевое соединение в текущий момент времени;

– опция *Пропускная способность всего* показывает в процентах суммарное количество информации, прошедшей через сетевое соединение, в текущий момент времени;

– опции *Отправлено байт* и *Получено байт* позволяют, соответственно, определить в байтах суммарное количество переданных и полученных данных через сетевое соединение за все время его существования.

Все сетевые программы, работающие в системе, вносят свой вклад в загрузку определенных сетевых интерфейсов, если действительно работают с ними. Их активность отображается на окне мониторинга сетевых соединений *Диспетчера задач*.

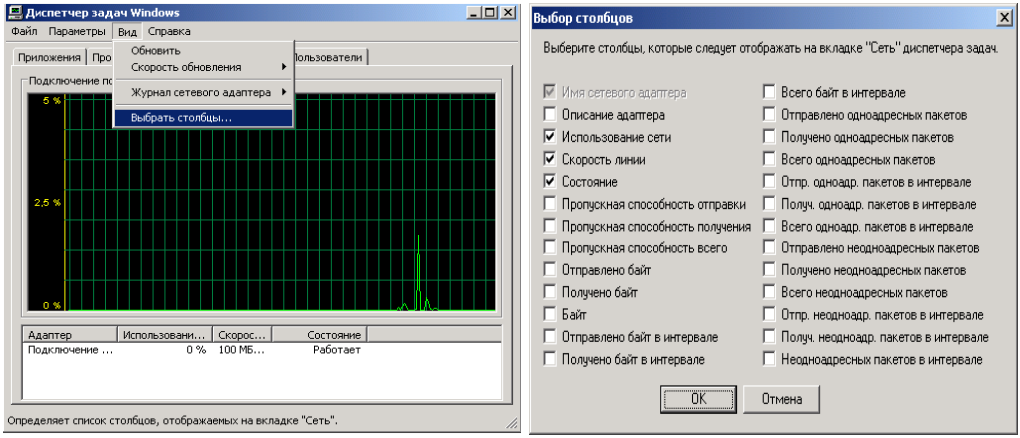


Рис. 15. Опции, позволяющие отображать в окне мониторинга сетевых соединений дополнительные параметры.

Содержимое закладки *Сеть* предоставляет дополнительную возможность поиска посторонних программ. Например, если в окне мониторинга существует постоянная загрузка канала, равная определенному значению (при условии, что не были запущены сетевые программы и обновление операционной системы выключено), то тогда с уверенностью можно сказать, что в системе удобно устроился вирус, троянская программа или программа-шпион. Следовательно, необходимо проверить систему антивирусным сканером и убедиться в корректности настроек сетевого экрана. В отличие от других средств *Диспетчера задач*, данная

закладка может практически гарантированно обнаружить деструктивное программное обеспечение.

8) Закладка *Пользователи.*

Закладка *Пользователи* отображает пользователей, работающих в текущий момент в системе (рис. 16).

В данном окне можете выбрать пользователя и посмотреть его параметры в соответствующих столбцах:

– столбец *Код* отображает идентификатор сессии пользователя в системе;

– столбец *Состояние* – отображает статус пользователя;

– столбец *Имя клиента* – отображает имя машины, с которой пришел пользователь, если он работает в сети;

– столбец *Сеанс* – отображает имя сессии пользователя на компьютере.

С помощью кнопок, расположенных внизу окна, можно выполнять ряд системных действий по управлению пользователями:

– кнопка *Отключить* – отключает выбранного пользователя от компьютера;

– кнопка *Выйти из системы* – заставляет пользователя выйти из системы;

– кнопка *Отправить сообщение* – посылает другому пользователю сообщение.

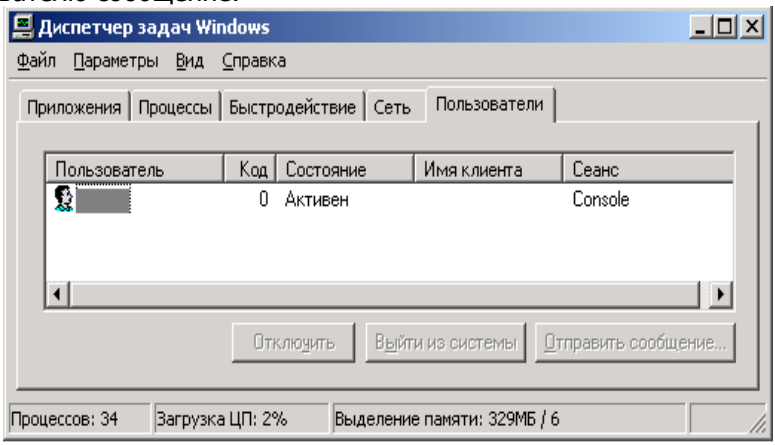


Рис. 16. Закладка *Пользователи.*

Окно просмотра активных пользователей в системе удобно тем, что всегда можно контролировать пользователей или программы, которые работают в системе под соответствующими

учетными записями. При обнаружении подозрительного пользователя можете его отключить или послать ему соответствующее сообщение. Кроме того, в случае обнаружения каких-либо проблем, всегда можно знать, кто работает в системе, и, как следствие, предпринять административные или иные меры, в случае обнаружения причин этих проблем.

9) Просмотр дополнительных внутренних параметров системы.

Возможности диспетчера задач широки, но некоторые функции, связанные с функционированием системы, ее настройкой и конфигурацией, он не может контролировать. Для этого *в Windows XP* существуют другие средства. Если в процессе работы системы возникнут какие-либо вопросы по ее конфигурации или времени работы (*аптайму*), то можно узнать причины, запустив программу *SystemInfo* в командной строке (рис. 17).

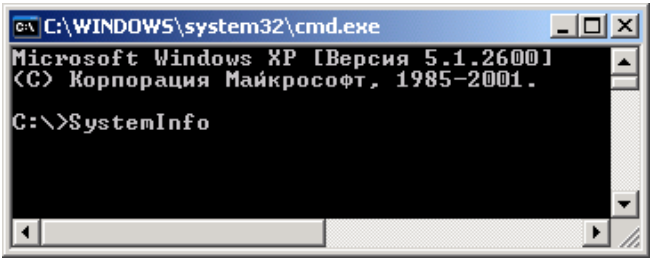


Рис. 17. Запуск программы *SystemInfo* в командной строке.

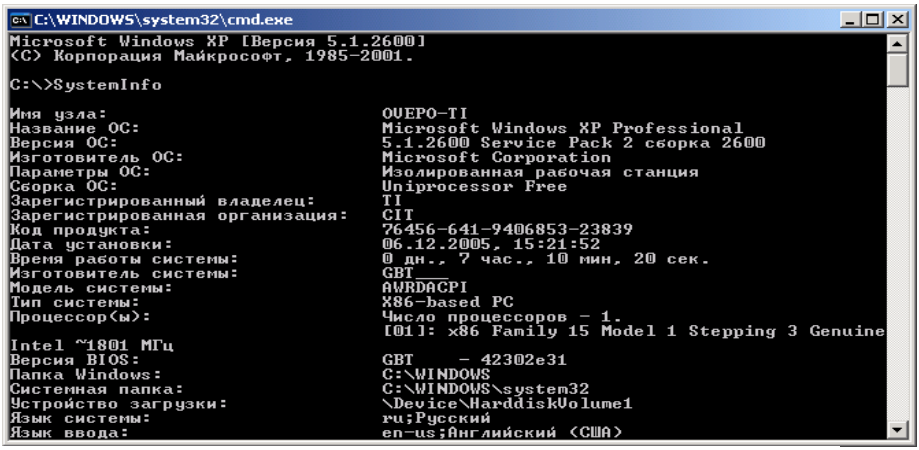


Рис. 18. Окно программы *SystemInfo.*

На экран будет выведена подробная информация. Можно запустить программу с каналом *more*, набрав в командной строке: *systemInfo | more*

Программа при заполнении текстового экрана будет ожидать нажатия пробела, чтобы показать следующий экран с информацией.

Для отображения информации с помощью графического интерфейса можете запустить программу: *System Information* (рис. 19.)

Пуск|Все программы|Стандартные|Служебные|Сведения о системе

В левой части этого окна расположено дерево, в котором можно выбирать логическую область информации, относительно которой нужно узнать параметры системы. В правой части окна отображается ее непосредственное значение. Например, выбрав *Ресурсы аппаратуры* (*Hardware Resources*) можно посмотреть информацию по какому-либо аппаратному ресурсу системы. Данная программа позволяет быстро, легко и удобно просмотреть содержимое системы.

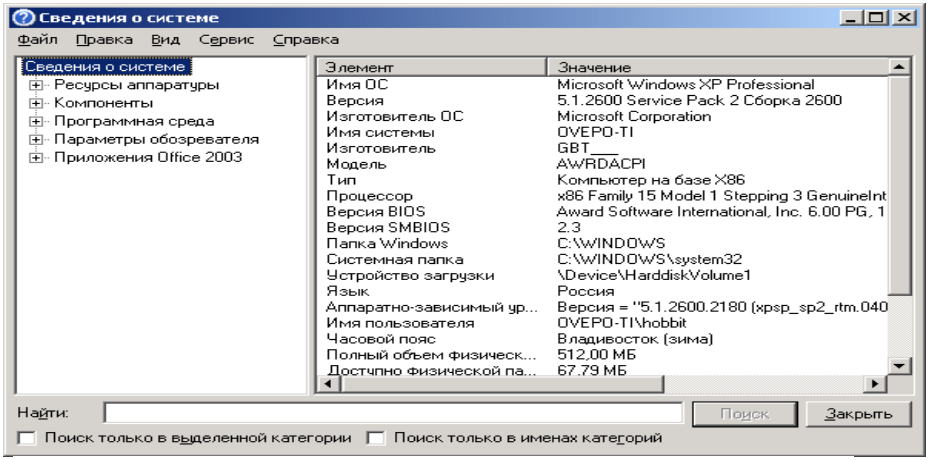


Рис. 19. Окно программы *System Information.*

В левой части этого окна расположено дерево, в котором можно выбирать логическую область информации, относительно которой нужно узнать параметры системы. В правой части окна отображается ее непосредственное значение. Например, выбрав *Ресурсы аппаратуры* (*Hardware Resources*) можно посмотреть информацию по какому-либо аппаратному ресурсу системы. Данная программа позволяет быстро, легко и удобно просмотреть содержимое системы.

2.Практическая часть

1) Вопросы по разделу:

1)Что собой представляет механизм *Windows XP*, называемый *аудитом системы*?

2)Перечислите функции, выполняемые вышеуказанным механизмом ОС.

3)Каким образом произвести настройку *аудита локальной системы*?

4)Что собой представляют настройки *аудита событий*?

5)Комплекс каких действий нужно выполнить для определения того, когда будет происходить запись того или иного события, определенного соответствующей строкой списка политики аудита?

6)Перечислите виды аудита событий (сделайте копию окна настройки аудита с видами аудита событий).

7)Какими характерными особенностями обладают политики аудита?

8)Каким образом произвести запись всех попыток входа пользователей в систему?

9)Каким образом можно произвести запись всех попыток входа пользователей в систему?

10) Какие данные политики аудита могут пригодиться в случае, если в системе будет происходить что-то странное и необходимо выяснить причины возникших ситуаций?

11) Какая политика аудита позволяет проводить аудит системных событий перезагрузки, выключение компьютера и других важных сообщений, касающихся безопасности системы?:

12) Перечислите особенности аудита системы.

13) Каким образом просмотреть события, происходящие в системе?

14) Определите назначение программы *Event Viewer*.

15) Каким образом загрузит программу *Event Viewer*?

16) Дайте определение термину «лог-файл».

17) Какая информация находится в лог-файлах?

18) Перечислите типы протоколируемых системой событий в логах и их назначение.

19) Какой сервис ответственен за запись сообщений в лог системы?

20) Каким образом просмотреть свойства конкретного уведомления?

21) Перечислите и опишите информационные поля в описании события *Even*.

22) На каких типах событий следует сконцентрировать свое внимание?

23) С какими событиями (действиями) могут быть связаны сообщения системы безопасности *Аудит отказов*?

24) Какие действия следует предпринять при переполнении разделов лог-файла системы?

25) Каким образом просмотреть сохраненные события?

26) Определите назначение *Диспетчера задач*.

27) Перечислите функции *Диспетчера задач*.

28) Какие неприятности доставляют операционной системе зависшие программы, как их определить и как с ними бороться?

29) Каким образом идентифицировать процесс, происходящий в системе?

30) Что позволит в любой момент времени контролировать исполняющиеся процессы?

31) Поясните термин «имя исполняемого образа».

32) Каким образом в *Диспетчере задач* можно опре-

делить возможные атаки на систему (перечислите все сти *Диспетчера задач*)?

33) Каким образом определить в *Диспетчере задач*, в каком состоянии находится процесс (в состоянии ожидание, в состоянии исполнения или завис)?

34) По каким признакам в Диспетчере задач можно определить, что процесс завис?

35) По каким признакам с помощью *Диспетчера задач* можно определить, что процесс, запущенный в системе направлен на причинение ущерба системы?

36) Перечислите Ваши действия в случае обнаружения неизвестного Вам и системе процесса.

37) С помощью какого параметра можно найти нужный процесс в системе (при использовании программы *Диспетчер задач*)?

38) С помощью каких параметров в *Диспетчере задач* можно определить степень использования процессом центрального процессора?

39) Что могут означать «большие запросы к виртуальной памяти» и с помощью какого параметра *в Диспетчере задач* можно определить степень использования виртуальной памяти?

40) Какой приоритет имеет процесс *Idle.exe* и как определить в *Диспетчере задач* уровень приоритета процессов?

41) Какие неприятности ОС могут причинить большое количество процессов с уровнем приоритета *Средний*?

42) Как определить с помощью *Диспетчера задач,* какой активностью обладает процесс? Для какой цели нужна данная информация?

43) На что указывает большое количество потоков (>100) у процесса? Как определить количество потоков у процесса с помощью Диспетчера задач?

44) Как предотвратить возможные атаки на систему? Какие профилактические действия следует проводить для этих целей?

45) Что может означать ситуация, когда средняя загрузка системы составляет более пяти процентов? Какие программы имеют тенденцию находиться постоянно в системе?

46) Какая загруженность микропроцессора должна быть в идеале? Как определить загрузку системы с помощью *Диспетчера задач*?

47) Что означает ситуация, когда файл подкачки используется больше чем на половину при условии, что не были запущены большие программы?

48) Какая ситуация может произойти если количество дескрипторов, потоков и процессов будет слишком большим? Как определить эти параметры с помощью Диспетчера задач?

49) Что может означать ситуация, когда группа параметров *Выделение памяти* резко изменяются (раза в два). Какие действия следует предпринять в этом случае?

50) Каким образом можно дополнить отображаемые характеристики сетевых соединений в *Диспетчере задач*?

51) Что происходит, если в окне мониторинга сетевых соединений существует постоянная загрузка канала, равная определенному значению (при условии, что не были запущены сетевые программы и обновление операционной системы выключено)?

52) Каким образом можно с помощью *Диспетчера задач* идентифицировать пользователя в системе? Какие действия можно предпринять, если обнаружен неизвестный пользователь?

53) Какие дополнительные средства, связанные с функционированием системы, ее настройкой и конфигурацией в *Windows XP* Вы знаете?

54) Опишите работу программ для просмотра дополнительных внутренних параметров системы.

2) Задание.

1)Произвести настройку *аудита локальной системы* на своем ПК.

2)Просмотреть события, происходящие в Вашей системе.

3)Проанализировать текущие параметры Вашей системы.

4)Просмотреть состояние сетевых соединений в Вашей системы.

4.Порядок отчетности и форма контроля выполнения работы

Контроль выполнения задания производится по окончании занятия и на консультациях в форме защиты выполненной работы, предоставленной в электронном и в бумажном виде в форме «Отчет по лабораторной работе …».

5.Материально-техническое обеспечение.

Специализированная мебель и технические средства для представления учебной информации, включая проекционное оборудование; компьютерный класс с компьютерами AMD 2400 – 12 шт., оснащенными операционной системой Windows XP и пакетом Microsoft Office.

ЛАБОРАТОРНАЯ РАБОТА 8
ИСПОЛЬЗОВАНИЕ ПРОГРАММЫ MICROSOFT SECURITY ASSESSMENT TOOL (MSAT) ДЛЯ ОЦЕНКИ РИСКОВ

Цель занятия – приобретение обучаемыми необходимого объёма знаний и практических навыков для самостоятельной оценки рисков, связанных с информационной безопасностью.

Время – 4 часа.

Учебные вопросы:

1. Теоретическая часть:

1) Программа для самостоятельной оценки рисков, связанных с информационной безопасностью – Microsoft Security Assessment Tool (MSAT).

2. Практическая часть:

1) Вопросы по разделу.

2) Задание.

3) Порядок отчетности и форма контроля выполнения работы.

3. Материально-техническое обеспечение.

1. Теоретическая часть:

1) Программа для самостоятельной оценки рисков, связанных с информационной безопасностью – Microsoft Security Assessment Tool (MSAT).

В ходе данной лабораторной работы мы познакомимся с разработанной Microsoft программой для самостоятельной оценки рисков, связанных с безопасностью - Microsoft Security Assessment Tool (MSAT). Она бесплатно доступна на сайте Microsoft по ссылке

http://www.microsoft.com/downloads/details.aspx?displaylang=ru&FamilyID=cd057d9d-86b9-4e35-9733-7acb0b2a3ca1

Как отмечают разработчики, приложение предназначается для организаций с числом сотрудников менее 1000 человек, чтобы содействовать лучшему пониманию потенциальных проблем в сфере безопасности. В ходе работы, пользователь, выполняющий роль аналитика, ответственного за вопросы безопасности, отвечает на две группы вопросов.

Первая из них посвящена бизнес-модели компании, и призвана оценить риск для бизнеса, с которым компания сталкивается в данной отрасли и в усло- виях выбранной бизнес-

модели. Создается так называемый профиль риска для бизнеса (ПРБ).

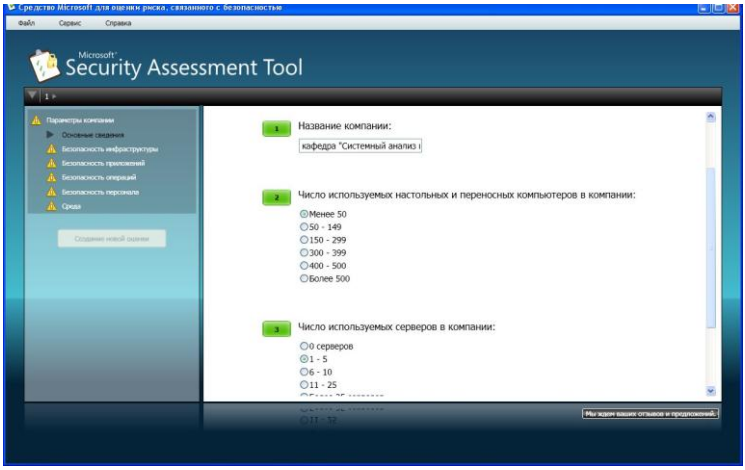


Рис.1. Информация о компании.

Вопросы этого этапа разбиты на 6 групп. Первая (рис. 1) касается общих сведений о компании – название, число компьютеров, серверов и т.д. Вторая группа вопросов озаглавлена «Безопасность инфраструктуры». Примеры вопросов – «использует ли компания подключение к Интернет», «размещаются ли службы, используемые как внешними, так и внутренними клиентами, в одном и том же сегменте» и т.д. Остальные группы – «Безопасность приложений», «Безопасность операций», «Безопасность персонала», «Среда».

Надо отметить, что при локализации не все вопросы первого этапа были качественно переведены с английского. Чего стоит вопрос: «Прошла ли ваша организация через «копирование и замена» касающиеся любого основного компонента технологии, за последние 6 месяцев?»! Однако во всех случаях можно из контекста понять, о чем идет речь (в приведенном примере вопрос был, относительно того, менялись ли используемые технологии обработки информации).

Когда проведен первый этап оценки, полученная информация обрабатывается (для этого требуется подключение к Интернет), после чего начинается второй этап анализа. Для технических специалистов он будет более интересен, т.к. касается используемых в компании политик, средств и механизмов защиты

(рис. 2). Стоит сказать, что и перевод вопросов второго этапа выполнен существенно лучше.

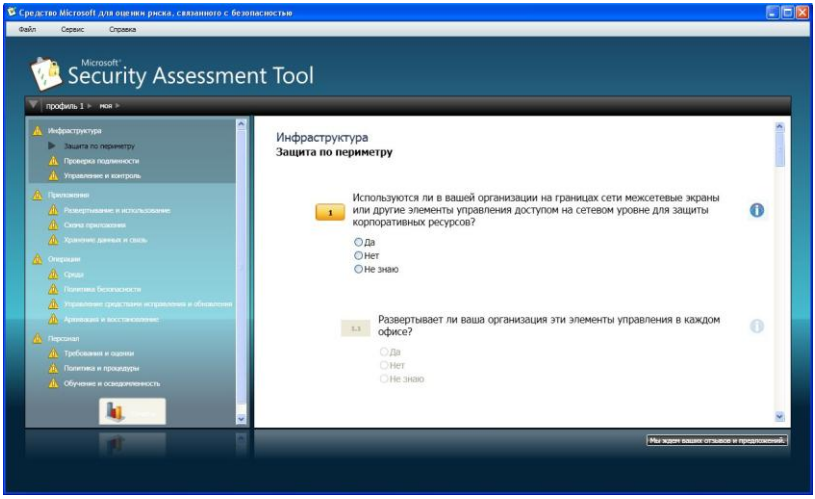


Рис. 2. Анализ используемых механизмов защиты.

Вопросы организованы в соответствии с концепцией многоуровневой (эшелонированной) защиты. Сначала рассматривается защита инфраструктуры (защита периметра, аутентификация…), затем вопросы защиты на уровне приложений, далее проводится анализ безопасности операций (определена ли политика безопасности, политика резервного копирования и т.д.), последняя группа вопросов касается работы с персоналом (обучение, проверка при приеме на работу и т.д.).

Во многом тематика вопросов соответствует разделам стандартов ISO 17799 и 27001, рассмотренных в теоретической части курса.

После ответа на все вопросы программа вновь обращается к удаленному серверу и генерирует отчеты. Наибольший интерес для технических специалистов представляет «Полный отчет». В частности, он содержит предлагаемый список приоритетных действий. Фрагмент списка представлен в таблице 1.

Таблица 1

Список предлагаемых действий

Список приоритетных действий	
Предмет анализа	***Рекомендация***
Высокий приоритет	
Операции > Управление средствами исправления и обновления > Управление средствами исправления	Наличие политики исправлений и обновлений для операционных систем является полезным начальным шагом, однако необходимо разработать такую же политику и для приложений. Разработайте такую политику, пользуясь сведениями, доступными в разделе, посвященном передовым методикам. Сначала установите исправления для внешних приложений и приложений Интернета, затем для важных внутренних приложений и, наконец, для не особо важных приложений.

2.Практическая часть

2) Вопросы по разделу:

1)Что включает использование программных средств для поддержки управления безопасностью?

2)В чём заключается программная поддержка работы с политикой безопасности?

3)В чём заключается программная поддержка анализа рисков?

4)В чём заключается интеграция программных средства в информационную систему предприятия?

5)Какие данные могут быть использованы для анализа поведения пользователей в информационной системе?

3) Задание.

1)Подробно опишите реально существующее или вымышленное малое предприятие: сферу деятельности, состав и структуру информационной системы, особенности организации процесса защиты информации, применяемые методы и средства.

2)С помощью программы MSAT проведите оценку рисков для предприятия.

3) Порядок отчетности и форма контроля выполнения работы

Контроль выполнения задания производится по окончании занятия и на консультациях в форме защиты выполненной работы, предоставленной в электронном и в бумажном виде в форме «Отчет по лабораторной работе …».

6. Материально-техническое обеспечение.

Специализированная мебель и технические средства для представления учебной информации, включая проекционное оборудование; компьютерный класс с компьютерами AMD 2400 – 12 шт., оснащенными операционной системой Windows XP и пакетом Microsoft Office.