Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра вычислительной техники и защиты информации

Ю.И. Синицын

КОМПЛЕКСНАЯ ЗАЩИТА РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ И ТЕЛЕКОММУНИКАЦИЙ

Методические указания

Рекомендовано к изданию редакционно-издательским советом федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет» для обучающихся по образовательной программе высшего образования по направлению подготовки 09.04.01 Информатика и вычислительная техника

Оренбург
2019

УДК 004.056(076.5)
ББК 32.971.3я7
С 38

Рецензент – доцент, кандидат технических наук Р. Р. Галимов

Синицын, Ю.И.
С 38 Комплексная защита распределенных информационно-вычислительных систем и телекоммуникаций: методические указания / Ю. И. Синицын; Оренбургский гос. ун-т. – Оренбург: ОГУ, 2019.

Методические указания предназначены для проведения лабораторных работ студентами, изучающими дисциплину «Комплексная защита распределенных информационно-вычислительных систем и телекоммуникаций». Выполнение лабораторных работ позволит изучить работу оборудования, необходимое для защиты компьютерных сетей.

Методические указания предназначены для студентов направления подготовки 09.04.01 Информатика и вычислительная техника.

УДК 004.056(076.5)
ББК 32.971.3я7

Содержание

Введение

Главная тенденция развития современного общества тесно связана с ростом информационной составляющей и, как следствие, информационной безопасности. Вопросы информационной безопасности на современном этапе рассматриваются как приоритетные в коммерческих фирмах, государственных структурах, в научных учреждениях. Информационные системы не могут оставаться в вопросах обеспечения информационной безопасности только на уровне традиционных средств: криптографическая защита, совершенствование систем разделения доступа, проведение организационных мероприятий по усилению режима.

Защита информации представляет собой многоцелевую проблему, часть которой еще даже не имеет четкой постановки. Наиболее разработаны вопросы защиты информации, содержащей государственную, коммерческую и прочие тайны.

В настоящее время выделяют организационно-правовую, программно-аппаратную и инженерно-техническую защиту информации. Организационно-правовая защита информации осуществляется путем выполнения требований и рекомендаций правовых документов. Программно-аппаратная защита занимается обеспечением средств вычислительной техники и автоматизированных систем от несанкционированного доступа и криптографической защитой циркулирующей в них информации. Защиту информации с помощью инженерных конструкций и технических средств обеспечивает инженерно-техническая защита информации.

Защита информации – важнейшая составляющая задачи обеспечения информационной безопасности, такая же, как обеспечение бесперебойной работы оборудования.

Поэтому при включении компьютера в сеть, при интеграции корпоративной информационной системы в сеть необходимо в первую очередь продумать вопросы обеспечения защиты этой системы.

Существующие на сегодняшний день методы и средства защиты информации в автоматизированных системах достаточно разнообразны, что, несомненно,

отражает многообразие способов и средств возможных несанкционированных действий.

Главным недостатком существующих методов и средств защиты информации, включая современные средства поиска уязвимостей автоматизированных систем и обнаружения несанкционированных действий, является то, что они, в подавляющем большинстве случаев, позволяют организовать защиту информации лишь от постфактум выявленных угроз, что отражает определенную степень пассивности обороны.

Адекватный уровень информационной безопасности в состоянии обеспечить только комплексный подход, предполагающий целенаправленное использование традиционных организационных и программно-технических правил обеспечения безопасности на единой концептуальной основе с одновременным поиском и глубоким изучением новых приемов и средств защиты.

1 Лабораторная работа № 1. Аудит комплексной защиты информации предприятия

Цель работы.

Изучение принципов организации, проектирования и анализа систем защиты информации и основ их комплексного построения на различных уровнях защиты.

Краткие теоретические сведения.

Аудит комплексной защиты информации является основой построения системы защиты информации предприятия. Для его проведения и получения достоверных результатов требуется, как правило, привлечение сторонних специализированных организаций.

При создании любой информационной системы (ИС) на базе современных компьютерных технологий неизбежно возникает вопрос о защищенности этой системы от внутренних и внешних угроз безопасности информации.

Но прежде чем решить, как и от кого защищать информацию, необходимо уяснить реальное положение в области обеспечения безопасности информации на предприятии и оценить степень защищенности информационных активов [1].

Для этого проводится комплексное обследование защищенности ИС (или аудит безопасности), основанные на выявленных угрозах безопасности информации и имеющихся методах их парирования, результаты которого позволяют:

– оценить необходимость и достаточность принятых мер обеспечения безопасности информации;

– сформировать политику безопасности;

– правильно выбрать степень защищенности информационной системы;

– выработать требования к средствам и методам защиты;

– добиться максимальной отдачи от инвестиций в создании и обслуживании СОБИ.

Комплексное обследование (аудит безопасности информации) защищенности представляет собой системный процесс получения и оценки объективных данных о

текущем состоянии обеспечения безопасности информации на объектах информатизации, действиях и событиях, происходящих в информационной системе, определяющих уровень их соответствия определенному критерию.

Комплексное обследование защищенности ИС (аудит) позволяет оценить реальное положение в области защиты информации и принять комплекс обоснованных управленческих решений по обеспечению необходимого уровня защищенности информационных активов предприятия.

Аудит защищенности ИС ставит своей целью методологическое обследование процессов, методов и средств обеспечения безопасности информации при выполнении информационной системой своего главного предназначения - информационное обеспечение бизнеса. При этом предполагается, что сама информационная система является оптимальной для решения бизнес задач.

Результатом аудита защищенности могут быть рекомендации по изменению инфраструктуры сети, когда по экономическим соображениям нецелесообразно или невозможностью достичь требуемого уровня защищенности информации при существующей инфраструктуре ИС [1].

Поскольку информационная безопасность должна быть обеспечена не только на техническом, но и на организационно-административном уровне, должный эффект может дать только комплексный подход к обследованию (аудиту), то есть:

1 Проверка достаточности принятых программно-аппаратных и технических мер защиты (соответствие установленным требованиям применяемых в ИС программно-аппаратных средств защиты).

2 Проверка достаточности инженерно-технических, правовых, экономических и организационных мер защиты (физической защиты, работы с персоналом, регламентации его действий).

Целью проведения работ по комплексному обследованию защищенности ИС является получение объективных данных о текущем состоянии обеспечения безопасности информации на объектах ИС, позволяющих провести минимизацию вероятности причинения ущерба собственнику информационных активов в результате нарушения конфиденциальности, целостности или доступности

информации, подлежащей защите, за счет получения несанкционированного доступа к ней, а также выработка комплекса мер, направленных на повышение степени защищенности информации ограниченного доступа.

Процесс комплексного обследования защищенности информационной системы состоит из трех основных частей:

1 Сбор необходимых исходных данных и их предварительный анализ (или стадия планирования).

2 Оценка соответствия состояния защищенности ИС предъявляемым требованиям и стандартам (стадии моделирования, тестирования и анализа результатов)

3 Формулирование рекомендаций по повышению безопасности информации в обследуемой ИС (стадии разработки предложений и документирования полученных результатов) [1].

На разных этапах обследования используются различные методы: технические, аналитические, экспертные, расчетные. При этом, результаты, полученные одними методами, могут дублироваться (дополняться) результатами, полученными другими методами. Совокупность всех применяемых методов позволяет дать объективную оценку состояния обеспечения безопасности информации на обследуемом объекте.

Основными группами методов при обследовании являются:

1 Экспертно-аналитические методы предусматривают проверку соответствия обследуемого объекта установленным требованиям по безопасности информации на основании экспертной оценки полноты и достаточности представленных документов по обеспечению необходимых мер защиты информации, а также соответствия реальных условий эксплуатации оборудования предъявляемым требованиям по размещению, монтажу и эксплуатации технических и программных средств.

2 Экспертно-инструментальные методы предполагают проведение проверки функций или комплекса функций защиты информации с помощью специального инструментария (тестирующих средств) и средств мониторинга, а также путем

пробного запуска средств защиты информации и наблюдения реакции за их выполнением. В процессе испытаний технических и программных средств используются тестирующие средства, принятые в установленном порядке.

3 Моделирование действий злоумышленника («дружественный взлом» системы защиты информации) применяются после анализа результатов, полученных в ходе использования первых двух групп методов, - они необходимы как для контроля данных результатов. Этим методом подтверждаются также реальные возможности потенциальных злоумышленников (как внутренних, легально допущенных к работе с тем или иным уровнем привилегий в ИС, так и внешних - в случае подключения ИС к глобальным информационным сетям). Кроме того, подобные методы могут использоваться для получения дополнительной исходной информации об объекте, которую не удалось получить другими методами.

Важным моментом является то, что применение методов моделирования действий злоумышленника ограниченно. При использовании данных методов необходимо учитывать, что при осуществлении тестовой атаки, используемое в ИС оборудование может быть выведено из строя, информационные ресурсы утрачены или искажены [1].

Задание на выполнение лабораторной работы.

Провести аудит комплексной защиты информации предприятия, где работает (работал) студент (магистр).

Порядок выполнения работы.

Работа состоит из следующих этапов:

1 Изучить теоретический материал.

2 Выполнить работу по аудиту комплексной защиты информации предприятия.

3 Проанализировать проделанную работу и предложить свой метод проведения аудита комплексной защиты информации на предприятии.

4 Результат отразить в отчете.

Содержание отчёта:

1 Цель работы.

2 Описание организации проведения Аудита на предприятии.

3 Формальный отчет по результатам Аудита.

4 Вывод, в котором предлагаются методы решения проблемы защиты информации.

2 Лабораторная работа № 2. Организация аттестации выделенного помещения по требованиям безопасности информации

Цель работы.

Провести аттестацию выделенного помещения на основе требований безопасности информации.

Краткие теоретические сведения.

Опыт организации специальных исследований говорит, что, с целью сокращения времени, перед проведением подготовительного этапа Заказчик должен подготовить следующие исходные данные:

1 Атрибуты объекта – т.е. полный адрес Заказчика, полное наименование объекта, а также его размещение (этаж, № или название помещения).

2 Контролируемая зона (КЗ) – Реквизиты документа, устанавливающего КЗ. Кроме этого должна быть дана планировка, определяющая размещение объекта на генплане, его месторасположение с указанием названия улиц, скверов и т.п. Минимальное расстояние от объекта до границы КЗ [2].

3 Установленная категория объекта.

4 Граничащие помещения (спереди, сзади, справа, слева, снизу, сверху).

5 Ограждающие конструкции (спереди, сзади, справа, слева, снизу, сверху). Необходимо по каждому направлению указать вид материала конструкции и его толщину. Если конструкция сложная, т.е. исполнение в несколько слоев, необходимо перечислить все слои с указанием толщины каждого. Указать наличие сквозных щелей и пустот в ограждающих конструкциях. Например: ограждающими конструкциями помещений являются железобетонные стены здания толщиной

500 мм (монолитный железобетон) и внутренние перегородки в капитальном исполнении (в один кирпич, 250 мм). Перегородка комнаты отдыха кабинета заместителя руководителя с залом заседаний выполнена из двух слоѐв оргалита (6 мм) на деревянном каркасе (брус 5-50 мм). Перекрытия пола и потолка железобетонные (стандартные плиты пустотелого железобетона 305 мм).

6 Наличие фальшпола и фальшпотолка (с указанием модели, материала, толщины и расстояния от перекрытия до фальшпола/потолка).

7 Описание дверей помещения (материал, размеры, двойные/одинарные, одностворчатые/двухстворчатые, наличие порога и его высота).

8 Описание окон помещения (материал, размеры, двойные/одинарные, толщина остекления). Куда выходят окна – внутренний двор, улица и т. п.

9 Система отопления. Где расположен тепловой пункт. Как построена система отопления (тип радиаторов отопления, как осуществляется подача (розлив) теплоносителя, количество радиаторов, количество стояков отопления в помещении).

10 Система водоснабжения (описание аналогично системе отопления).

11 Система вентиляции (количество вентиляционных каналов, сечение коробов и их местопрохождение с указанием ближайших выходов в другие помещения).

12 Описание применяемых средств защиты (марка, вид аппаратуры защиты, места установок датчиков и т.п.).

На подготовительном этапе проводится качественная оценка вибро- и звукоизоляции помещения с целью определения наиболее вероятных разведопасных направлений. Анализируются архитектурно-планировочные решения помещения, конструктивные особенности его ограждающих конструкций (стен, перекрытий, дверей, окон) и инженерно-технических систем. Обследуются коммуникации трубопроводов различных систем жизнеобеспечения, выявляются неоднородности в ограждающих конструкциях, обследуются конструктивные особенности элементов отделки [2].

Уточняются пространственные соотношения ограждающих конструкций

помещения и элементов технических систем относительно установленной границы контролируемой зоны и относительно прилегающих к контролируемой зоне зданий, строений и пр.

Оценивается (или уточняется) степень секретности речевой информации (категории объекта защиты) и определяется необходимое значение нормированного показателя противодействия акустической речевой разведке, на соответствие которому необходимо проводить инструментальный контроль.

Уточняются условия речевой деятельности в контролируемом помещении. Проводится слуховой (качественный) контроль звукоизоляции ограждающих конструкций путем прослушивания сигналов, формируемых в контролируемом помещении. В качестве таких сигналов рекомендуется использовать естественную речь, записанную, например, на магнитофон.

Пример исходных данных для составления плана поиска.

(В работе составляются самостоятельно путем осмотра выделенного помещения и прилегающей территории)

Представитель ОАО ХХХ , как представитель Заказчика, представил следующие исходные данные на исследуемое помещение:

1 Атрибуты объекта – ОАО ХХХ , г. Оренбург, ул. Строителей, дом №.., расположено на первом этаже 3-х этажного здания. На 2-ом и 3-ем этажах расположены сторонние организации. Имеется общая охраняемая территория. Допуск посторонних лиц и автомашин только с согласия руководителя ОАО ХХХ и руководителей сторонних организаций. Все сотрудники ОАО ХХХ имеют допуск не ниже третьего. Сторонние организации с гостайной не работают. В ОАО ХХХ имеется одно выделенное помещение (ВП) – кабинет руководителя. Планируется аттестовать в качестве выделенного помещения – помещение для переговоров.

2 Контролируемая зона (КЗ) объекта проходит по ограждающим конструкциям третьего этажа, за исключением лестницы на верхние этажи. Исследуемое ВП – переговорная - граничит с КЗ по одной стене, на которой расположено одно окно и дверь, и по потолку. Средства звукоусиления в переговорной отсутствуют. Источник речи не локализован.

3 Помещению планируется установить 2-ую категорию.

4 Граничащие помещения (спереди, сзади, справа, слева, снизу, сверху).

5 Ограждающие конструкции:

Стены 1 и 2 выполнены из кирпича. Толщина 2,5 кирпича. Внутренняя штукатурка толщиной 1см.

Боковые стены 3 и 4 выполнены из кирпича. Толщина 1 кирпич. Внутри и снаружи штукатурка толщиной 1см.

Пол и потолок выполнены из стандартных бетонных плит перекрытия толщиной 30 см. Подвала нет. Сквозных щелей и пустот не обнаружено. Пол деревянный на лагах, покрыт линолеумом. Фальшпотолка нет.

6 Двери двойные с тамбуром. Ширина тамбура – 0,5 м. По периметру каждой двери проложен уплотнитель. Двери тяжелые деревянные. Дверные коробки отделены друг от друга и от стены резиновыми уплотнителями. Дверь выходит на границу КЗ.

7 Окно пластиковое в специальном исполнении. Рама окна отделена от стены резиновыми прокладками. Окно граничит с КЗ.

8 В помещении имеется одна батарея отопления. Трубы системы отопления выполнены из металлопластика. Ввод трубы системы отопления осуществлен со второго этажа, выход трубы идет под пол. Тепловой пункт размещен за пределами КЗ. Таким образом, система отопления имеет выход за пределы КЗ.

9 Система вентиляции выполнена в виде вентиляционных коробов и имеет ближайший выход в общий коридор первого этажа и затем выходит на второй и третий этаж (по легенде).

10 На элементах ограждающих конструкций и инженерных коммуникаций имеются средства активной защиты [2].

Порядок выполнения работы:

1 Составить самостоятельно (или получить у преподавателя) документацию на контролируемое помещение, изучить ее, определить возможные разведопасные направления и возможные виды разведки.

2 Изобразить план-схему исследуемого помещения.

3 На основании нижеприведенной методики, составить план проведения визуального осмотра помещения и выявить объекты, требующие при обследовании использования имеющихся средств видеонаблюдения и металодетектора.

4 Сделать выводы по результатам проделанной работы и подготовить отчет.

Методика проведения осмотра помещений.

Ниже приведены общие рекомендации по поиску устройств негласного съема информации. Всю процедуру поиска можно условно разбить на несколько этапов:

– подготовительный этап;
– физический поиск и визуальный осмотр;
– обнаружение радио-закладных устройств;
– выявление технических средств с передачей информации по токоведу-
– щим линиям;
– обнаружение ЗУ с передачей информации по ИК-каналу;
– проверка наличия акустических каналов утечки информации.

Подготовительный этап.

Предназначен для определения глубины поиска, а также формирования перечня и порядка проводимых мероприятий Он включает в себя следующие элементы:

1 Оценку возможного уровня используемых технических средств. Объем проводимых мероприятий существенным образом зависит от того, в чьих интересах они проводятся.

2 Анализ степени опасности, исходящей от своих сотрудников и представителей соседних организаций.

3 Оценку возможности доступа посторонних лиц в помещения.

4 Изучение истории здания, в котором планируется проводить поисковые мероприятия. Оценивается возможность установки закладок как во ремя строительства, так и оставления их в наследство от предыдущих обитателей.

5 Определение уровня поддерживаемой безопасности в соответствии с экономическими возможностями и степенью желания заказчика, а также фактической необходимостью.

6 Выработку плана действий, который должен отвечать следующим условиям:

– время поиска должно приходиться на рабочие часы, когда ЗУ активизированы;

– должны быть созданы условия, провоцирующие к действию возможно внедренные жучки, поскольку в них могут быть использованы как устройство автоматического включения передатчика при появлении акустического сигнала (схемы VOX) и включающие устройства только при определенном уровне акустического сигнала, так и системы дистанционного управления (проведение фиктивных, но правдоподобных деловых переговоров — хороший повод, чтобы побудить противоположную сторону активизировать свои устройства);

– должна быть обеспечена скрытность проводимых мероприятий — если есть необходимость ведения своей контрразведывательной игры, то следует помнить, что разговоры с коллегами и заказа ком, приход, развертывание аппаратуры, характерный шум поиска раскрывают содержание и результат проводимых мероприятий;

– неожиданность — поиск следует проводить регулярно, но через случайные промежутки времени [2].

Физический поиск и визуальный осмотр.

Физический поиск и визуальный осмотр является важным элементом выявления средств негласного съема информации, особенно таки как проводные и волоконно-оптические микрофоны, пассивные и полуактивные радио-закладные устройства, дистанционно управляемые ждущие устройства и другие технические средства, которые невозможно обнаружить спомощью обычной аппаратуры.

Проведение поисковых мероприятий следует начинать с подготовки помещения, подлежащего проверке:

1 Необходимо закрыть все окна и занавески для исключения визуального контакта.

2 Включить свет и все обычные офисные устройства, характерные для данного помещения.

3 Включить источник известного звука (тестового акустического сигнала) в центре зоны контроля. Во время поиска он будет выполнять важные функции: маскировать большинство шумов, производимых во время физического поиска; работать как источник для звуковой обратной связи, необходимой для выявления радио-микрофонов; активизировать устройства, оснащенные системой VOX. Источник известного звука не должен настораживать противоположную сторону, следовательно, это может быть любой плейер. Необходимо только помнить, что лучшие результаты достигаются при использовании аппаратуры средних размеров. Это объясняется оптимальными размерами громкоговорителя. Выберите наиболее уместную в данной ситуации запись, будь то музыка, бизнес-семинар или курс самообучения. Подберите соответствующую длительность, поскольку качественный поиск может занять много часов.

Примечание: в качестве источника известного звука не рекомендуется использовать радиоприемник, поскольку эту же станцию может поймать и ваша поисковая аппаратура, что может привести к ошибке и радиостанция будет зафиксирована как нелегальный радиопередатчик.

4 За пределами зоны контроля (в незащищенной комнате/зоне) как можно более бесшумно разверните вашу аппаратуру. Незащищенная зона — это место, которое не вызывает интереса у противоположной стороны и не контролируется ею, поэтому ваши действия останутся скрытыми.

5 Установите обычный уровень радиоизлучения окружающей среды

перед поиском в зоне контроля [2].

Основные процедуры поиска.

Визуально, а также с помощью средств видеонаблюдения и металлодетекторов, обследуйте все предметы в зоне контроля, размеры которых достаточно велики для того, чтобы можно было разместить в них технические средства негласного съема информации. Тщательно осмотрите и вскройте, в случае необходимости, все настольные приборы, рамы картин, телефоны, цветочные горшки, книги, питаемые от сети устройства (компьютеры, ксероксы, радиоприемники и т. д.).

Для поиска скрытой проводки обследуйте плинтуса и поднимите ковровые покрытия. Тщательно осмотрите потолочные панели, а также все устройства, содержащие микрофоны, магнитофоны и камеры.

С особой тщательностью обследуйте места, где ведутся наиболее важные переговоры (обычно это стол с телефоном). Большинство нелегальных устройств располагаются в радиусе 7 м от этого места для обеспечения наилучшей слышимости и (или) видимости.

Если вы при этом используете металлодетектор, то скрупулезно выполняйте требования его инструкции на эксплуатацию.

Особо следует обратить внимание на проверку телефонных линий, сетей пожарной и охранной сигнализации. Следует обязательно разобрать телефонный аппарат, розетки и датчики и искать детали, непохожие на обычные, с разноцветными проводами и спешной или неаккуратной установкой.

Затем осмотрите линию от аппарата (датчика) до стены и, удалив стенную панель, проверьте, нет ли за ней нестандартных деталей.

Проведите физический поиск в коммутационных панелях и коммуникационных каналах, в случае необходимости используйте эндоскопические и портативные телевизионные средства видеонаблюдения. Проверьте места входа/выхода проводов внутри и снаружи здания.

С целью облегчения последующих поисковых мероприятий после завершения всех работ скрытно пометьте шурупы на стенных панелях, сетевых розетках, телефонных корпусах и других местах, куда могут быть установлены закладки. Тогда при проведении повторных проверок видимые в ультрафиолетовых лучах метки покажут нарушение целостности ранее обследованного объекта, если оно имело место, а соответствующие записи в ашем журнале проверок помогут сориентироваться в будущей работе. Для контроля изменений в окружающих устройствах очень удобны ультрафиолетовые маркеры.

При проведении поиска ЗУ в автомобиле тщательно осмотрите не только салон, но и раму автомашины, багажник и т. п., внимательно проверьте цепи, имеющие выход на автомобильную антенну. При проведении этих операций досмотровые портативные телевизионные системы также могут оказаться очень полезными [2].

Содержание отчёта:

1 Цель работы.

2 Выполнить требования стандартов по оформлению отчетов (ЕСКД, ЕСПД) в соответствии с образцами типовых форм отчетных документов, приведенными в приложении.

3 Использовать рабочие материалы, подготовленные на этапе, предшествующем выполнению лабораторной работы.

4 Результаты выполнения работы.

5 Выводы.

3 Лабораторная работа № 3. Работа с сетевым экраном DFL-260E. Создание и обновление конфигурационного файла межсетевого экрана

Цель работы.

Изучение интерфейса и основных команд межсетевого экрана DFL-260E.

Задание на выполнение лабораторной работы:

1 Создание резервной копии настроек.

2 Обновление аппаратного обеспечения.

Порядок выполнения работы.

Откройте web-браузер и введите IP-адрес межсетевого экрана в адресную строку (по умолчанию, 192.168.**10.1**). Нажмите на **Enter**.

По выполнению на экране появится окно, как на рисунке 1.

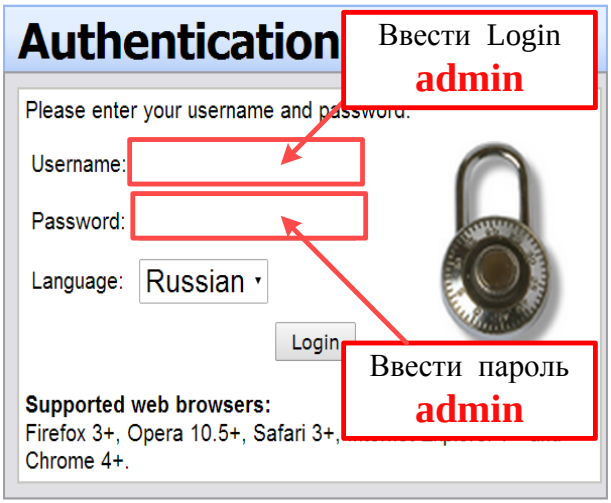

Рисунок 1 – Окно web-браузера

Имя пользователя - **admin** и пароль - **admin**. После ввода пароля нажмите **«Enter»** , как на рисунке 2.

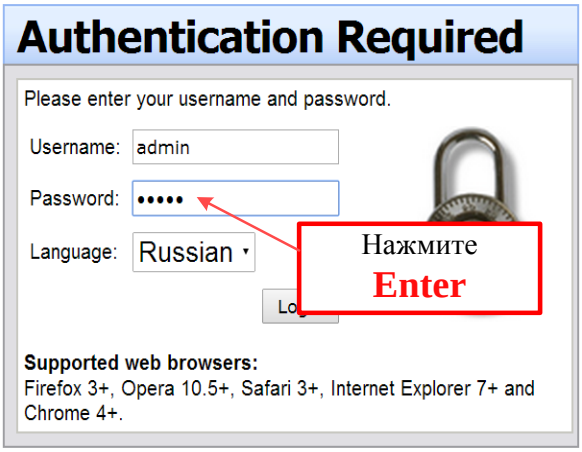

Рисунок 2 - Окно web-браузера

Появится общее **«Меню»**, как на рисунке 3.

Установите указатель ее вкладку **«Обслуживание» (Maintenance)**.

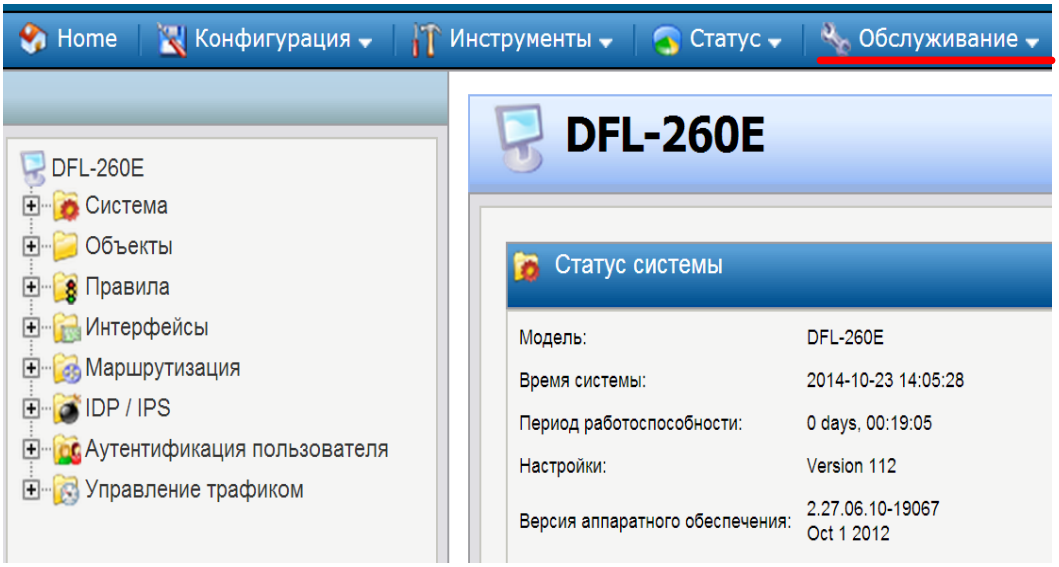

Рисунок 3 – Окно общего «Меню»

Задача № 1. Создание резервной копии настроек.

Кликните по вкладке **«Обслуживание» (Maintenance)**. Появится выпадающее подменю, показанное на рисунке 4.

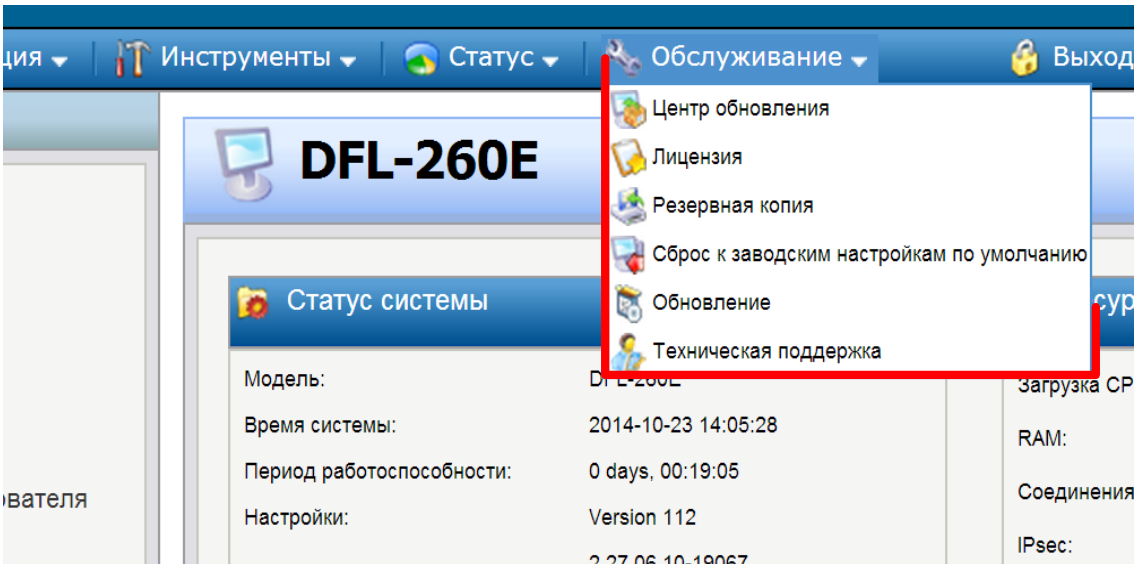

Рисунок 4 - Вкладка «Обслуживание»

Указателем «кликаем» по опции **«Резервная копия»**, как на рисунке 5.

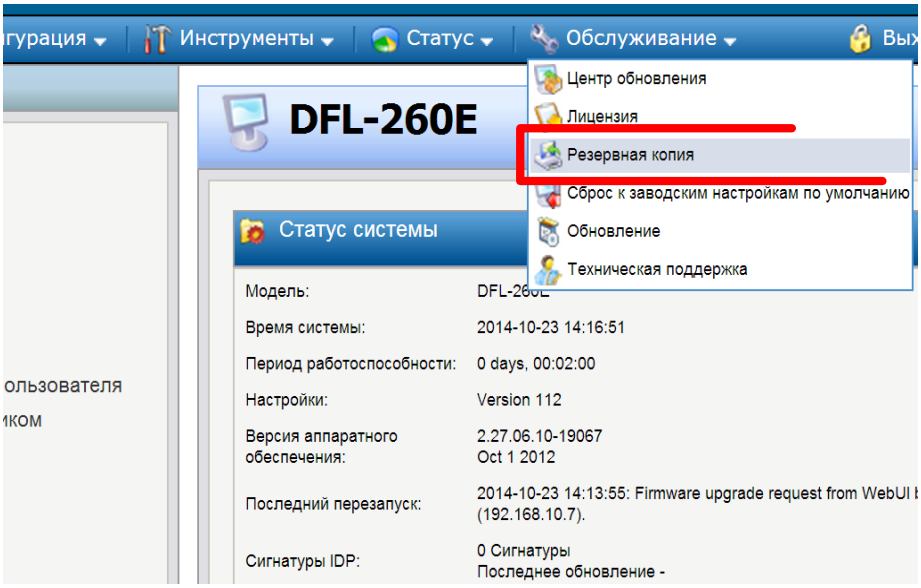

Рисунок 5 - Вкладка «Обслуживание» - «Резервная копия»

Кликаем **«Резервная копия настроек»** , как на рисунке 6.

Выпал файл *.bak.

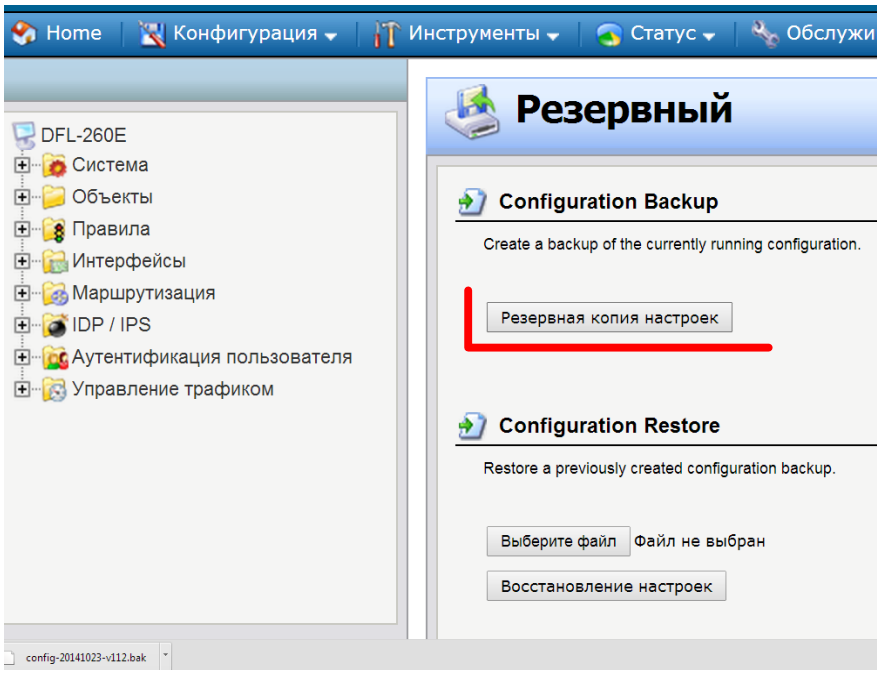

Рисунок 6 - Вкладка «Резервная копия» - «Резервная копия настроек»

Нажимаем «Выберите файл», как на рисунке 7.

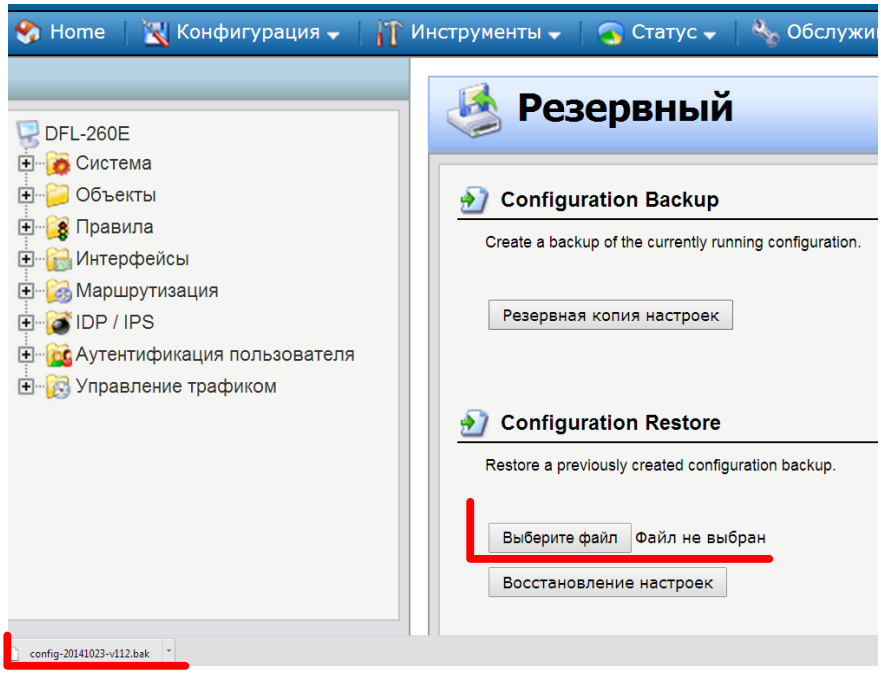

Рисунок 7 – Выбор файла

Выбираем файл, который выпал, как на рисунке 8.

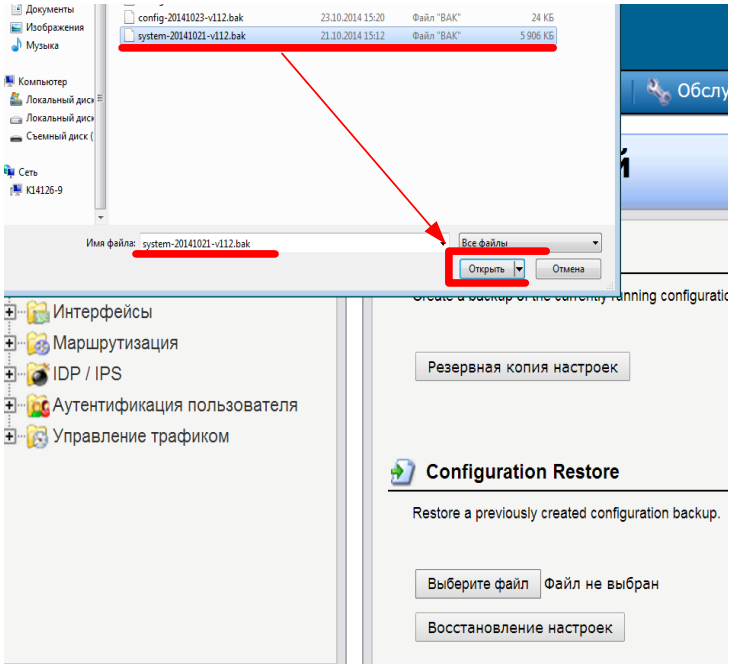

Рисунок 8 – Выбор файла

Нажимаем **«Открыть».**

Файл настроек для резервного копирования готов, как на рисунке 9.

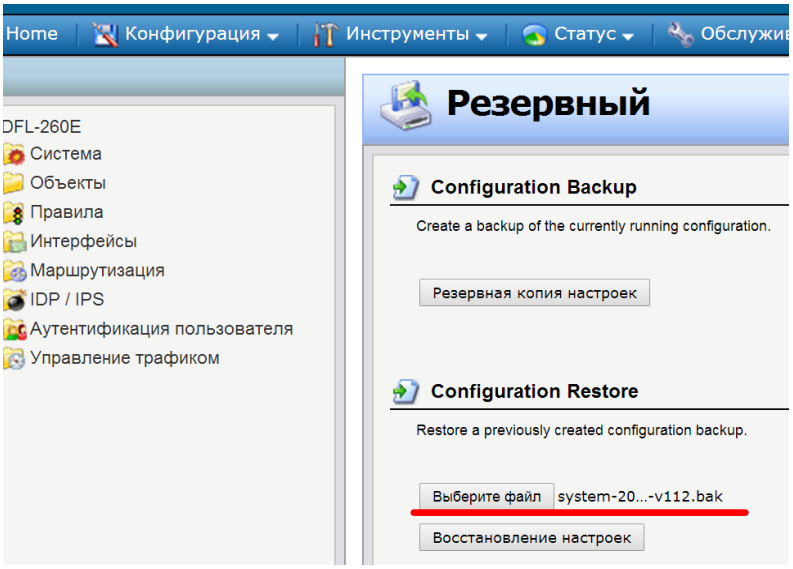

Рисунок 9 - Открываем файл

Записываем файл настроек на диск, как на рисунке 10.

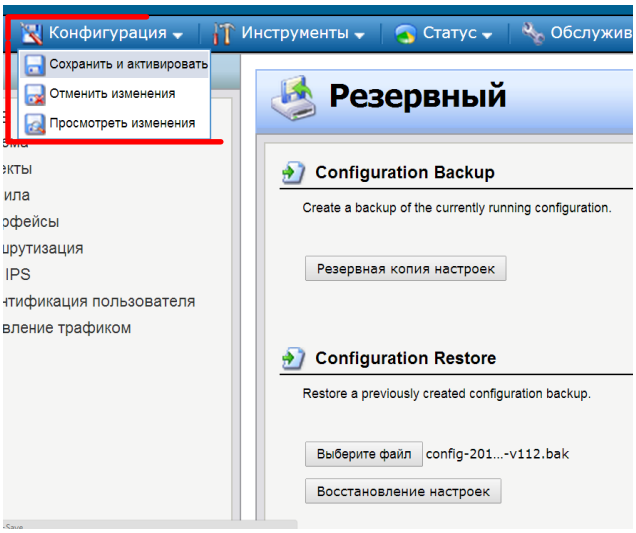

Рисунок 10 - Записываем файл настроек на диск

Работа завершена.

Пригласите **преподавателя** для **визуального контроля** за результатом выполнения работы.

Задачи № 2. Обновление аппаратного обеспечения.

Установите указатель на вкладку **«Обслуживание» (Maintenance)**, как на рисунке 11.

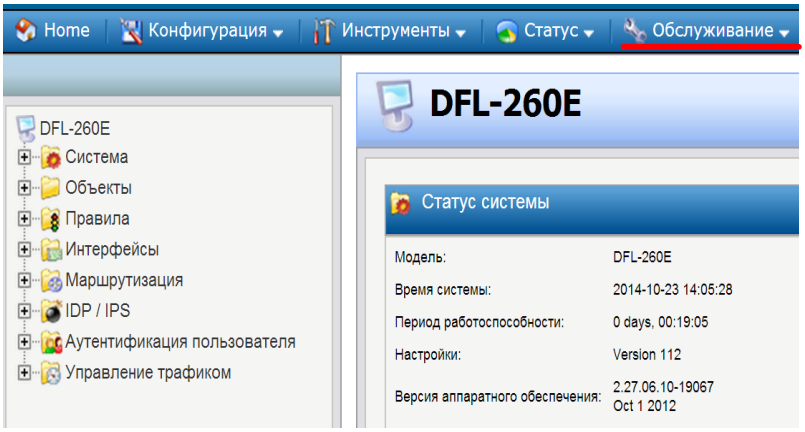

Рисунок 11 - Указатель на вкладку «Обслуживание»

Кликните по вкладке **«Обслуживание» (Maintenance)**, как на рисунке 12. Появится выпадающее подменю.

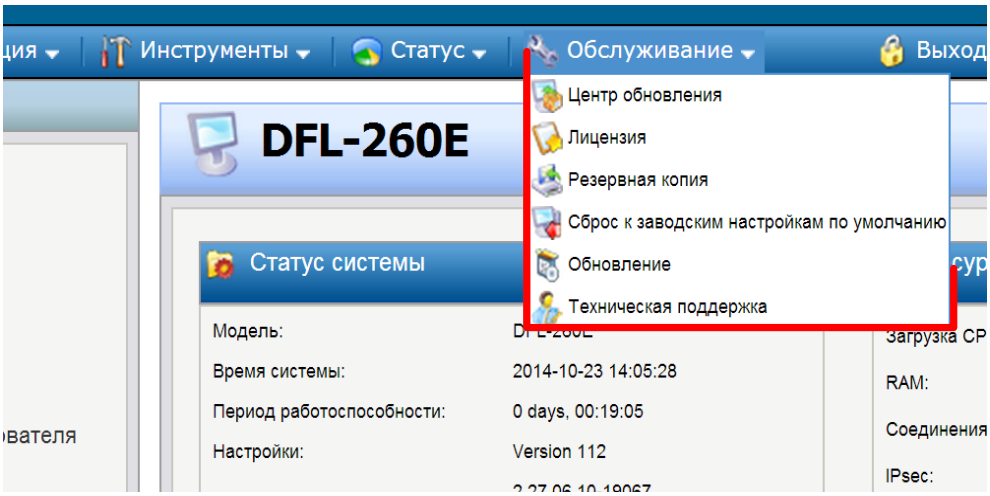

Рисунок 12 - Вкладка «Обслуживание»

Указателем «кликаем» по опции **«Обновление»**, как на рисунке 13.

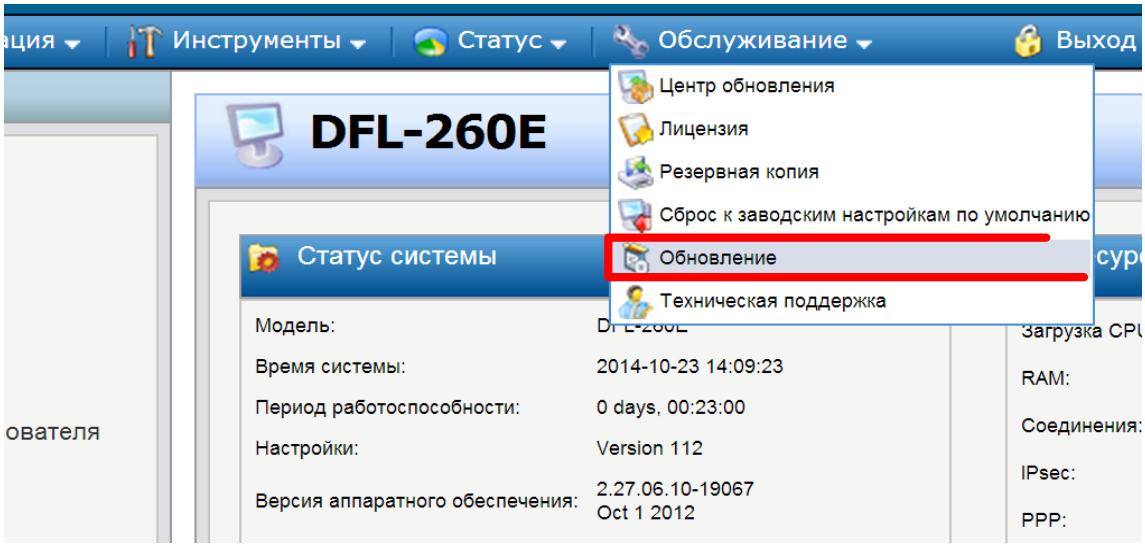

Рисунок 13 - Опция «Обновление»

Появляется окно **«Обновить»**, как на рисунке 14.

Здесь показано, не выбран файл обновления.

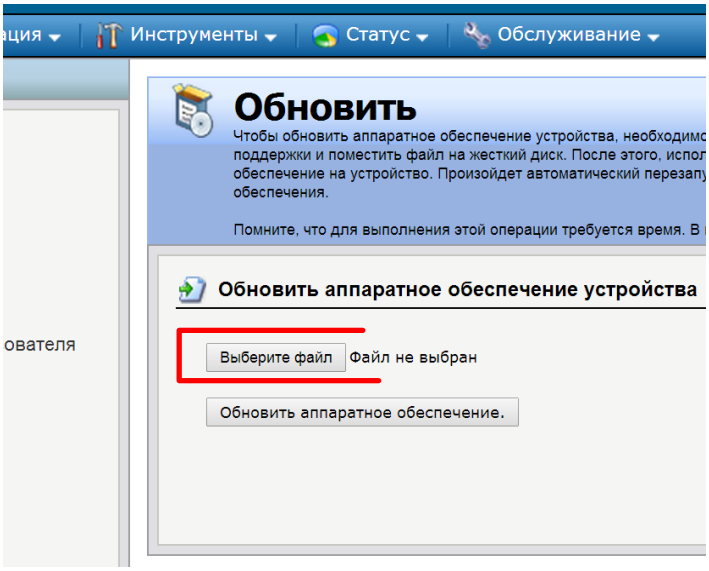

Рисунок 14 - Окно «Обновить»

Устанавливаем указатель на кнопку **«Выберите файл»**, и жмем левую кнопку мышки.

Появится всплывающее «подменю», как на рисунке 15.

Выбираем файл и жмем **«Открыть»**.

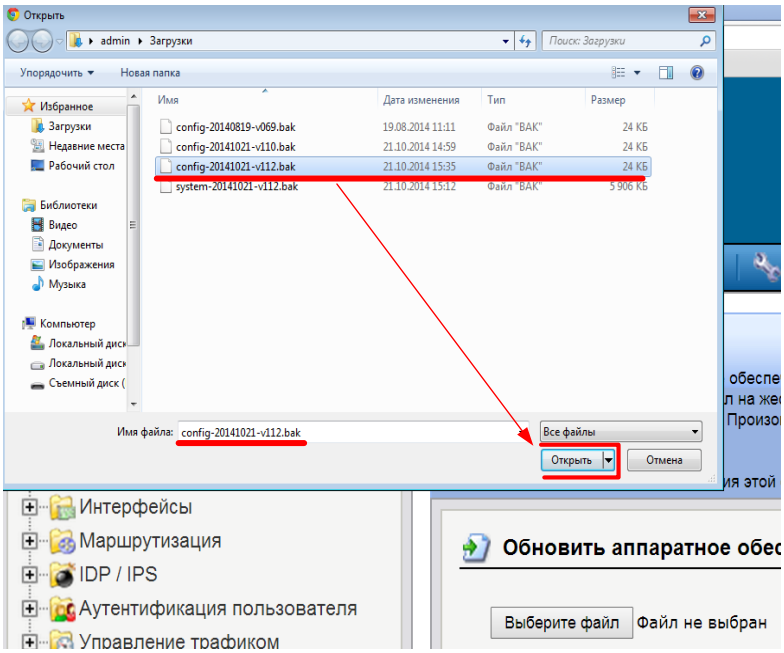

Рисунок 15 – Открываем файл

Появится окно **«Обновить»** с выбранным файлом конфигурации, как на рисунке 16.

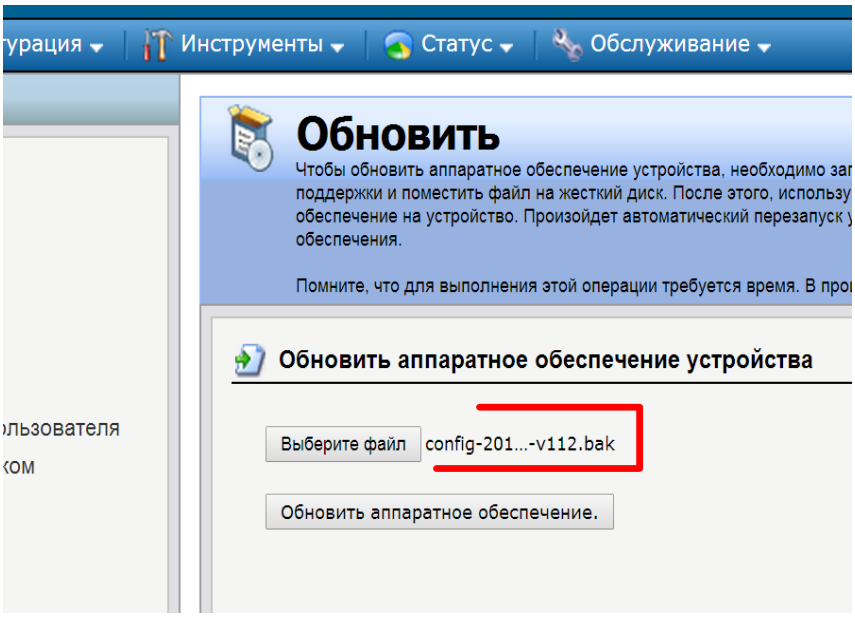

Рисунок 16 - Окно «Обновить»

Активируем кнопку **«Обновить аппаратное обеспечение»**, как на рисунке 17.

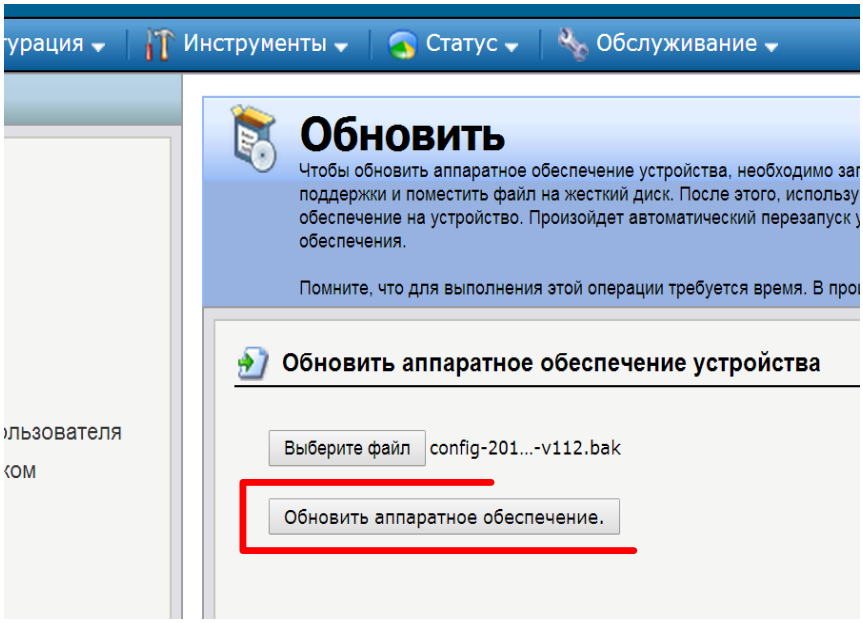

Рисунок 17 - Активация «Обновить аппаратное обеспечение»

Если все этапы проведены правильно – появится окно с комментарием – **«Загрузка аппаратного обеспечения завершена»**, как на рисунке 18.

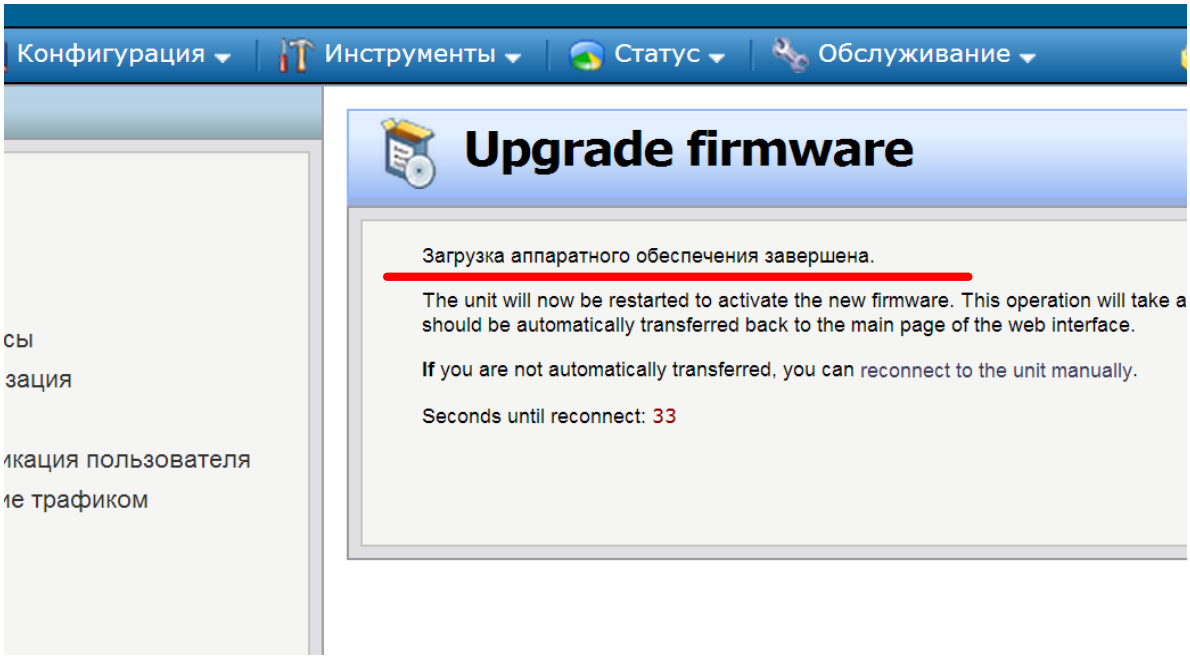

Рисунок 18 - Окно с комментарием – «Загрузка аппаратного обеспечения завершена»

Работа завершена.

Пригласите **преподавателя** для **визуального контроля** за результатом выполнения работы.

Содержание отчета:

1 Название и цель работы.

2 Показать основные шаги и этапы проведения лабораторной работы.

3 Представить основные экранные формы процесса работы.

4 Представить результаты работы.

5 Выводы по выполненной работе.

6 Список использованных источников.

4 Лабораторная работа № 4. Фильтрация Web-содержимого трафика

Цель работы.

Получение практических навыков и теоретических знаний при настройка «**черного списка**» URL-адресов.

Задание на выполнение лабораторной работы.

Заблокировать весь web-сайт http://www.osu.ru/.

Краткие теоретические сведения.

Web-трафик является одним из крупнейших источников нарушения безопасности и неправомерного использования сети Интернет. Просмотр Web-страниц может стать причиной угрозы безопасности сети. Производительность и пропускная способность Интернет-каналов также может быть нарушена.

Механизмы фильтрации.

С помощью HTTP ALG межсетевой экран применяет следующие механизмы фильтрации сомнительного Web-содержимого.

Функция ***Active Content Handling*** может использоваться для фильтрации web-страниц с содержимым, рассматриваемым администратором как потенциальная угроза, например, объекты ActiveX и Java Applets.

С помощью функции ***Static Content Filtering*** (фильтрация статического содержимого) можно вручную классифицировать web-сайты на разрешенные и запрещенные. Эта функция также известна как «белый/черный список» URL-адресов.

Dynamic Content Filtering (фильтрация динамического содержимого) – это эффективная функция, позволяющая администратору разрешать или блокировать доступ к Web-сайтам в зависимости от категории их классификации, выполненной службой автоматической классификации. Фильтрация динамического содержимого требует минимум усилий администратора и обеспечивает высокую точность.

Алгоритм для настройки фильтрации на основе белого или черного списка представлен на рисунке 20.

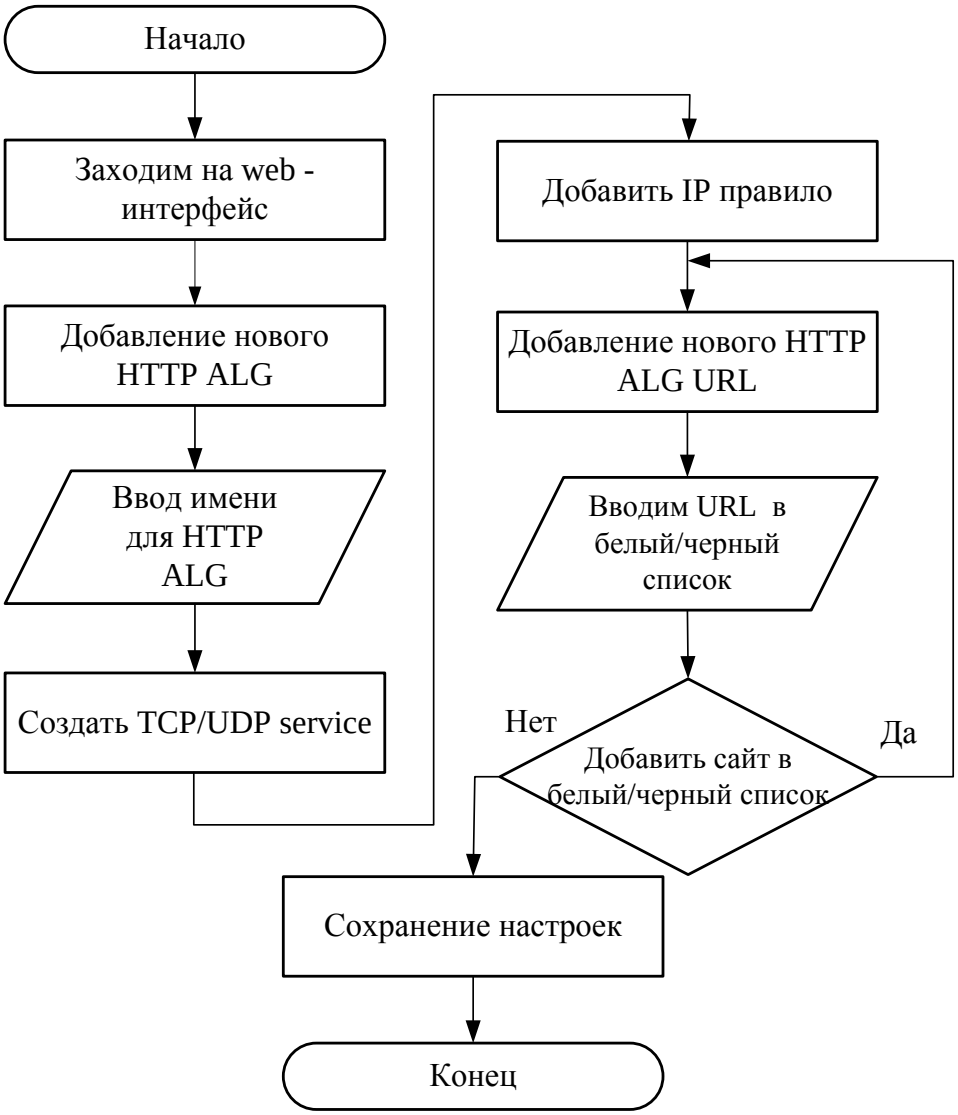

Рисунок 20 – Настройка фильтрации web-страниц

И черный, и белый списки URL-адресов поддерживают метод подстановки URL-адреса для обеспечения наибольшей гибкости использования. Этот метод также применим к имени пути в URL-адресе хоста, что означает, что фильтрацией можно управлять на уровне файлов и папок.

В таблице 1 приведены корректные и некорректные примеры использования URL-адресов в «черном списке».

Таблица 1 – Примеры использования URL-адресов

Пример	Описание
.example.com/	Корректно. Блокировка всех хостов в домене example.com и всех Web-страниц, используемых этими хостами
www.example.com/*	Корректно. Блокировка Web-сайтов www.example.com и всех Web-страниц
/.gif	Корректно. Блокировка всех файлов с расширением «.gif»
www.example.com	Некорректно. Блокировка только первого запроса доступа на Web-сайт. Доступ, например на www.example.com/index.html, не будет заблокирован
example.com/	Некорректно. Блокировка доступа на www.myexample.com, так как будет запрещен доступ на все сайты, имя которых заканчивается на example.com.

Порядок выполнения работы.

Откройте web-браузер и введите IP-адрес межсетевого экрана в адресную строку (по умолчанию, 192.168.**10.1**). Нажмите на **Enter.**

По выполнению на экране появится окно, как показано на рисунке 21.

Рисунок 21 - Окно web-браузера

Имя пользователя - **admin** и пароль - **admin**. После ввода пароля нажмите **«Enter»**, как показано на рисунке 22.

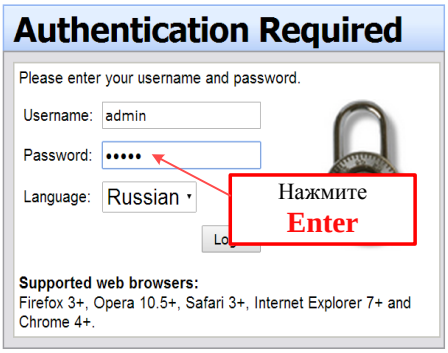

Рисунок 22 - Окно web-браузера

Появится общее **«Меню»**, как показано на рисунке 23.

Работаем с **древовидным «Меню»** в левом окне.

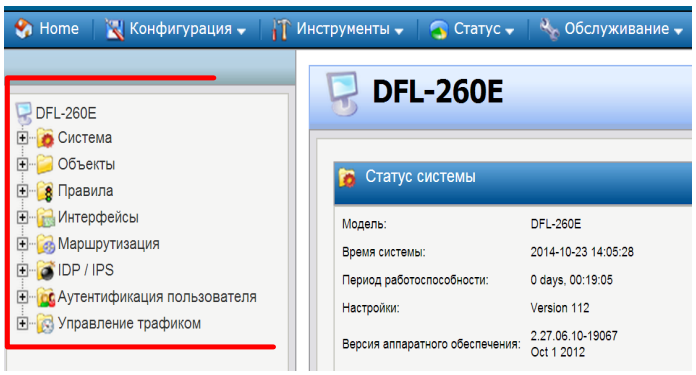

Рисунок 23 - Окно общего «Меню»

Кликните по знаку «+» рядом с папкой **«Объекты»**, как показано на рисунке 24. Создание ***объекта HTTP ALG.***

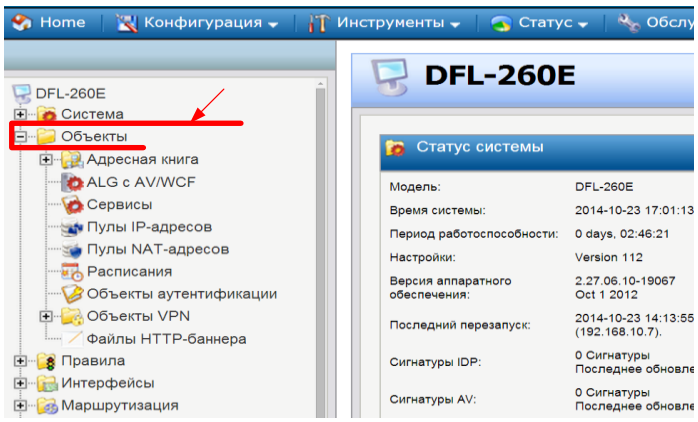

Рисунок 24 – Вкладка «Объекты»

Заходим **«Объекты ->ALG»**. Вкладка «Объекты» - ALG на рисунке 25.

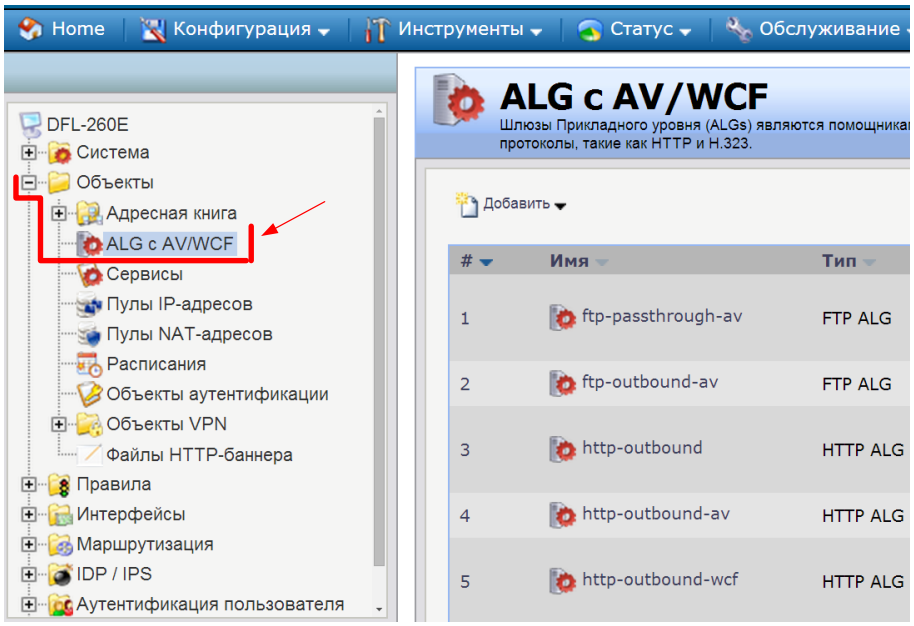

Рисунок 25 - Вкладка «Объекты» - ALG

Добавляем новый **HTTP ALG**. Вкладка «Объекты»-HTTP ALG на рисунке 26. **Добавить.**

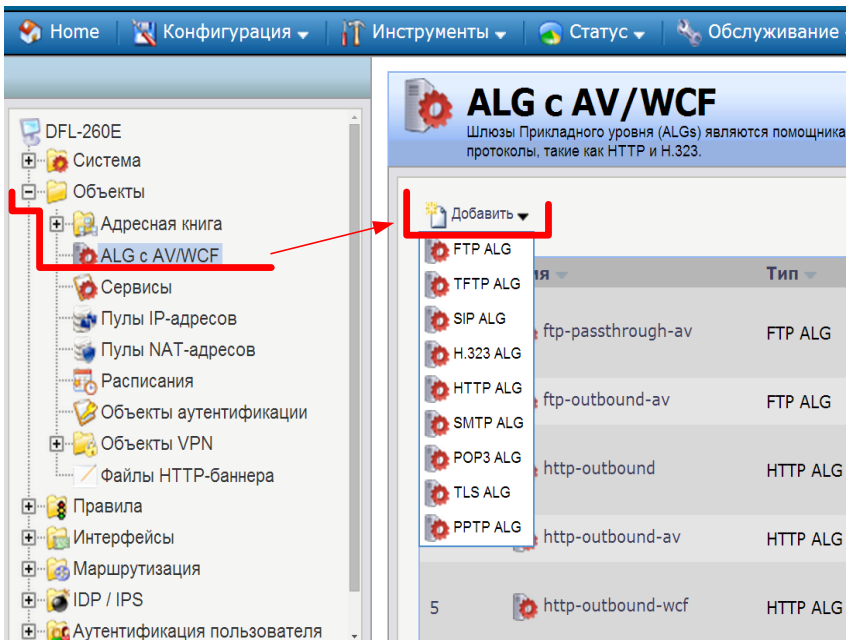

Рисунок 26 - Вкладка «Объекты» - HTTP ALG

Выбор протокола *HTTP ALG.* Создание объекта HTTP ALG показано на рисунке 27.

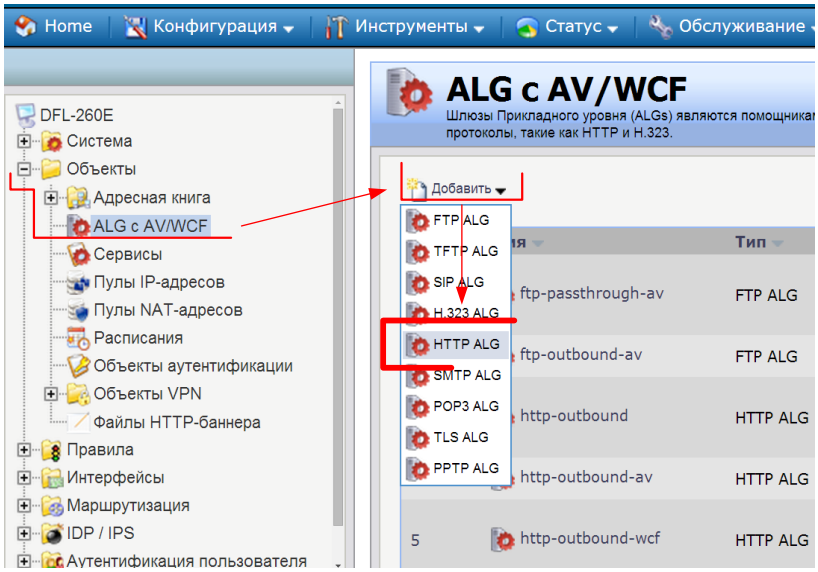

Рисунок 27 – Создание объекта HTTP ALG

HTTP ALG – это расширенная подсистема в межсетевом экране, состоящая из опций фильтрации статического и динамического содержимого.

Получили создание объекта HTTP ALG**, как на рисунке 28.**

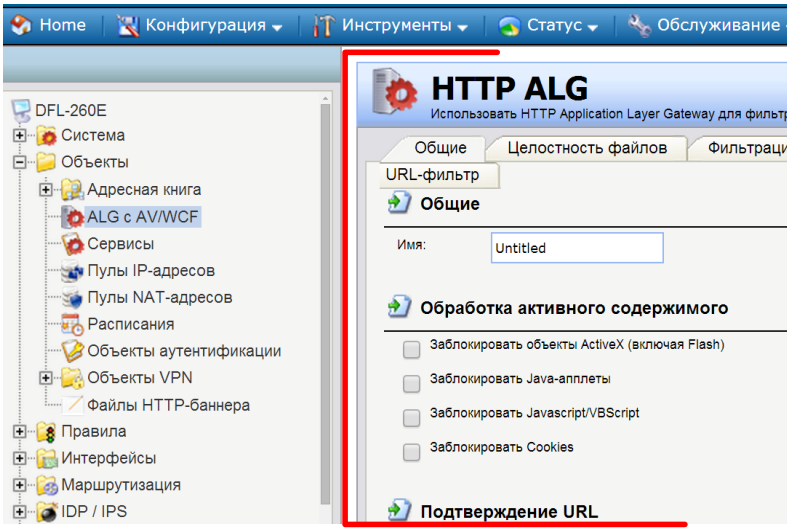

Рисунок 28 - Создание объекта HTTP ALG

Вводим имя для нового объекта **Vt**, как на рисунке 29.

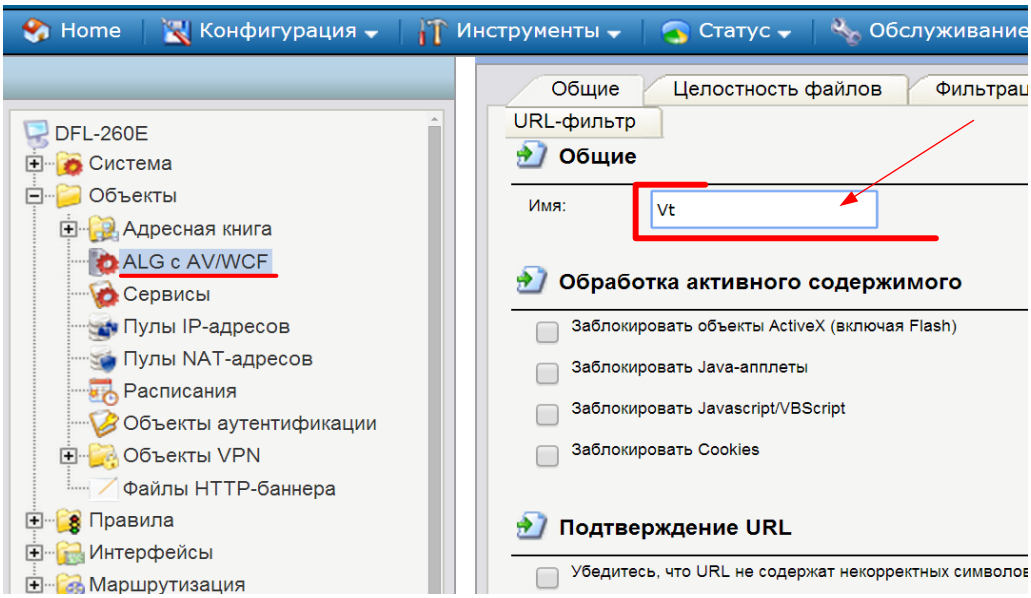

Рисунок 29 – Ввод имени для созданного HTTP ALG

Включаем антивирусное сканирование — **Вкладка «Антивирус».**

Получаем окно - вкладка «Антивирус», как на рисунке 30.

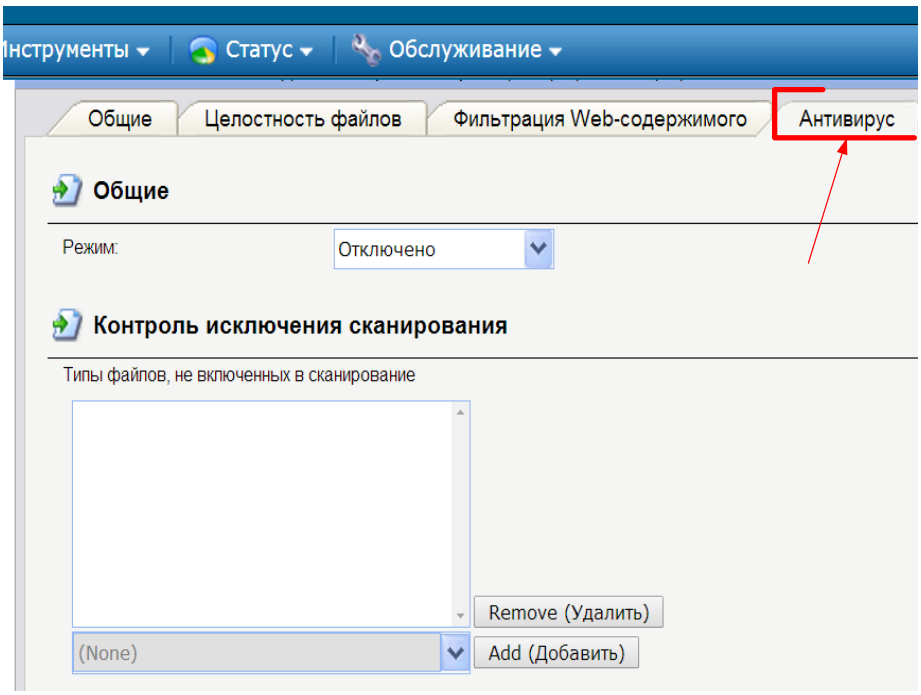

Рисунок 30 - Вкладка «Антивирус»

Во вкладке **«Антивирус»** активируем опцию **«Защита»**, как на рисунке 31.

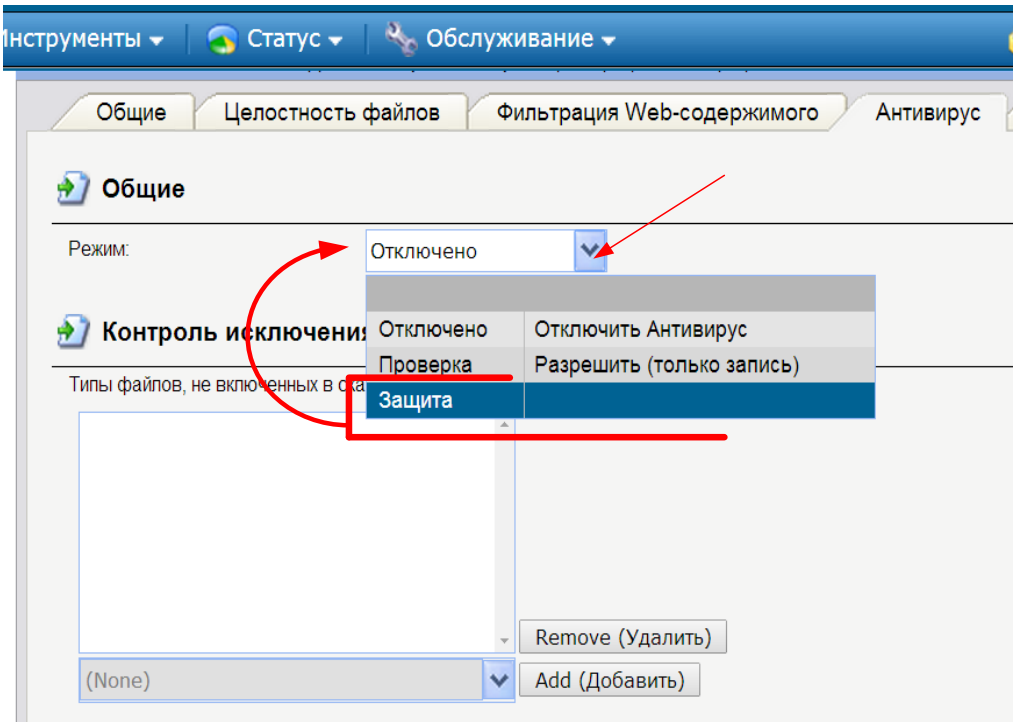

Рисунок 31 - Вкладка «Антивирус» - опция «Защита»

Получили - вкладка «Антивирус» - «Защита», показанной на рисунке 32.

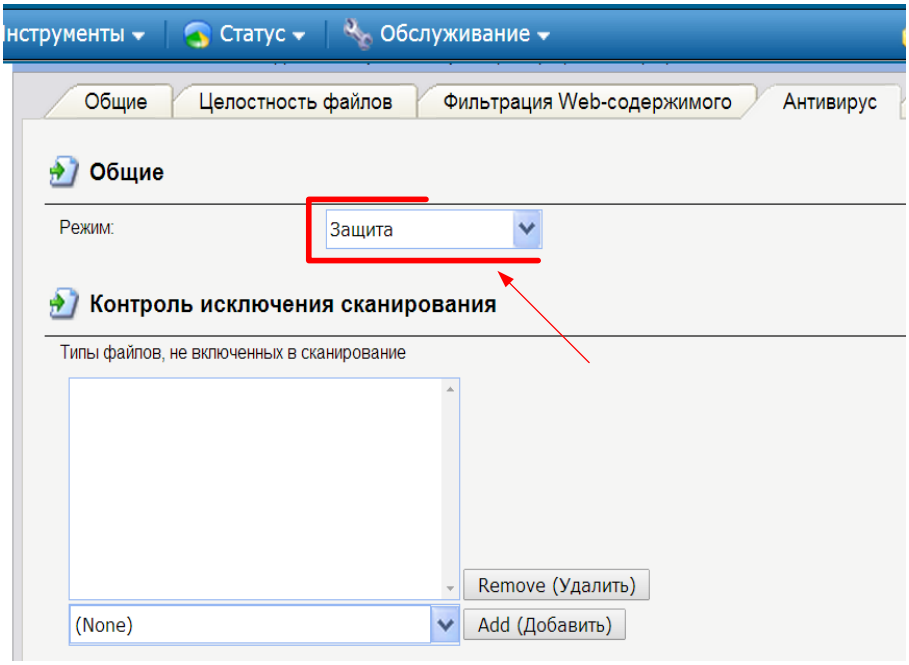

Рисунок 32 - Вкладка «Антивирус» - «Защита»

Справа от вкладки «Антивирус» активируем вкладку **«URL-фильтр».** Получили окно, как на рисунке 33.

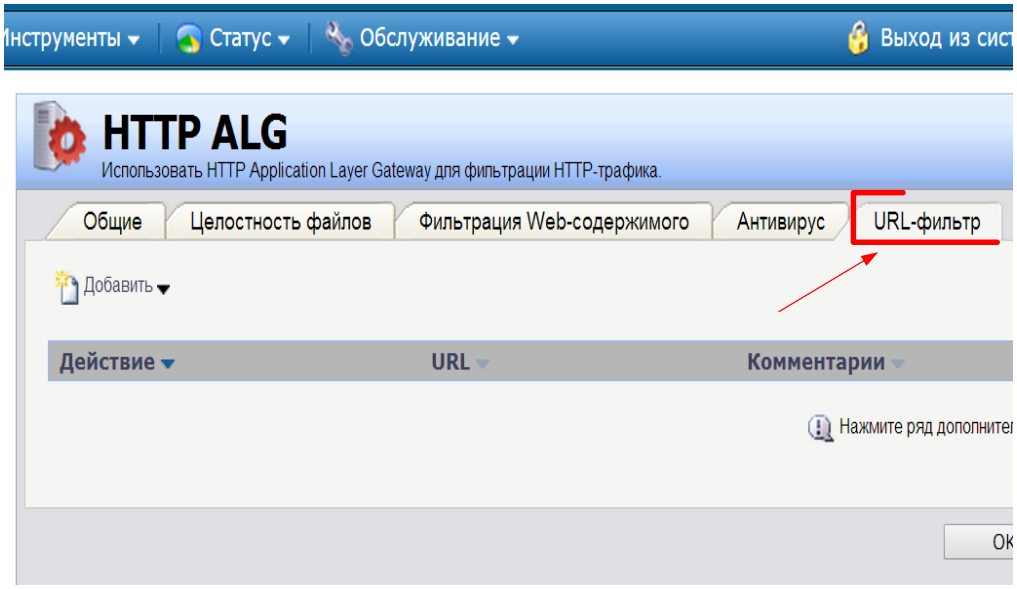

Рисунок 33 - Вкладка «URL-фильтр»

Жмем **«Добавить»** и добавляем HTTP ALG UR, как на рисунке 34.

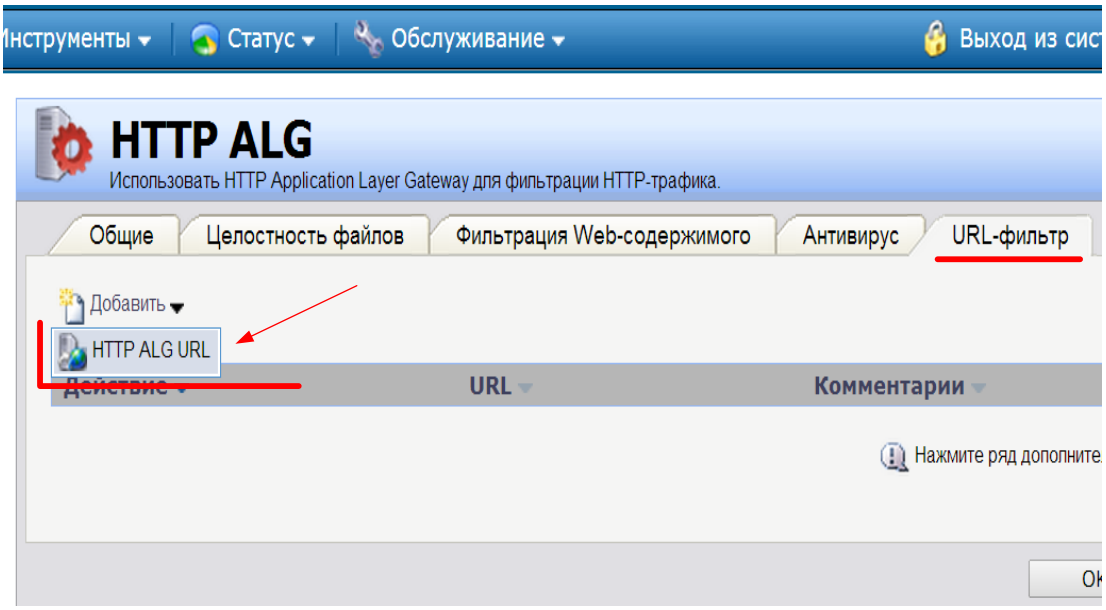

Рисунок 34 - Вкладка «URL-фильтр» - HTTP ALG URL

Переходим во вкладку **«Общие».**

В поле **«Действие»** выберем **«Черный список»**, как на рисунке 35.

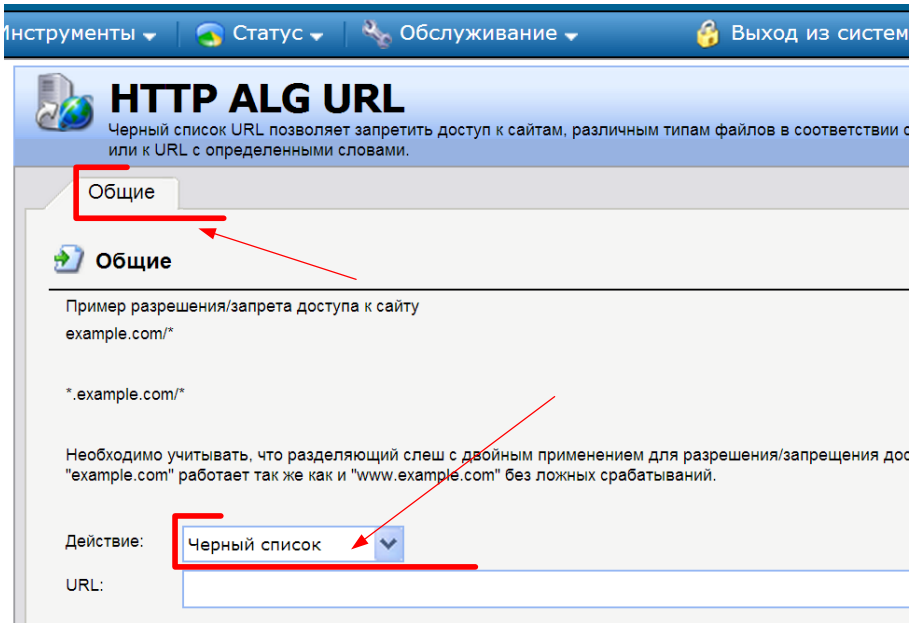

Рисунок 35 – Вкладка «Черный список»

В окне **«URL»** - введем ***.osu.ru/***, как на рисунке 36.

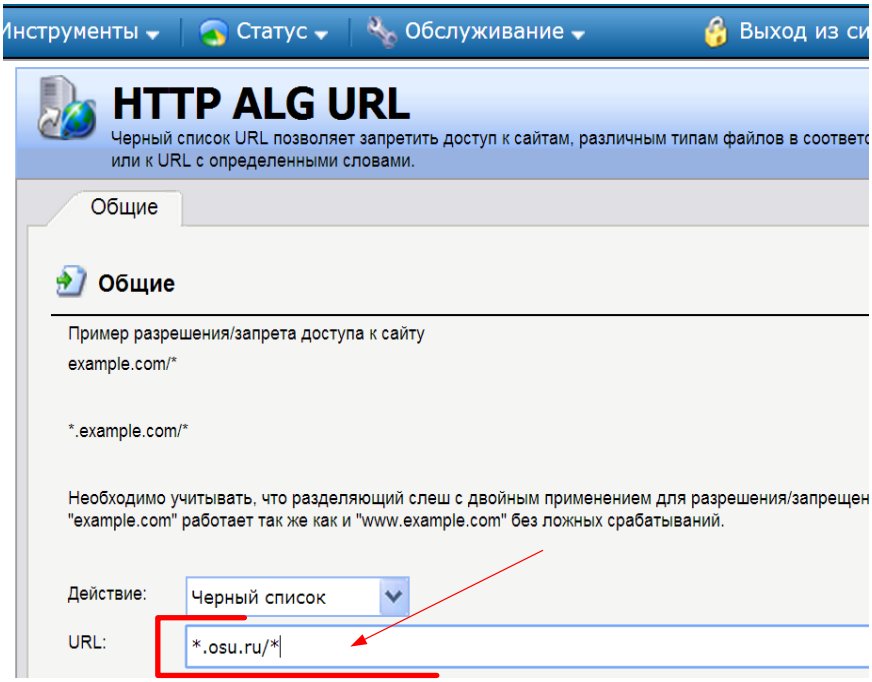

Рисунок 36 – Добавление web-сайта в черный список

Нажимаем **ОК** и получаем окно с указанным сайтом, внесенным в **«Черный список»**, как на рисунке 37.

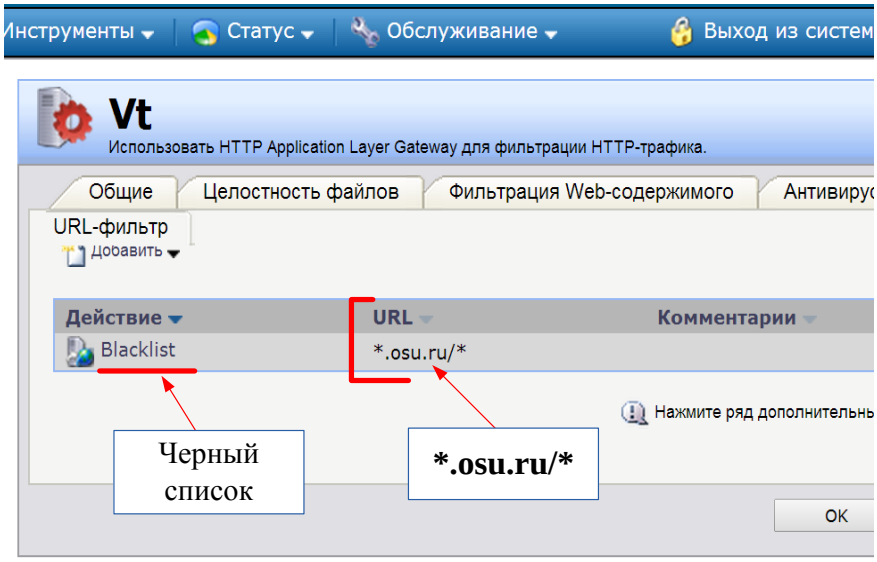

Рисунок 37 - Получаем окно с сайтом внесенным в «Черный список»

Активируем «Объект» - **«Сервисы»**, как на рисунке 38.

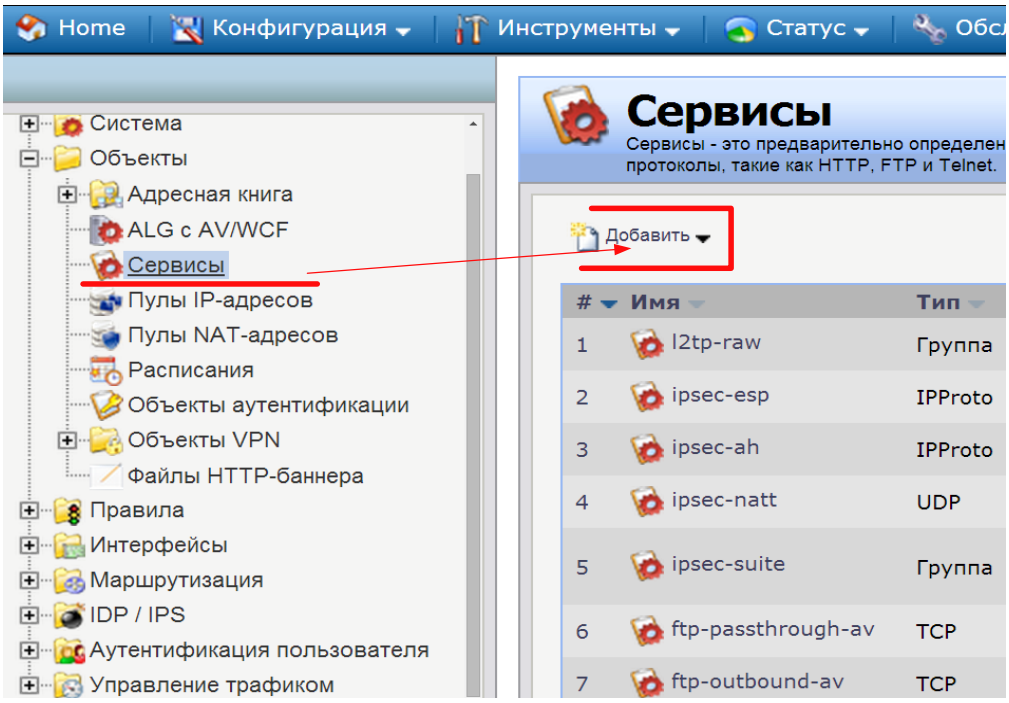

Рисунок 38 - Активируем «Объект» - «Сервисы»

Произведем настройки нового **«Сервис TCP/UDP»**, показанные на рисунке 39.

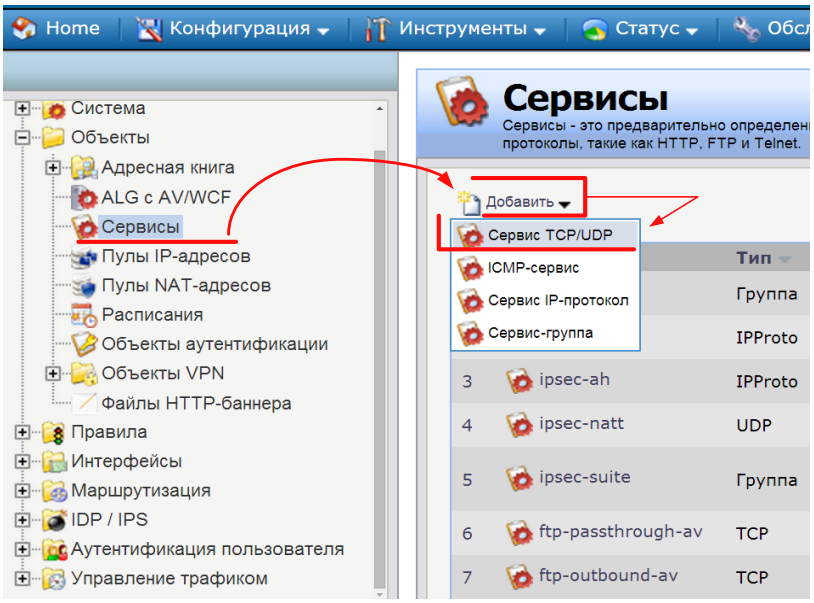

Рисунок 39 - Настройка нового «Сервис TCP/UDP»

Далее производим настройки **«Сервис TCP/UDP»**, как на рисунке 40.

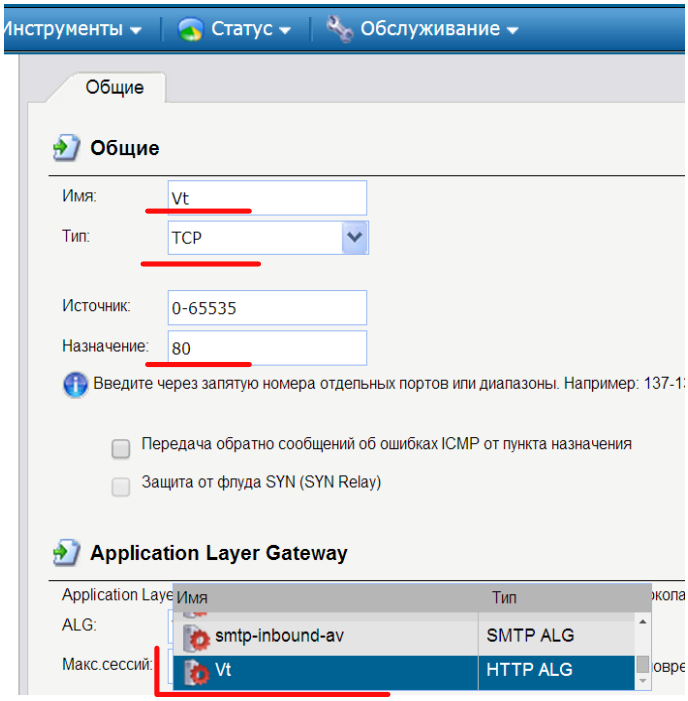

Рисунок 40 - Настройки «Сервис TCP/UDP»

Добавляем новое **IP-правило**.

Открываем правила, как показано на рисунке 41.

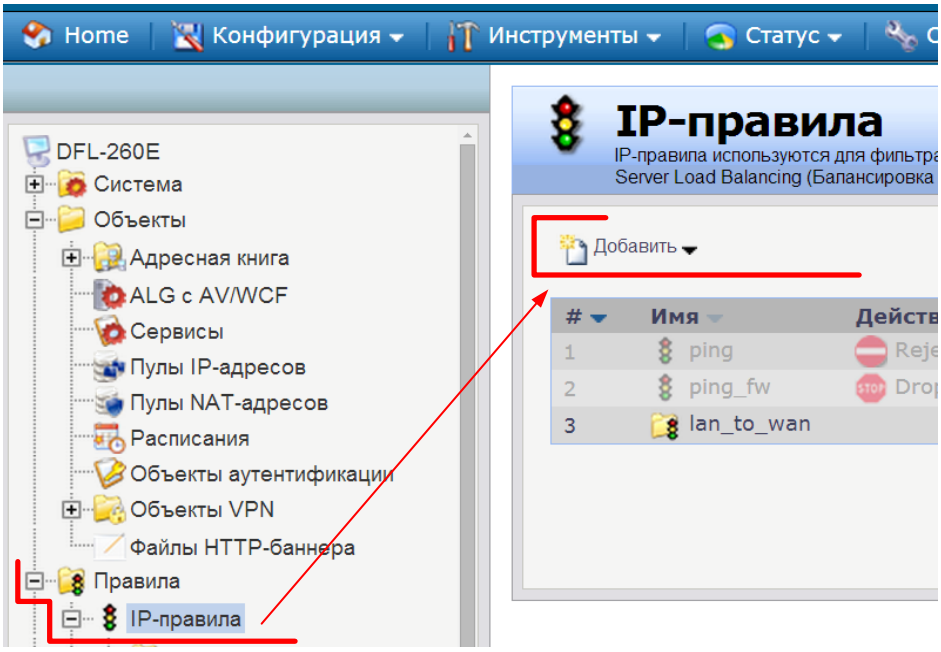

Рисунок 41 - Добавляем новое IP-правило

Добавляем «**IP-правило**», как показано на рисунке 42.

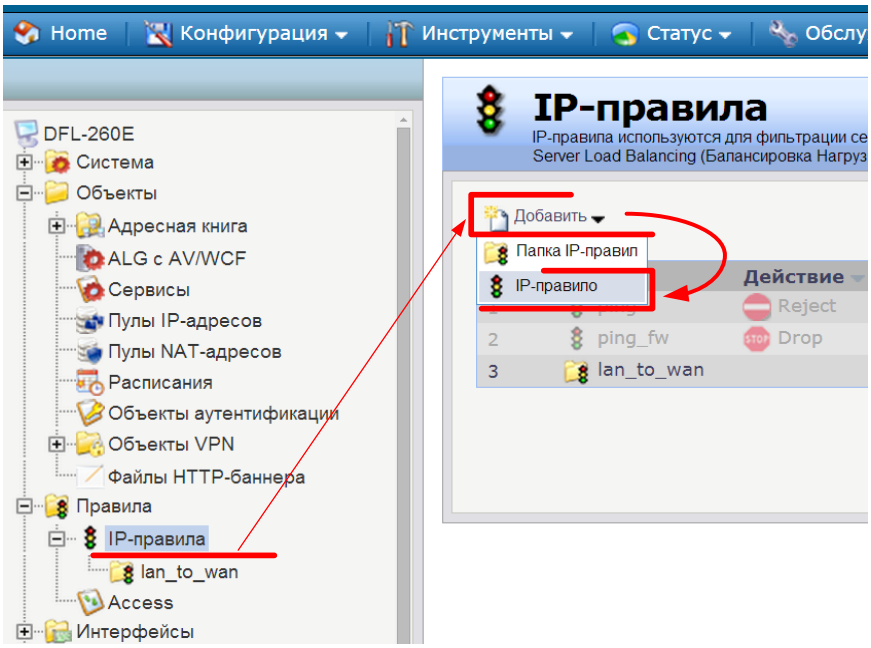

Рисунок 42 - Новое IP-правило

Получаем окно, показанное на рисунке 43.

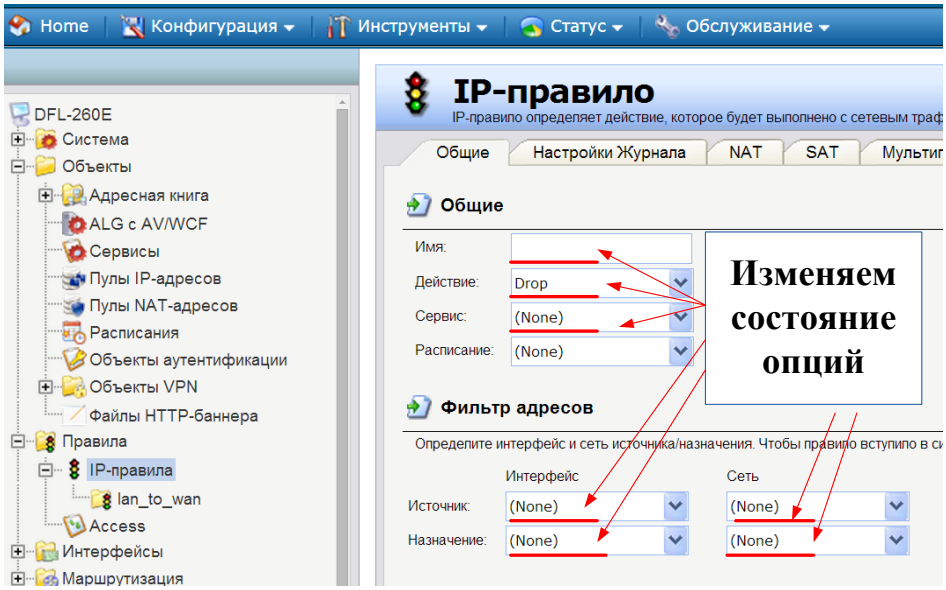

Рисунок 43 – Изменяем состояние опций

Во вкладке **«Общие»** установим следующие значения, которые показаны на рисунке 44.

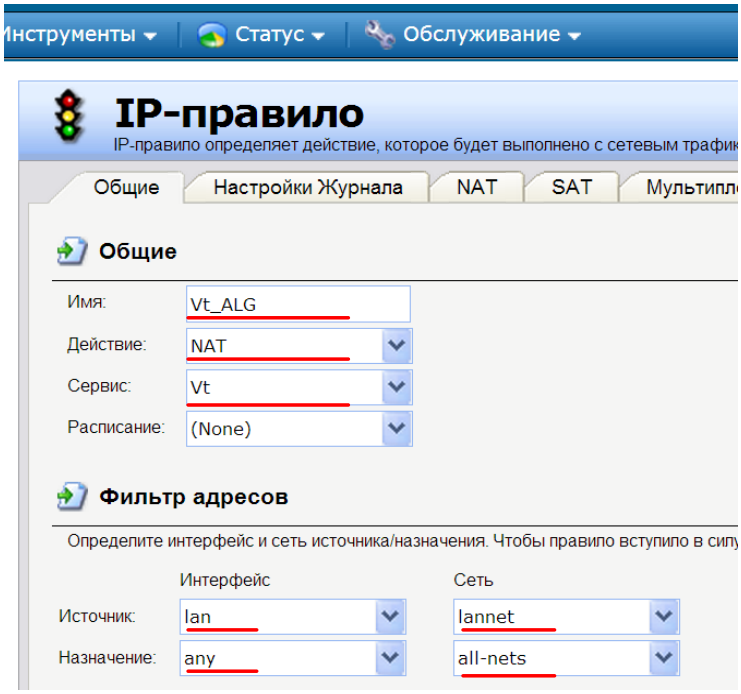

Рисунок 44 – Настройки IP правила

Нажиаем **ОК.**

Получаем окно со списком, который показан на рисунке 45.

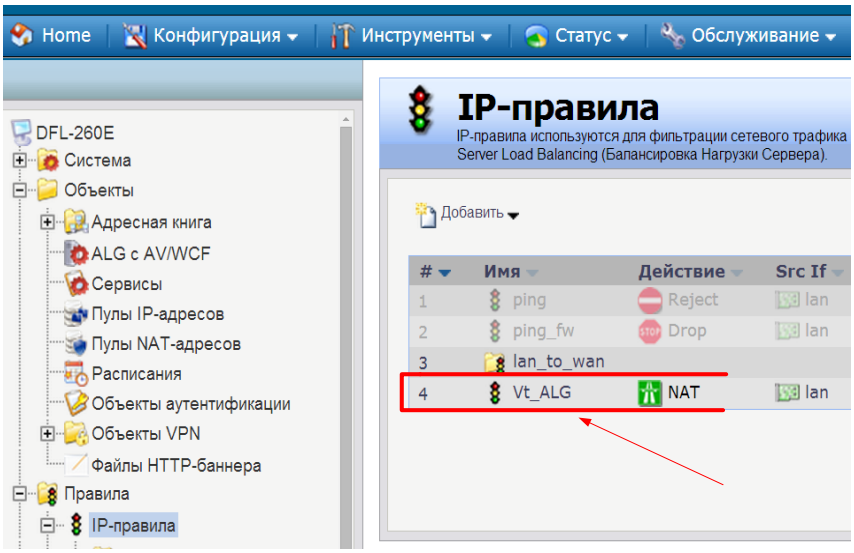

Рисунок 45 - Окно со списком

Нажмите правой кнопкой мыши на **«vt_alg»** и получаем окно правил, как на рисунке 46.

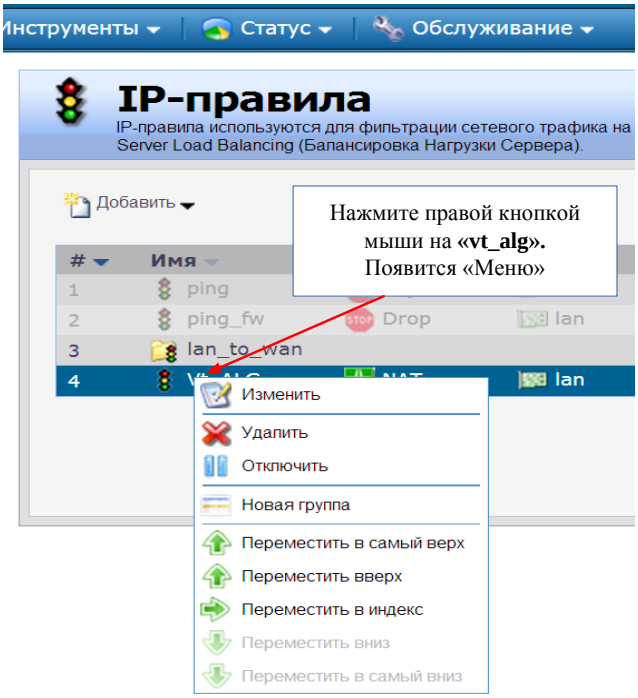

Рисунок 46 – Окно правил

Выберите **«Переместить в самый верх»** для того что бы **«Новое правило»** стояло **первым** в списке (высшим приоритетом обладает **Правило** с номером № 1).

Установка правила **«vt_alg»** первым в списке показана на рисунке 47.

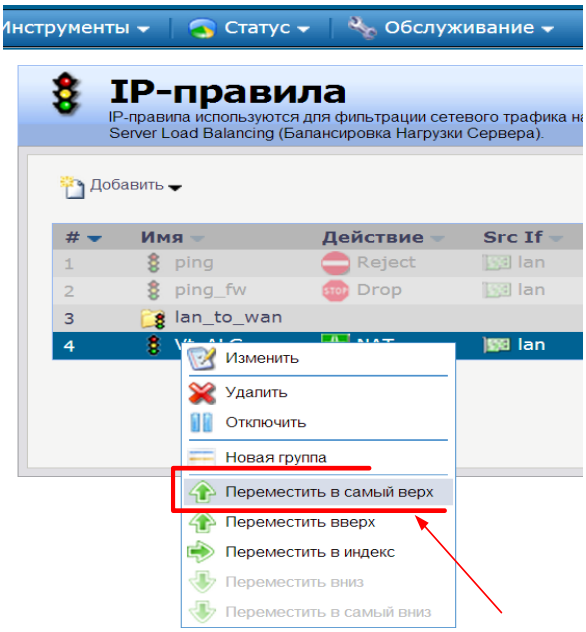

Рисунок 47 – Установка правила **«vt_alg»** первым в списке

Получим новое правило, как на рисунке 48.

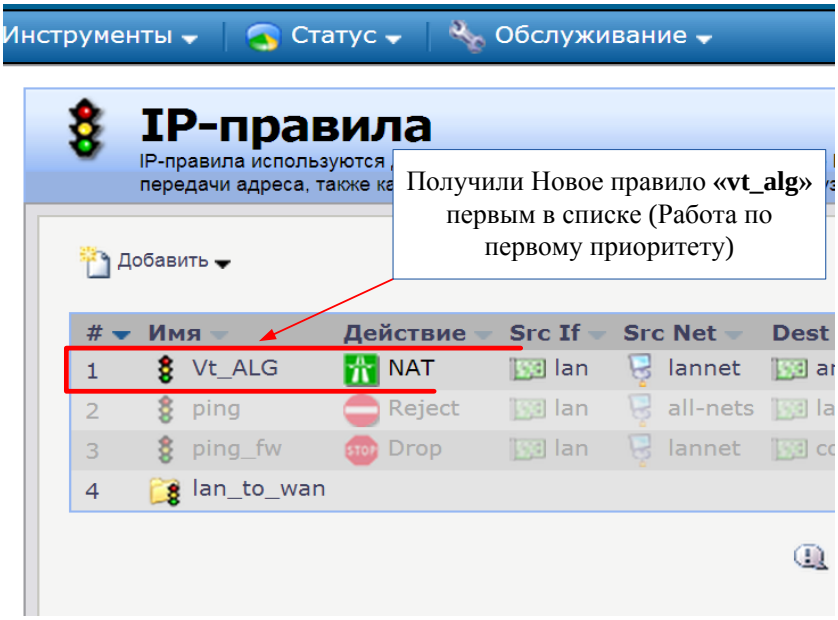

Рисунок 48 – Получаем новое правило

Активируйте опцию **«Конфигурация»** в основном **«Меню»**.

Нажмите **«Сохранить и активировать»** для сохранения настроек, как на рисунке 49.

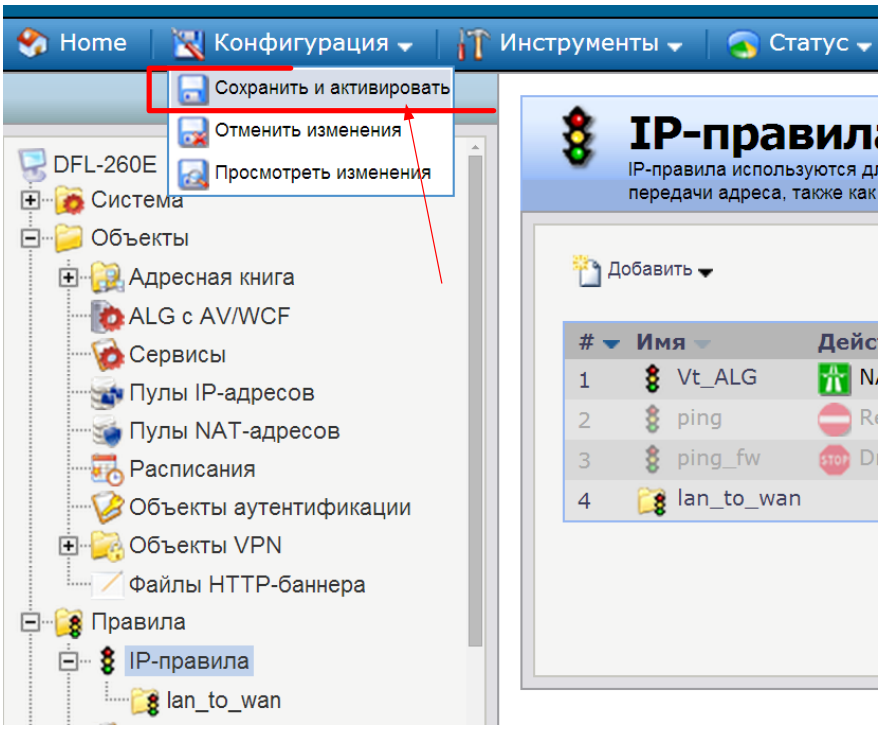

Рисунок 49 - Нажмимаем «Сохранить и активировать» для сохранения настроек

Выходит окно, показанное на рисунке 50.

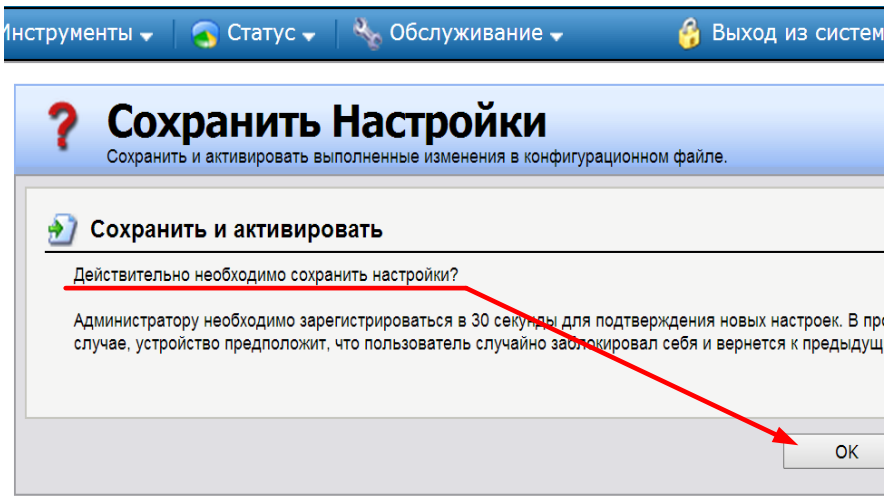

Рисунок 50 – Сохранить и активировать

Ок. Окно - блокировка сайта закончена, как показано на рисунке 51.

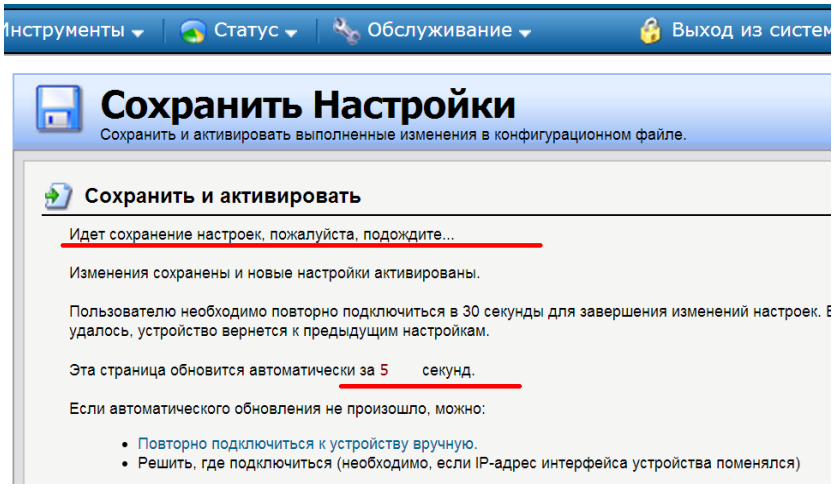

Рисунок 51 - Блокировка сайта закончена

Блокировка сайта закончена. Пригласите преподавателя.

Удаление настройки.

Зайти в IP-правила.

В правом окне установить указатель на **«vt_alg»** в списке.

Нажмите правой кнопкой мыши на **«vt_alg».**

Появится «Меню» - Удаление настройки, как на рисунке 52.

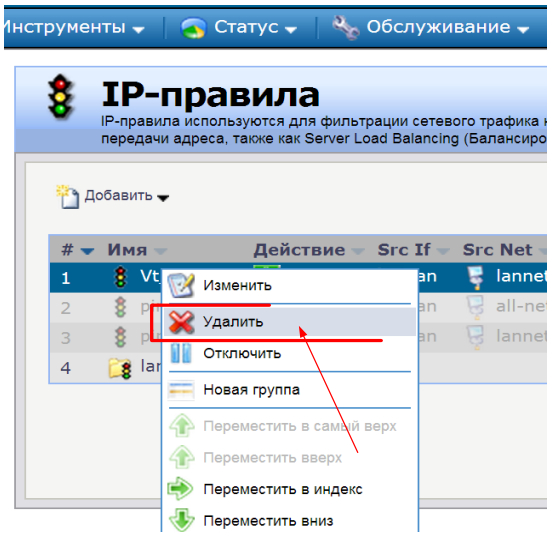

Рисунок 52 - Удаление настройки

Появится окно. Правило удалено, как показано на рисунке 53.

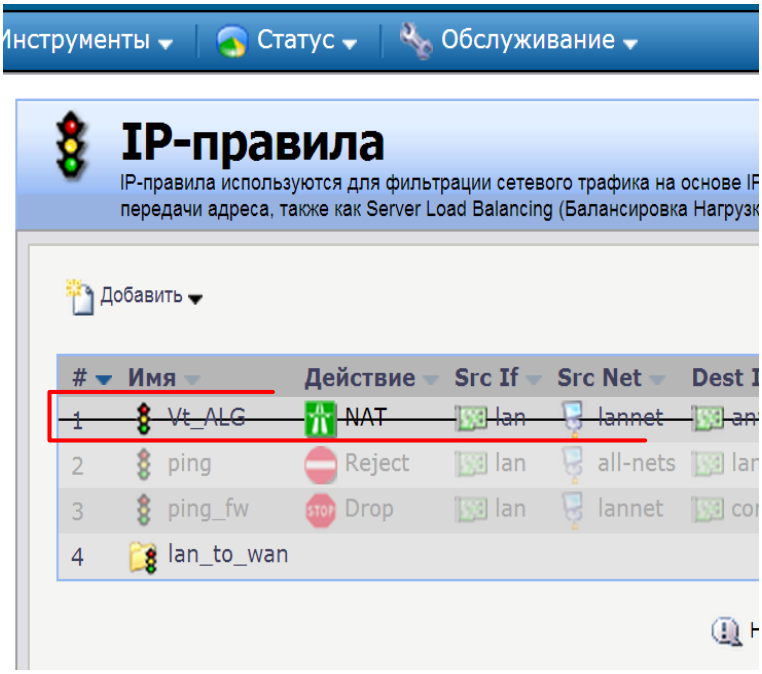

Рисунок 53 - Окно «Правило удалено»

Для чистоты **процесса удаления** в основном меню **«Конфигурация»** активируйте команду **«Сохранить и активировать».**

Работа выполнена.

Содержание отчета:

1 Название и цель работы.

2 Показать основные шаги и этапы проведения лабораторной работы.

3 Представить основные экранные формы процесса работы.

4 Представить результаты работы.

5 Выводы по выполненной работе.

6 Список использованных источников.

5 Лабораторная работа № 5. Исследование основных функций

межсетевого экрана Cisco ASA 5505

Цели работы:

1 Изучить основные функциональные особенности оборудования Cisco ASA 5505.

2 Освоить принципы использования оборудования Cisco ASA 5505.

3 Освоить принципы конфигурирования оборудования Cisco ASA 5505.

Краткие теоретические сведения.

Программное обеспечение.

HyperTerminal - это встроенное приложение, позволяющее получить терминальный доступ к другим компьютерам, системам электронных досок объявлений (BBS), оперативным службам и хост-компьютерам с помощью модема или нуль-модемного кабеля в Windows XP.

Программа HyperTerminal предоставляет чрезвычайно полезные средства для диагностики соединений, устанавливаемых с помощью модема. Чтобы убедиться в правильности настроек модема, можно воспользоваться этой программой для отправки команд и проверки результатов. Кроме того, HyperTerminal можно использовать для отправки файлов большого объема с компьютера на компьютер (например, с настольного компьютера на портативный) через последовательный порт (это более удобно, нежели подключение портативного компьютера к сети).

Аппаратное обеспечение.

Межсетевой экран или сетевой экран — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами [1].

Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

Схема включения Фаервола в сети показана на рисунке 54.

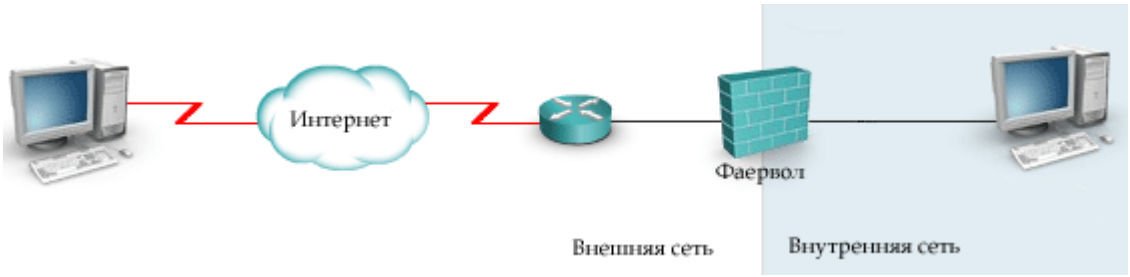

Рисунок 54 - Схема включения Фаервола в сети

Существует три фундаментальные технологии, на основе которых фаерволы выполняют свою работу:

– статическая пакетная фильтрация (packet filtering) – пакеты фильтруются на основе статической информации в заголовке сетевых пакетов;

– прокси-фаервол (proxy firewall) – устройство находится между клиентом и внешней сетью и все запросы и соединения клиента с внешними хостами осуществляются от имени прокси сервера;

– динамическая пакетная фильтрация (stateful packet filtering) – сочетает в себе лучшее первых двух.

Далее, для удобства, будем называть ее просто - динамической фильтрацией, чтобы противопоставить обычной статической пакетной фильтрации.

Статическая пакетная фильтрация (packet filtering).

Статическая пакетная фильтрация используется для фильтрации пакетов, входящих в сеть, а также пакетов, проходящих между разными сегментами сети. Пакетный фаервол инспектирует входящий трафик, анализируя информацию сетевого и транспортного уровней модели OSI.

Фаервол анализирует IP пакет и сравнивает его с заданным набором правил, аксес листом (ACL – Access Control List). ACLs задаются администратором вручную. Анализируются только следующие элементы:

– адрес источника;

– порт источника;

– адрес назначения;

– порт назначения;

– протокол;

– некоторые фаерволы также могут анализировать информацию из заголовка пакета, проверяя, является ли пакет частью нового либо установленного соединения.

Если пакет, не удовлетворяет правилам, заданным в ACL, по которым он может быть пропущен в защищенную сеть, пакет отбрасывается. Преимущество статической пакетной фильтрации в ее быстродействии. У статической пакетной фильтрации есть следующие недостатки:

– произвольный пакет будет пропущен в сеть, если он удовлетворяет правилам ACL (например, спуфинг);

– пакеты, которые должны быть отфильтрованы, могут попасть в сеть, если они фрагментированы;

– в процессе задания правил ACL могут формироваться очень большие списки, которыми сложно управлять;

– ряд сервисов не может контролироваться пакетной фильтрацией. Это, например, приложения мультимедии, где соединения динамически устанавливаются на произвольных портах, номера которых будут известны только после установки соединения.

Статическая пакетная фильтрация часто используется на маршрутизаторах. Устройства защиты Cisco также могут использовать такую фильтрацию.

Прокси-фаервол (proxy-firewall).

Прокси-фаервол, называемый также прокси-сервером – это обычно прикладная программа, устанавливаемая на сервер, имеющий доступ в защищенную и внешнюю сеть. Все соединения хостов защищенной сети с хостами внешней сети осуществляются от имени прокси-фаервола, как если бы прокси-фаервол сам устанавливал эти соединения. Хосты защищенной сети никогда сами не устанавливают соединений с внешним миром. Для установки связи, хосты внутренней сети посылают запросы прокси-фаерволу, запросы сравниваются с базой

правил. Если запрос соответствует правилу в базе и разрешен, прокси-фаервол посылает запрос внешнему хосту и затем форвардит ответ внутреннему хосту.

Прокси-фаерволы работают на верхних уровнях модели OSI. Соединения устанавливаются между сетевым и транспортным уровнем, однако прокси-фаервол анализирует запрос вплоть до седьмого уровня на предмет соответствия набору правил, если все удовлетворяет, он устанавливает соединение.

Анализ пакетов до седьмого уровня является большим преимуществом прокси-фаерволов. Но имеются и следующие недостатки:

– если прокси-фаервол будет взломан, доступ ко всей внутренней сети будет открыт;

– прокси-сервер – это программа работающая под управлением определенной операционной системы, поэтому прокси-сервер будет настолько безопасным, насколько безопасна сама эта система;

– значительная процессорная нагрузка для осуществления прокси сервисов, что сказывается на производительности, при увеличении числа запросов на соединение [2].

Динамическая пакетная фильтрация (stateful packet filtering).

Данная технология обеспечивает лучшую комбинацию безопасности и производительности. Используется не только ACL, но также анализируется состояние сессии, записываемое в базу, которую называют таблицей состояния (state table). Эту технологию Cisco преимущественно использует в своих устройствах защиты.

После того как соединение установлено, все данные сессии сравниваются с таблицей состояния. Если данные сессии не соответствуют информации в таблице состояния для этой сессии, соединение сбрасывается.

В этой технологии сохраняется состояние каждой открытой сессии. Каждый раз, когда устанавливается разрешенное внешнее либо внутреннее TCP или UDP соединение, информация об этом соединении запоминается в таблице состояния сессий. В таблицу заносится адрес источника и назначения, номера портов, порядковые номера TCP сессии (sequence numbers), также дополнительные флаги.

Работа динамической фильтрации заключается в следующем - если соединение, запрашиваемое хостом разрешено Cisco фаерволом, то он запоминает это и помещает информацию о соединении в таблицу состояний (state table) и при возвращении трафика, то есть при ответе другого хоста на запрос, пакеты разрешаются, если они соответствуют тому, что ожидает устройство защиты, то есть соответствуют информации, хранящейся в state table.

Этот метод эффективен по трем причинам:

– он работает и с пакетами и с соединениями;

– производительность выше, чем у прокси-фаерволов;

– сохраняется информация каждого соединения, что позволяет определить является ли пакет частью этого соединения.

Принципы использования оборудования сетевых экранов расмотрим на примере оборудования Cisco ASA 5505.

Cisco ASA 5505.

Cisco ASA 5505 - многофункциональное устройство защиты ресурсов сети от внутренних и внешних атак для небольших офисов. Внешний вид представлен на рисунке 55.

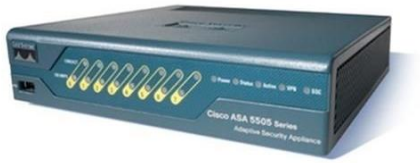

Рисунок 55 - Межсетевой экран Cisco ASA 5505

Особенности Cisco ASA 5505:

– производительность МСЭ: до 150 Мбит/сек;

– производительность МСЭ и отражения атак: недоступно;

– производительность VPN: до 100 Мбит/сек;

– количество одновременно поддерживаемых сессий: 10 000/25 000 (доступно при помощи дополнительных лицензий);

– число IPSec VPN-туннелей:10/25 (доступно при помощи дополнительных лицензий);

– число SSL VPN-туннелей: 2/25 (доступно при помощи дополнительных лицензий);

– «Виртуальные» МСЭ: 0;

– кластеризация и балансировка VPN: Нет;

– поддерживаемые физические интерфейсы: 8-ми портовый коммутатор 10/100, 2 интерфейса поддерживают PoE;

– поддержка дополнительного четырехпортового модуля Gigabit Ethernet: Нет

– поддерживаемые логические интерфейсы VLAN 802.1:3 (без транковых интерфейсов)/20 (с транковыми интерфейсами) - доступно при помощи дополнительных лицензий.

Технические характеристики ASA 5505:

– предназначение - небольшие, домашние офисы;

– количество защищаемых узлов: 10, 50, не ограничено (в зависимости от типа лицензий);

– производительность межсетевого экрана, Мб/с: 150;

– производительность шифрования 3DES/AES, Мб/с: 100;

– максимальное количество IPSEC VPN сессий: 10, 25 (в зависимости от типа лицензий);

– максимальное количество SSL VPN сессий: 2/25 (в зависимости от типа лицензий);

– максимальное количество контролируемых соединений: 10 000, 25000 (в зависимости от типа лицензий);

– максимальное количество новых сессий в 1 секунду: 3000;

– максимальная скорость обработки пакетов (64 байт) пакетов в секунду: 85000;

– объем оперативной памяти: 256;

– минимальный объем флэш памяти: 64;

– количество интегрированных портов: 8x10/100 включая 2 PoE;

– количество виртуальных сетей (VLAN): 3/20 (с использованием транков)

– поддержка аппаратных модулей SSC/SSM: нет;

– количество контекстов включено/максимум: 0.

Передняя панель Cisco ASA 5505 показана на рисунке 56.

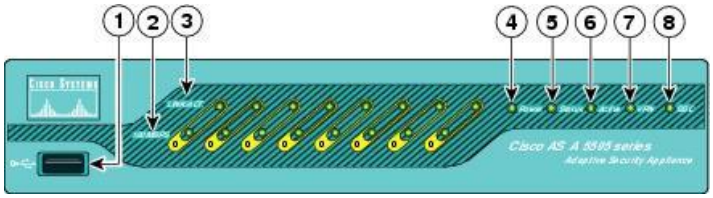

Рисунок 56 - Передняя панель Cisco ASA 5505

Обозначение светодиодов передней панели экрана показано в таблице 2.

Таблица 2 – Обозначение светодиодов передней панели Cisco ASA 5505

Инд	Порт/ Индикац.	Цвет	Статус	Описание
1	USB Port	—	—	Резервный USB порт для применения в будушем.
2	Speed Indicators	—	—	Скорость сети 10 Mbps.
		Зеленый	Горит	Скорость сети 100 Mbps.
3	Link Activity Indicators	Зеленый	Горит	Физическое соеденение установлено
		Зеленый	Мигает	Обмен даными в сети
4	Power	Зеленый	Горит	Устройство включено
		—	—	Устройство выключено
5	Status	Зеленый	Мигает	Диагностика и загрузка системы
			Горит	Система работает
		Желный	Горит	Система не работает, в следстии ошибок
6	Active	Зеленый	Горит	Система в работе
		Желтый	Горит	Система в резерве
7	VPN	Зеленый	Горит	VPN тунель установлен.
			Мигает	Система устанавливает VPN тунель.
		Желтый	Горит	Тунель разорван
8	SSC	—	—	Наличие SSC.

Задняя панель Cisco ASA 5505 показана на рисунке 57.

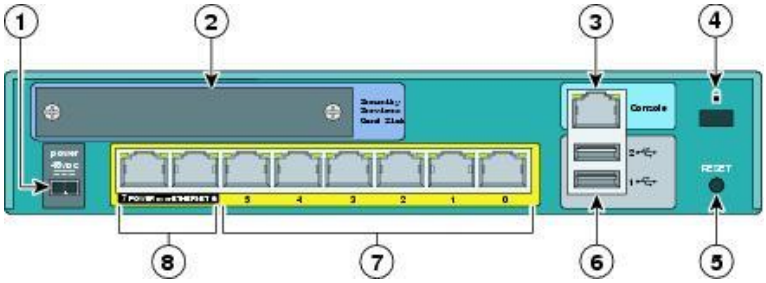

Рисунок 57 - Задняя панель Cisco ASA 5505

Обозначение светодиодов задней панели экрана показы в таблице 3.

Таблица 3 – Обозначение светодиодов задней панели Cisco ASA 5505

Инд.	Порт/ Индикация	Описание
1	Power connector	Порт подключения питания
2	Security service card slot	Резервный слот для применения в будущем.
3	Serial console port	Порт управления (консоль)
4	Lock device	Разъем установления ключа
5	RESET button	Перезапуск устройства
6	Two USB v2.0 ports	Два резервный USB порта для применения в будущем.
7	Ethernet switch ports 0-7	Ethernet порты имеюшие гибкие настройки VLAN
8	PoE switch ports 6-7	Два порта для подключения PoE устройств (например IP телефон)

Межсетевой экран ASA 5505 имеет возможность управления через Telnet. Так же как и коммутатор Catalyst 2960 экран первоначально не имеет никаких настроек. Первоначальная настройка производится через интерфейс консоль (например, программу HyperTerminal). Экранная форма первоначальной настройки показана на рисунке 58.

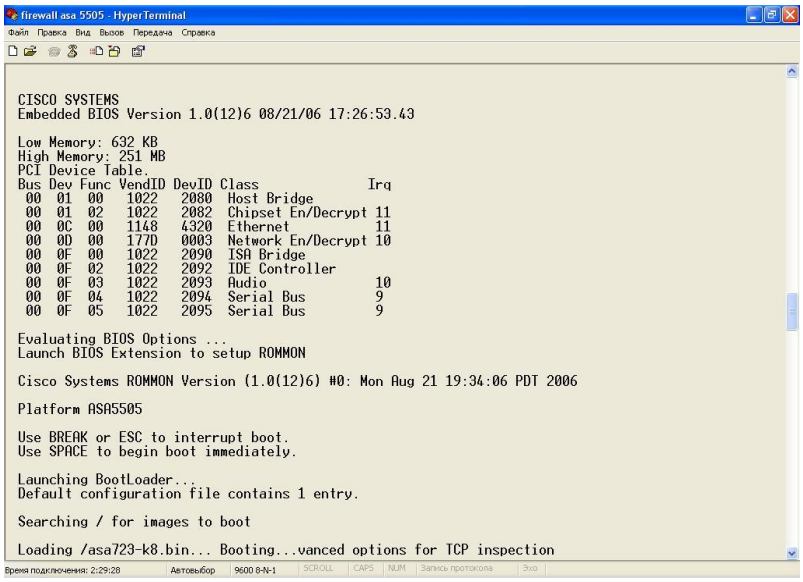

Рисунок 58 - HyperTerminal

Рассмотрим базовые команды устройств защиты Cisco ASA, необходимые для работоспособности данного устройства. Минимальные команды, которые необходимы для начала работы это: hostname, interface, nameif, security-level, ip address.

При первом включении необходимо войти в режим конфигураций.

Пример команды:

– ciscoasa> **enable;**

– ciscoasa# **config terminal;**

– ciscoasa (config)# .

Hostname – индивидуальное имя устройства. Имя может иметь до 63 буквенно-числовых символов в верхнем и нижнем регистрах.

Пример команды:

- ciscoasa (config)# **hostname ASA5505** ASA5505 (config)#.

Interface - определяет интерфейс и его расположение (слот). Для входа в конфигурацию интерфейса, необходимо указать его тип, слот и порт. Например, GigabitEthernet0/0 либо Management0/0. После чего мы можем задать необходимые параметры.

Надо помнить, что по умолчанию интерфейсы выключены, поэтому не забываем их включать командой **no shutdown**.

Пример команды:

- ciscoasa (config)# **interface vlan1;**
- ciscoasa (config-if)#.

Nameif - команда дает имя интерфейсу на устройстве защиты. По умолчанию первые два интерфейса имеют имена inside и outside.

Пример команды:

- ciscoasa (config)# **interface vlan1;**
- ciscoasa (config-if)# **nameif inside.**

Любому из интерфейсов устройства защиты вы можете присвоить **ip адрес**. Командой clear configure ip сбрасываются ip адреса на всех интерфейсах. Командой ip address также задается резервный адрес в конфигурации файловера (failover).

Пример команды:

- ciscoasa (config)# **interface vlan1;**
- ciscoasa (config-if)# **nameif inside;**
- ciscoasa (config-if)# **ip address 192.168.1.1 255.255.255.0.**

Security level - по умолчанию, когда вы включите Cisco ASA, вы увидите, что внутреннему (inside) и внешнему (outside) интерфейсам уже присвоены уровни безопасности. 100 - внутреннему, 0 - внешнему. При задании имени другим интерфейсам, устройство защиты автоматически назначает им уровень безопасности 0, который вы должны будете изменить в соответствии с вашим дизайном сети.

Пример команды:

- ciscoasa (config)# **interface vlan1;**
- ciscoasa (config-if)# **nameif inside;**
- ciscoasa (config-if)# **ip address 192.168.1.1 255.255.255.0.**
- ciscoasa (config-if)# **security-level 100.**

Схема стенда лабораторной работы показана на рисунке 59.

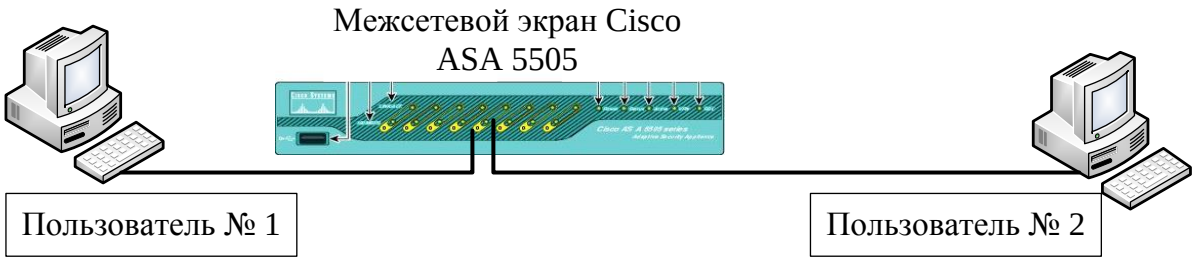

Рисунок 59 - Схема стенда лабораторной работы

Порядок выполнения работы:

1 Войти в управляющую программу сетевого экрана через HyperTerminal.

2 Войти в режим конфигурации.

3 Выписать индивидуальное имя устройства.

4 С помошью команды show ip address выпишите параметры VLAN (должно быть настроено два VLAN: внутреняя сеть и внешняя)

5 Изменить имя устройство, изменить конфигурацию VLAN.

Содержание отчета.

1 Цель работы.

2 Краткие теоретические сведенья.

3 Результаты выполнения практической части.

4 Вывод по результатам работы.

Контрольные вопросы:

1 Назначение сетевоно экрана Cisco ASA 5505?

2 Уровни модели OSI?

3 Какие уровни безопасности бывают (Security level)?

4 Какие технологии фильтрации используют firewall? Какие отличия между ними?

5 PoE устройства?

6 Лабораторная работа № 6. Настройка операционной системы Cisco

Цель работы.

Целью лабораторной работы является обучение методам и средствам первоначальной настройки специализированной ОС Cisco IOS, под управлением которой работают маршрутизаторы.

Краткие теоретические сведения.

Cisco IOS – это специализированная ОС, обеспечивающая функционирование сетевого оборудования компании «Cisco Systems, Inc». Взаимодействие с данной ОС возможно либо через web-браузер, либо через интерфейс командной строки (CLI-интерфейс).

Данная ОС поддерживает удаленный доступ к интерфейсу командной строки по протоколам Telnet или SSH. В Cisco IOS существует несколько режимов.

Пользовательский режим (user mode) – стандартный режим первоначального доступа к ОС. В этот же режим ОС переходит автоматически при продолжительном отсутствии ввода в режиме администратора. В режиме пользователя доступны только простые команды, не влияющие на конфигурацию оборудования. Приглашение командной строки имеет следующий вид [3]:

- router>.

Административный режим (privileged mode). Открывается командой *enable*, введенной в режиме пользователя:

- router> **enable.**

В административном режиме доступны команды, позволяющие получить полную информацию о конфигурации оборудования и его состоянии, а также команды перехода в режим конфигурирования, команды сохранения и загрузки конфигурации. Приглашение командной строки имеет следующий вид:

- router#.

Обратный переход в пользовательский режим производится по команде *disable* или по истечении установленного времени неактивности. Завершение сессии

– команда *exit*.

Глобальный режим конфигурирования (конфигурационный режим). Активизируется командой *config terminal*, введенной в административном режиме:

- router# **configure terminal.**

Глобальный режим конфигурирования организован иерархически – он содержит как непосредственно команды конфигурирования оборудования, так и команды перехода в режимы конфигурирования его подсистем (например, интерфейсов, протоколов маршрутизации, механизмов защиты).

Приглашения командной строки в наиболее часто используемых конфигурационных режимах имеют следующий вид:

- router(config)#;
- router(config-if)#;
- rounter(config-router)#;
- router(config-ext-nacl)#;
- switch(config-line)#;
- switch(vlan)#.

Выход из любого режима конфигурирования в режим верхнего уровня производится командой *exit* или комбинацией клавиш *Ctrl-Z.*

Кроме того, команда *end*, поданная в любом из режимов конфигурирования немедленно завершает процесс конфигурирования и возвращает пользователя в администраторский режим.

Любая команда изменения конфигурации вступает в действие немедленно после ввода. Все команды и параметры могут быть сокращены (например, "*enable*" – "*en*", "*configure terminal*" – "*conf t*", “*show running-config*” – “*sh run*”).

В любом месте командной строки для получения помощи может быть использован вопросительный знак, например:

- router#**?**

- router#**co?**

- router#**conf ?**

Имена сетевых интерфейсов также могут быть сокращены, например, вместо "*fast ethernet*0/1" достаточно написать "*fa*0/1".

Отмена любой команды (отключение опции или режима, включаемых командой, снятие или удаление параметров, назначаемых командой) производится подачей этой же команды с префиксом "*no*", например:

- router(config)#**int fa0/1;**

- router(config-if)#**shutdown;**

- router(config-if)#**no shutdown.**

При загрузке сетевого оборудования, работающего под управлением Cisco IOS, происходит считывание команд конфигурации из изменяемого постоянного запоминающего устройства (NVRAM), где они хранятся в виде текстового файла, называемого *рабочей конфигурацией* (running config). Конфигурация, сохраненная в NVRAM, называется *начальной конфигурацией* (startup config). В процессе работы оборудования администратор может вводить дополнительные конфигурационные команды, в результате чего рабочая конфигурация становится отличной от начальной [3].

Просмотр начальной и рабочей конфигураций маршрутизатора производится в административном режиме:

- router#**show startup-config;**

- router#**show running-config.**

Вывод последней команды позволяет просмотреть текущую конфигурацию. Однако если администратор не менял значения параметров, используемых в ОС по умолчанию, то они при выводе не отобразятся.

При копировании одной конфигурации поверх другой возможны два варианта: перезапись и слияние. При перезаписи старая конфигурация предварительно удаляется. При слиянии команды новой конфигурации добавляются к командам старой, как если бы они вводились вручную.

Ниже приведен список команд копирования конфигурации, первая из которых выполняется в режиме перезаписи, а последняя в режиме слияния:

- router#**copy running-config startup-config;**

- router#**copy startup-config running-config.**

Рассмотрим базовые команды получения информации о работе оборудования и его подсистем.

Просмотр информации об оборудовании (модель, объемы памяти, версия IOS, число и тип интерфейсов) выполняется по следующей команде:

- router#**show version.**

Просмотр содержимого флэш-памяти:

- router#**show flash.**

Мониторинг загрузки процессора:

- router#**show processes.**

Рассмотрим основные команды первоначальной конфигурации маршрутизатора.

Установить имя маршрутизатора:

- router(config)#**hostname** *my_router.*

Установить пароль администратора, требуемый при переходе в вводе команды *enable*:

- router(config)#**enable secret** *my_secret.*

Отключение разрешения DNS-имен:

- router(config)#**no ip domain-lookup.**

Базовая настройка FastEthernet-интерфейса:

- router#**configure terminal;**
- router(config)#**interface fastEthernet 0/1;**
- router(config-if)#**ip address 192.168.0.1 255.255.255.0;**
- router(config-if)#**speed 100;**
- router(config-if)#**duplex full;**
- router(config-if)#**no shutdown;**
- router(config-if)#**exit.**

Для последовательного интерфейса устройства, выполняющего роль DCE,

необходимо указывать тактовую частоту (пропускную способность), при этом данная команда выполняется только на одной стороне линии связи:

- router(config)#**interface serial0;**

- router(config-if)#**clock rate 125000.**

Если на последовательном интерфейсе необходимо использовать другой протокол 2-го уровня (например, Frame Relay), то это делается с помощью команды:

- router(config-if)#**encapsulation frame-relay.**

Параметры интерфейсов, протоколов 2-го уровня, а также статистика отправленных и полученных кадров может быть просмотрена следующей командой в режиме администратора:

- router#**show interface.**

Подробная информация о параметрах протокола IP доступна в режиме администратора по команде:

- router#**show ip interface** *interface.*

Краткая сводная таблица состояний IP-интерфейсов:

- router#**show ip interface brief.**

Рассмотрим настройку статической маршрутизации. Маршруты, ведущие в сети, к которым маршрутизатор подключен непосредственно, автоматически добавляются в маршрутную таблицу после конфигурирования интерфейса при условии, что интерфейс корректно функционирует.

Для назначения дополнительных статических маршрутов в режиме глобальной конфигурации вводится команда:

- router(config)#**ip route** *prefix mask ip_address.*

Маршрут по умолчанию (стандартный маршрут) назначается следующей командой:

-router(config)#**ip route** 0.0.0.0 0.0.0.0;

- *ip_address.*

Просмотреть таблицу маршрутов можно по команде:

- router#**show ip route.**

Задание на выполнение лабораторной работы:

1 Разработать шаблон конфигурационного файла маршрутизатора для удобства настройки, включить в него основные изученные команды.

2 Предложить набор учетных записей и прав доступа для эксплуатации маршрутизаторов в крупной корпоративной сети.

3 Изучить порядок наименование модулей линейных карт и сетевых интерфейсов на маршрутизаторах и коммутаторах Cisco.

4 Выполнить первоначальную настройку сетевых параметров ОС Cisco IOS маршрутизатора Cisco 2811 с рабочей станции администратора сети, используя данные в таблице 4 [3].

Таблица 4 - Параметры настройки маршрутизатора

Параметр	Значение
IP-адрес интерфейса FaO/0	10.194.7.1/24
IP-адрес интерфейса FaO/1	192.168.100.26/30
Стандартный шлюз	192.168.100.25
Имя маршрутизатора	R7
Домен	net.bank
Пароль доступа enable	Xkld7Hn434!2&^{A}
Локальный пользователь пароль	noc/nTefa#51

Порядок выполнения работы:

1 Подключить к маршрутизатору Cisco 2811 рабочую станцию через консольный шнур и интерфейс RS-232.

2 Запустить терминальный клиент и проверить правильность параметров его настройки.

3 Просмотреть список команд пользовательского режима.

Выполнить команду:

- router>**show version.**

4 Перейти в административный режим, выполнив команду:

- router>**enable.**

5 Просмотреть уровень доступа в системе и текущую конфигурацию:

- router#**show privilege;**

- router#**show running-config.**

6 Просмотреть список доступных команд. Определить и выполнить все возможные информационные команды. Например:

– router#**show flash;**

– router#**show version;**

– router#**show logging.**

7 Выполнить настройку маршрутизатора в соответствии с указанными параметрами, выполнив следующие команды:

– **configure terminal;**

– **hostname R7;**

– **interface fastEthernet 0/1;**

– **ip address 192.168.100.26 255.255.255.252;**

– **no shutdown;**

– **interface fastEthernet 0/0;**

– **ip address 10.194.7.1 255.255.255.0;**

– **no shutdown;**

– **ip domain-name net.bank;**

– **ip route 0.0.0.0 0.0.0.0 192.168.100.25.**

8 Сохранить конфигурацию маршрутизатора, выполнив команду:

- write memory.

9 Выключить питание маршрутизатора. Установить сетевой модуль NM-ESW161. Включить питание маршрутизатора. Проверить возможность загрузки маршрутизатора с новой конфигурацией.

10 Просмотреть список всех портов и их имен:

- sh ip interface brief.

11 Выполнить следующие команды и просмотреть их результаты:

- sh processes;

- sh file systems.

12 Выключить режим шифрования паролей в конфигурационном файле, создать пользователя и убедиться, что пароль в конфигурационном файле записан в открытом виде, затем включить режим шифрования паролей и убедиться, что теперь пароль представляется в зашифрованном виде:

- **no service password-encryption;**
- **username noc1 secret test;**
- **username noc2 password test;**
- **enable secret test2;**
- **show running-config;**
- **service password-encryption;**
- **show running-config.**

13 Удалить всех созданных ранее пользователей, задать стойкие к перебору пароли пользователей и пароли для администра тивного доступа. Проверить, что для подключения к маршрутизатору и перехода в административный режим требуется пароль:

- **line console 0;**
- **password n&bbR4d21;**
- **login;**
- **no username noc1;**
- **no username noc2;**
- **enable secret xkld7Hn434!2&^;**
- **username noc secret nTefa#51.**

14 Выполнить настройку механизма ролевого управления доступа к командам маршрутизатора, реализующего следующую политику безопасности.

Существуют следующие роли и соответствующие им уровни безопасности: администратор (15), инженер (5) и оператор (3). Доступ пользователям, авторизованным на роль инженера, может быть предоставлен только через

консольную сессию. При этом могут быть выполнены основные команды по диагностике и настройке средств маршрутизации, коммутации и адресации.

Пользователи, авторизованные на роль оператора, могут только просматривать диагностические данные на маршрутизаторе. Роль администратора имеет все привилегии:

- **username admin privilege 15 secret nTefa#51;**
- **enable secret 15 secret Rc@sxa&h;**
- **username engineer privilege 5 secret LwqndhR5;**
- **enable secret 5 secret Jnfbn&gd;**
- **username operator privilege 3 secret *mmfjj&D;**
- **enable secret 3 secret Mf88MMh1;**
- **privilege exec level 3 show running-config;**
- **privilege exec level 3 show startup-config;**
- **privilege exec level 3 show;**
- **privilege exec level 3 ping;**
- **privilege exec level 3 ssh;**
- **privilege exec level 3 telnet;**
- **privilege exec level 3 exit;**
- **privilege exec level 5 configure terminal;**
- **privilege exec level 5 configure;**
- **privilege configure level 5 ip;**
- **privilege configure level 5 no ip;**
- **privilege configure level 5 ip route;**
- **privilege configure level 5 no ip route;**
- **privilege configure level 5 router;**
- **privilege configure level 5 no router;**
- **privilege configure level 5 interface;**
- **line console 0;**
- **privilege 3.**

Содержание отчёта:

1 Цель работы.

2 Задание.

3 Результаты выполнения работы.

4 Выводы.

7 Лабораторная работа № 7. Идентификация операционных систем

Цель работы.

Целью лабораторной работы является обучение современным методам и средствам идентификации ОС анализируемой КС.

Краткие теоретические сведения.

Задача определения типа и версии ОС удаленного узла весьма актуальна при проведении анализа защищённости. Чем точнее идентификация ОС исследуемого узла, тем эффективнее может быть выполнена его проверка. Более того, в некоторых сканерах безопасности набор выполняемых проверок зависит от результатов идентификации ОС.

В настоящее время идентификация ОС основана на следующих основных методах:

− анализ заголовков, полей IP-дейтаграмм и набора открытых портов, характерных для каждой ОС;

− опрос стека TCP/IP, впервые реализованный в сканерах queso и nmap;

− анализ ICMP-дейтаграмм, впервые реализованный в сканере xprobe;

− анализ реализации таймеров в механизме повторной передачи протокола TCP;

− анализ значений полей IP- и TCP-пакетов, реализованный в сканере SinFP.

Точность определения ОС существенно зависит от наличия устройств нормализации сетевых пакетов, межсетевых экранов, систем обнаружения

вторжений, прокси-серверов и других сетевых средств защиты информации. Кроме того, серьезную задачу представляет собой распознавание ОС одного семейства [3].

Задание на выполнение лабораторной работы.

Выполнить идентификацию ОС узлов сети и анализ возможностей сетевых сканеров.

Порядок выполнения работы:

1 Загрузить виртуальную машину TWS1. Войти в систему (логин: root, пароль: toor). Настроить сетевые интерфейсы. Запустить анализатор протоколов tcpdump или wireshark.

2 С помощью утилиты hping2 исследовать значения полей TTL в IP-заголовке и Window в TCP-заголовке для ОС семейства GNU/Linux и Windows соответственно:

- hping2 –S –c 1 –p 80 172.16.8.11;

- hping2 –S –c 1 –p 25 172.16.8.51.

3 С помощью сетевого сканера nmap выполнить идентификацию ОС методом опроса стека TCP/IP:

- nmap –O 172.16.8.51 –vv;

- nmap –O 172.16.8.11 –vv.

Исследовать используемые тесты и механизмы сетевого сканера nmap. Проанализировать результаты.

4 С помощью сетевого сканера xprobe выполнить идентификацию ОС с использованием опроса модуля ICMP:

- xprobe2 172.16.8.11;

- xprobe2 -v 172.16.8.51.

Проанализировать результаты сканирования, сравнить с результатами использования сканера Nmap. Проанализировать трассировки.

5 Выполнить шаги 3 и 4, настроив МЭ серверов S1 и S2 на фильтрацию некоторых используемых портов и протоколов.

6 На узле TWS2 перейти в консоль XSpider. Обратить внимание на результаты определения ОС в ходе предыдущих сканирований. В используемом профиле

сократить диапазон портов до 1 – 30 и выполнить повторное сканирование. Убедиться, что ОС не определена. Прокомментировать данные результаты.

7 В профили сканирования включить опции «Искать уязвимости», «Искать скрытые каталоги». Выполнить сканирование. Убедиться в том, что ОС идентифицирована.

8 Определить методы, использованные сканером XSpider для идентификации ОС в процессе сканирования, путем изучения трассировок и файлов регистрации сканирования.

Содержание отчёта:

1 Цель работы.

2 Задание.

3 Результаты выполнения работы.

4 Выводы.

8 Лабораторная работа № 8. Идентификация уязвимостей сетевых приложений по косвенным признакам

Цель работы.

Целью лабораторной работы является обучение методам и средствам идентификации уязвимостей по косвенным признакам в сетевых приложениях КС.

Краткие теоретические сведения.

Уязвимостями КС принято называть любые их характеристики и свойства, использование которых нарушителем может привести к реализации угрозы. Существует множество вариантов классификации уязвимостей, например, по уровню инфраструктуры КС, по этапу жизненного цикла КС, по типу уязвимости и т.д.

В настоящее время информация об обнаруженных уязвимостях достаточно систематизирована, существует несколько общеизвестных источников, где эта информация представлена, например:

− http://xforce.iss.net – база данных компании IBM Internet Security Systems;

− http://www.kb.cert.org/vuls – база данных координационного центра CERT;

− http://www.securityfocus.com/bid – информация об обнаруженных уязвимостях с подробными пояснениями;

− http://www.ptsecurity.ru/lab/advisory – база данных ЗАО «Позитив Текнолоджис»;

− http://www.securitylab.ru/vulnerability;

− http://www.securitytracker.com.

Общепринятая система обозначений уязвимостей представлена в двух каталогах:

− http://cve.mitre.org/cve;

− http://nvd.nist.gov.

Инструментальный анализ защищенности, как правило, включает автоматизированный поиск уже известных уязвимостей в КС или, иначе, сканирование уязвимостей с помощью проверок, выполняемых сканером безопасности. Все проверки делятся на заключения и тесты [3].

Заключение (логический вывод) – это алгоритм определения наличия уязвимости в КС без выполнения атаки, использующей данную уязвимость, по косвенным признакам, на основе собранной информации. Иначе говоря, вывод о наличии уязвимости в КС делается на основе каких-либо характерных признаков (номер версии службы, версия ОС, присутствие на узле какого-либо файла и т.п.).

При этом используются данные, полученные на этапах идентификации открытых портов, служб, приложений в КС. Среди заключений выделяют локальные и «баннерные» проверки.

Тест – это алгоритм определения наличия уязвимости в КС путём выполнения атаки, использующей данную уязвимость, либо путём специальных запросов в отношении КС, позволяющих с высокой степенью вероятности утверждать о наличии уязвимости.

Таким образом, сканирование уязвимостей – это выполнение набора проверок, состоящих из тестов и заключений.

Сетевые службы и реализующие их приложения являются одним из основных объектов анализа защищённости, выполняемого сетевыми сканерами. После того, как в ходе сбора данных были определены открытые порты, соответствующие им службы и реализующие их приложения, начинается этап идентификации уязвимостей. Значительная часть проверок, направленных на выявление уязвимостей сетевых служб, таких, как DNS, HTTP, SSH, FTP – это «баннерные» проверки.

В силу того, что результат «баннерных» проверок зависит от многих факторов, при «верификации» найденных уязвимостей рекомендуется использовать следующие приёмы:

− ручная проверка службы (подключение на заданный порт, анализ баннера, использование команд прикладного уровня);

− поиск информации об уязвимости в различных базах;

− локальная проверка (версия, конфигурационные файлы);

− проверка действительного существования уязвимости.

Данный вариант инструментального анализа защищенности в зарубежной литературе часто называется оценкой защищенности [3].

Задание на выполнение лабораторной работы.

Выполнить идентификацию уязвимостей сетевых служб DNS, HTTP и SSH по косвенным признакам с помощью сканера XSpider.

Порядок выполнения работы:

1 Создать профиль сканирования «Сканирование Apache». Перечень сканируемых портов ограничить портом 80. Отключить сканирование служб UDP, в секции «Определение уязвимостей» отключить опции «Использовать финальные проверки», «Проверять на известные DoS-атаки», «Проверять на новые DoS-атаки».

2 В секции «HTTP» включить опцию «Включить анализатор директорий», остальные опции отключить. В секции «Анализатор контента» включить опцию «Не выходить за пределы стартовой страницы». В секции «Анализатор сценариев» оставить опцию «Искать уязвимости в GET запросах», отключить остальные опции. В секциях «Типы уязвимостей» и «Методы поиска» отключить все опции. В секции

«Подбор учётных записей» отключить опцию «Подбирать учётные записи». Сохранить профиль.

3 Создать задачу «Сканирование Linux», добавить в нее узел S1. Запустить на сканирующем узле анализатор протоколов. Выполнить сканирование узла S1. Обратить внимание на уязвимости, найденные на порту 80 веб-сервера Apache, а также на результаты идентификации службы HTTP. Найти результаты работы анализатора каталогов. Проверить наличие найденных уязвимостей вручную. Просмотреть трассировку сканирования в анализаторе протоколов.

4 Войти в ОС GNU/Linux сервера S1 (логин: root, пароль: 111111). Открыть для редактирования файл /etc/httpd/conf/httpd.conf. Найти директиву ServerTokens и присвоить ей значение ProductOnly. Перезапустить службу httpd, выполнив команду:

- service httpd reload.

5 Выполнить повторное сканирование сервера S1. Проанализировать результаты. Обратить внимание на результаты идентификации приложения.

6 Открыть для редактирования файл /etc/httpd/conf/httpd.conf и закомментировать директиву ServerTo kens. Перезапустить службу httpd. Вновь выполнить сканирование, проанализировать результаты.

7 Создать копию профиля «Сканирование Apache», задать ему имя «Сканирование сетевых служб». Перечень сканируемых портов ограничить портами 22 и 53. В секции «Сканер UDP-сервисов» отключить все опции, кроме DNS. Сменить профиль для задачи «Сканирование Linux».

8 Убедиться, что на сервере S1 служба DNS запущена. Выполнить сканирование сервера S1. Просмотреть результаты, обратить внимание на уязвимость CVE-2008-1657, изучить её описание. Определить версию ПО SSH командой:

- ssh –v.

Просмотреть описание уязвимости в базе securityfocus. Сравнить номера версий, сделать вывод о действительном существовании уязвимости.

9 Войти в ОС GNU/Linux сервера S1 (логин: user, пароль: abc123). Вывести содержимое какого-либо каталога, например, /tmp. Создать каталог .ssh, в нем

создать файл rc и вписать туда команду «ls /tmp». Выполнить команду:

- ssh localhost.

Проверить, что при входе выполняется команда, указанная в файле ~/.ssh/rc.

10 Выйти из ОС. Войти в ОС с правами учетной записи root. Отредактировать файл /etc/ssh/sshd_config, добавив в конец файла строку ForceCommand ls /usr. Перезапустить службу SSH. Выйти из ОС. Войти в ОС с правами учетной записи user. Выполнить команду:

- ssh localhost.

Убедиться, что после входа выполняются обе команды, при этом пользовательская команда выполняется первой.

10. Проанализировать результаты сканирования службы DNS, обратить внимание на версию BIND. Выполнить ручную проверку наличия уязвимостей, использую средство nslookup:

- **C:>nslookup;**
- **>server 172.16.8.11;**
- **>set class=chaos;**
- **>set test=txt;**
- **>version.bind.**

Выполнить запрос authors.bind:

- **>authors.bind.**

Проверить версию ПО bind, выполнив команду:

- **named –v.**

Проверить установленную версию пакета bind:

- **rpm –q bind.**

В файле /var/named/chroot/named.conf вписать строку version. Перезапустить службу DNS:

- **service named restart.**

Проверить работу команды **version.bind**. Выполнить повторное сканирование. Просмотреть результаты, обратить внимание на результат определения версии bind.

Содержание отчета:

1 Название и цель работы.

2 Краткая теоретическая справка.

3 Результаты проделанной работы (этапы, экранные формы, расчеты и т.д.).

4 Выводы по выполненной работе.

5 Список использованных источников.

9 Лабораторная работа № 9. Исследование системы защиты корпоративной информации на основе ПО «Secret Disk»

Цель работы.

Приобрести навыки в построение системы защиты информации от несанкционированного доступа на основе ПО «Secret Disk»

Краткие теоретические сведения.

Основные характеристики системы «Secret Disk».

Линейка аппаратно-программных средств криптографической защиты информации «Secret Disk», разработанная компанией ALADDIN Software Security R.D. (г. Москва), является менеджером секретных дисков и предназначена для шифрования разделов жесткого диска и создания на дисковом пространстве компьютера защищенных виртуальных дисков с многопользовательским доступом. Для работы с дисками в состав системы входит VXD-драйвер.

Система «Secret Disk» работает только в режиме двухфакторной аутентификации пользователей, когда наряду с вводом пароля пользователь обязан подключить к ПЭВМ внешний носитель ключевой последовательности (eToken в виде USB-ключа или смарт-карты или электронный ключ PCCard (PCMCIA) для портативных компьютеров).

В «Secret Disk 2.0» для шифрования данных могут использоваться следующие алгоритмы:

– собственный алгоритм преобразования данных системы «Secret Disk»;

– криптографический алгоритм ГОСТ 28147–89 (программный эмулятор

криптографической платы Криптон фирмы «Анкад»);

– алгоритм RC4, встроенный в ОС Windows (Microsoft CryptoAPI).

Хранение секретной информации на съемных носителях.

В СЗКИ «Secret Disk» предусмотрен режим работы в качестве архиватора, который не только сжимает, но и шифрует данные. Данный режим полезен, если необходимо перенести секретную информацию на сменном носителе на другой компьютер, где также установлена СКЗИ «Secret Disk». Программа архивации позволяет выбрать ключ шифрования и перечень шифруемых файлов. В результате будет создан файл архива, содержащий указанные файлы в зашифрованном и (при необходимости) сжатом видах и готовый для переноса на другой компьютер. На рисунке 60 показано окно архивации данных в СЗКИ «Secret Disk».

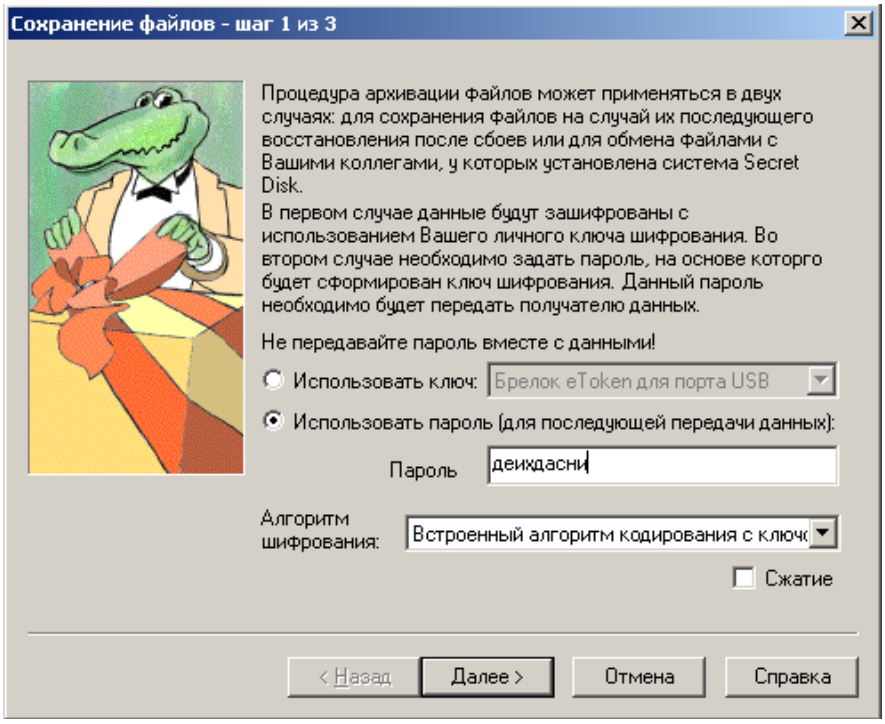

Рисунок 60 - Архивация данных в СЗКИ «Secret Disk»

В качестве ключа шифрования «Secret Disk» позволяет использовать либо личный ключ, хранящийся в электронном идентификаторе, либо пароль. Если файл не предназначен для отправки иному лицу, а должен храниться на съемном носителе, то в качестве ключа рекомендуется использовать личный ключ. Если

предполагается передача файла иному лицу, то ключом шифрования должен быть пароль. Вместе с тем возникает проблема передачи этого секретного пароля, так как при шифровании применяется симметричная схема.

Следует отметить, что режим архивации нельзя использовать для обработки (чтения, модификации) документов, так как в процессе редактирования на носителе будет создан «технологический мусор», содержащий секретные данные в открытом виде.

Инициализация системы «Secret Disk».

В процессе установки системы «Secret Disk 2.0» необходимо указать имеющийся в наличии носитель ключевой информации, выбрав соответствующий пункт в окне «Выбор компонентов», как на рисунке 61. После установки и перезагрузки компьютера будет запущен «Мастер первого запуска», который предложит создать на жестком диске защищенный виртуальный диск.

При этом необходимо активизировать электронный ключ, на котором будет храниться ключевая информация для доступа к создаваемому диску. Эта ключевая информация в СКЗИ «Secret Disk» называется «личным ключом».

Для активизации следует подключить по запросу СКЗИ носитель eToken к USB-порту, а затем сгенерировать случайную последовательность путем нажатия произвольных клавиш или перемещением «мыши», как на рисунке 62. Сгенерированный личный ключ будет записан в перепрограммируемую составляющую носителя eToken. Обратим внимание, что в результате будет уничтожен ранее записанный на eToken личный ключ, который, возможно, уже применялся при шифровании пользовательских данных. В связи с возможным ошибочным уничтожением личных ключей в СКЗИ предусмотрена возможность сохранения личного ключа в виде файла на ином носителе (например, на дискете) для последующего восстановления. После активации ключа соответствующее предупреждение выводится на экран.

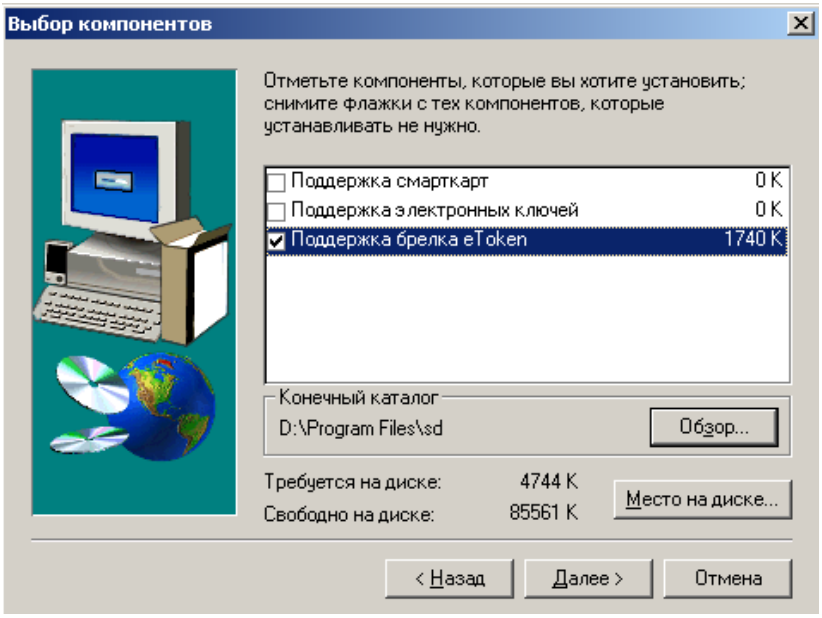

Рисунок 61 - Выбор электронного ключа

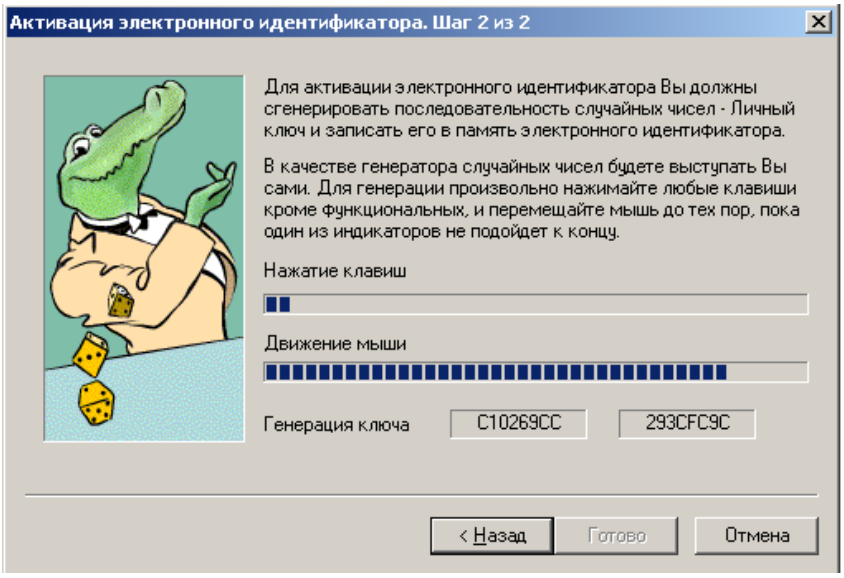

Рисунок 62 - Генерация личного ключа

Создание защищенных логических дисков.

«Мастер первого запуска» предлагает создать защищенный виртуальный диск. В качестве параметров виртуального диска необходимо указать имя файла и каталога, где он будет создан, объем создаваемого диска, пароль доступа к информации на диске, тип используемого электронного ключа, алгоритм

шифрования данных, а также пароль для входа под принуждением.

Отдельно задаваемым параметром является ключ шифрования данных (называемый в СКЗИ «рабочим ключом»), который будет храниться в заголовке файла-образа диска в зашифрованном виде. Рабочий ключ создается как генерируемая случайным образом последовательность символов и показан на рисунке 64.

СКЗИ «Secret Disk» рекомендует сделать резервную копию сгенерированного рабочего ключа на внешнем носителе (дискете), хранить который необходимо в защищенном месте (в сейфе). Эта резервная копия будет содержать рабочий ключ в виде незашифрованного файла, с помощью которого при необходимости (потере электронного ключа или пароля) можно будет получить доступ ко всей информации на зашифрованном диске. Окно параметров виртуального диска показано на рисунке 63.

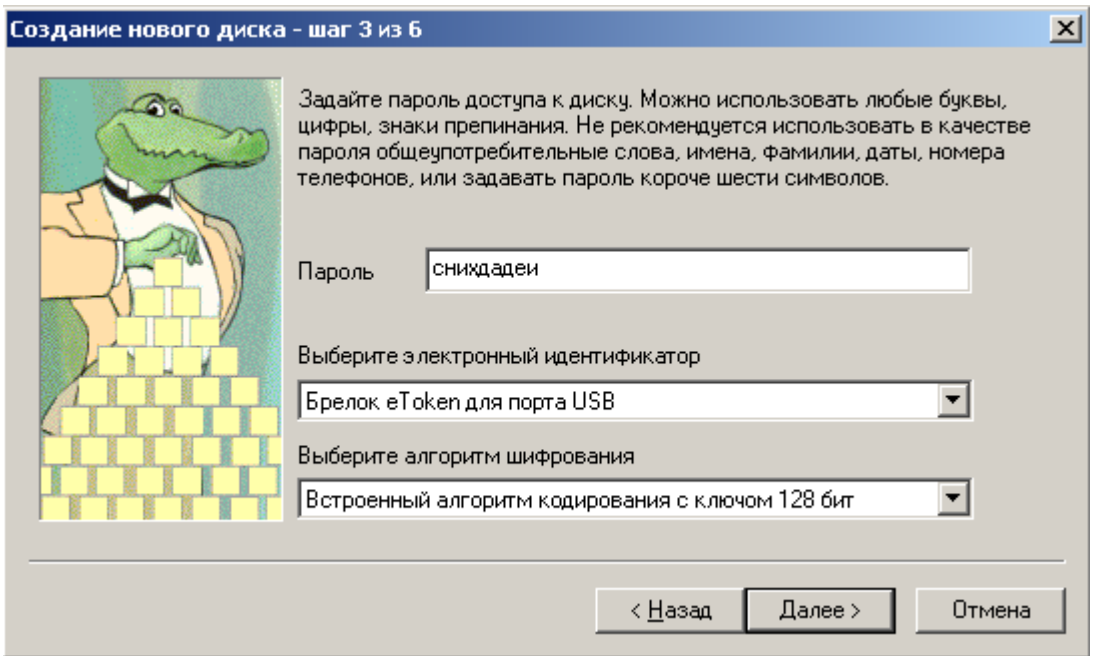

Рисунок 63 - Параметры виртуального диска

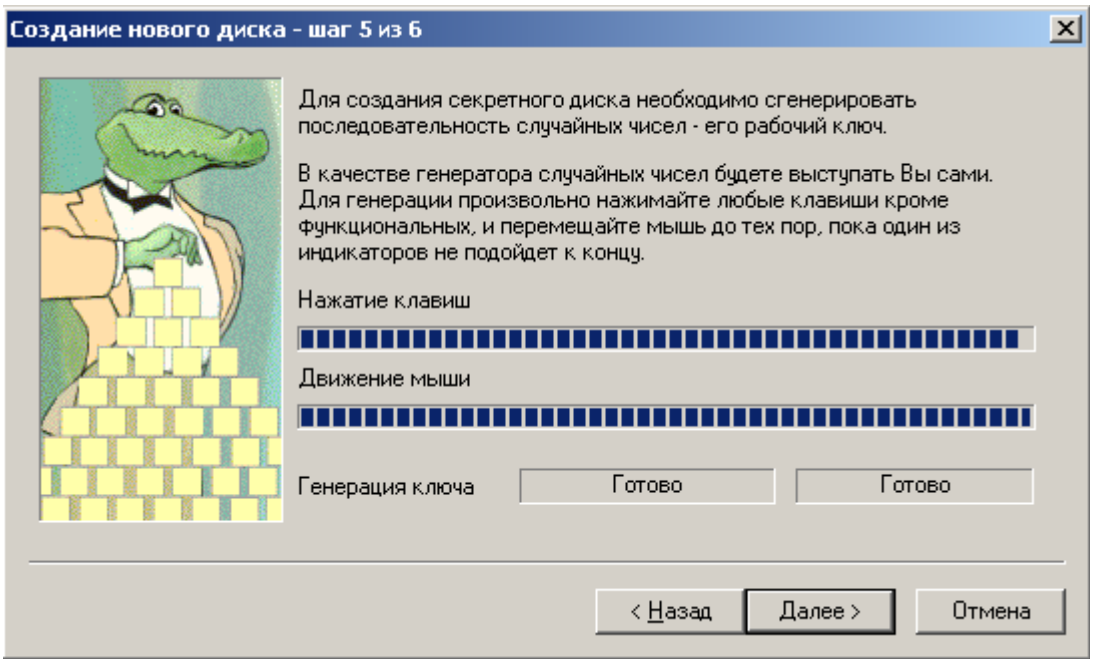

Рисунок 64 - Генерация ключа шифрования данных

Основная копия рабочего ключа будет храниться в заголовке файла-образа диска в зашифрованном виде, а ключом для ее расшифрования будет являться совокупность пароля и личного ключа (который хранится на eToken).

Таким образом, безопасному хранению внешних носителей, содержащих резервные копии рабочих ключей, должно уделяться особое внимание. Ни в коем случае не должно быть допущено резервное сохранение рабочих ключей на основном носителе.

Работа с защищенными дисками.

После создания файл-образ диска может быть подключен. Для этого необходимо подключить электронный ключ и ввести пароль. При их совпадении в системе появится дополнительный логический диск, работа с которым осуществляется как с обычным съемным носителем.

Подключение секретного диска показано на рисунке 65, а виртуального диска F нарисунке 66.

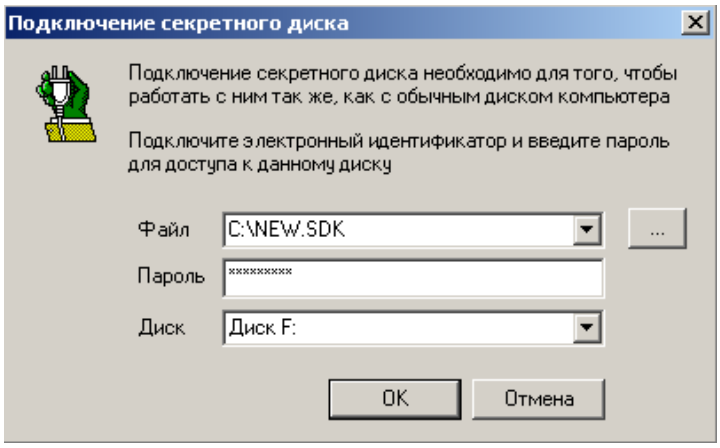

Рисунок 65 - Подключение секретного диска

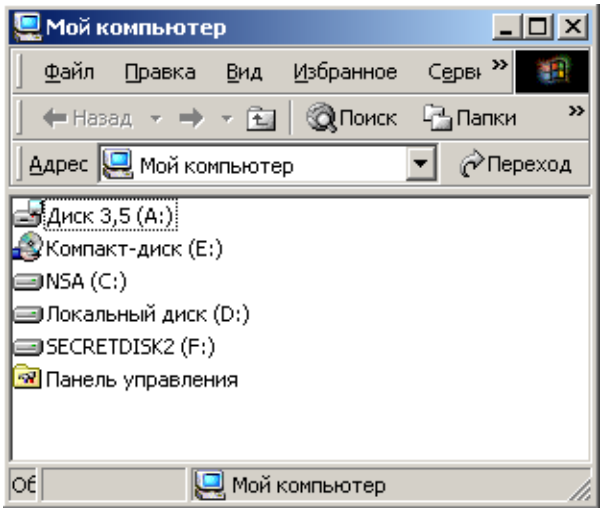

Рисунок 66 - Виртуальный диск F

СКЗИ «Secret Disk» позволяет организовать многопользовательский доступ к зашифрованной информации. Пользователь, создавший диск, может разрешить доступ к своему диску любому иному пользователю, имеющему электронный ключ. Для этого необходимо подключить электронный ключ добавляемого пользователя, в результате чего будет сделана еще одна копия рабочего ключа в заголовке файла-образа, но уже зашифрованная с использованием личного ключа добавляемого пользователя. Окно многопользовательского режима доступа показано на рисунке 67, а добавление нового пользователя на рисунке 68.

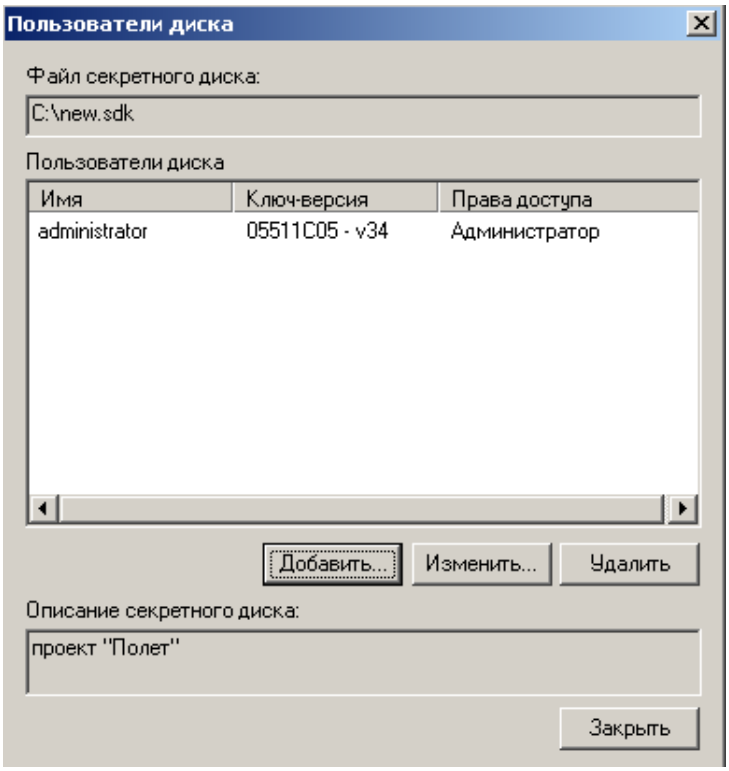

Рисунок 67 - Многопользовательский режим доступа

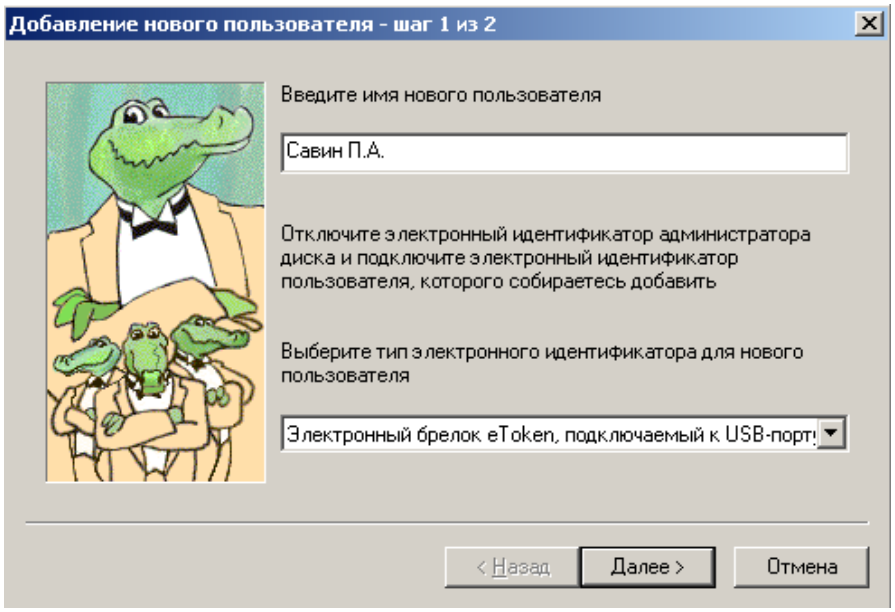

Рисунок 68 - Добавление нового пользователя

Порядок выполнения работы:

1 Установить и активировать СКЗИ «Secret Disk», используя электронный

ключ eToken. Сделать резервную копию электронного ключа на внешний носитель.

2 Создать в корневом каталоге диска «C:\» файл-образ защищенного диска. Сделать резервную копию рабочего ключа на внешний носитель.

3 Подключить защищенный диск. Создать на диске простой текстовый документ и документ Word, отключить диск. Просмотреть содержимое файлаобраза диска всеми доступными средствами, включая дисковый редактор.

Настройка СКЗИ «Secret Disk».

Настройка СКЗИ «Secret Disk» производится в окне «Параметры системы» и заключается в установке ряда параметров для обеспечения безопасности данных при наступлении «форс-мажорных» обстоятельств. Если пользователь отлучился на продолжительное время либо извлек электронный ключ, не отключив секретный диск, система самостоятельно через определенное время может включить блокировку экрана программой-заставкой. Для абсолютного блокирования доступа к секретным данным применяется режим «Красной кнопки», когда при нажатии специально задаваемой комбинации клавиш не только отключаются все секретные диски, но и стирается информация из подключенных электронных ключей. Настройка режима блокировок показана на рисунке 69.

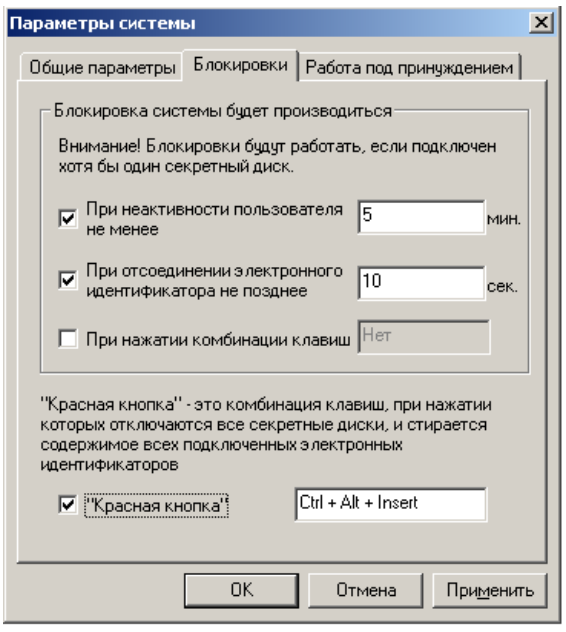

Рисунок 69 - Настройка режима блокировок

Стирание ключевой информации может произойти и в режиме работы под принуждением. Данный режим включается, когда в процессе подключения секретного диска будет введен специально заданный пароль. Кроме стирания информации из электронного ключа может имитироваться «зависание» компьютера, как на рисунке 70.

Порядок выполнения работы:

1 Установить минимально допустимое время неактивности пользователя, подключить диск, открыть документ для редактирования и проконтролировать блокировку экрана по истечении этого времени.

2 Назначить «горячие клавиши» для включения режима «Красная кнопка». Подключить секретный диск, открыть для редактирования имеющийся на нем текстовый документ, внести в документ изменения и включить режим «Красная кнопка». Попытаться вновь подключить секретный диск.

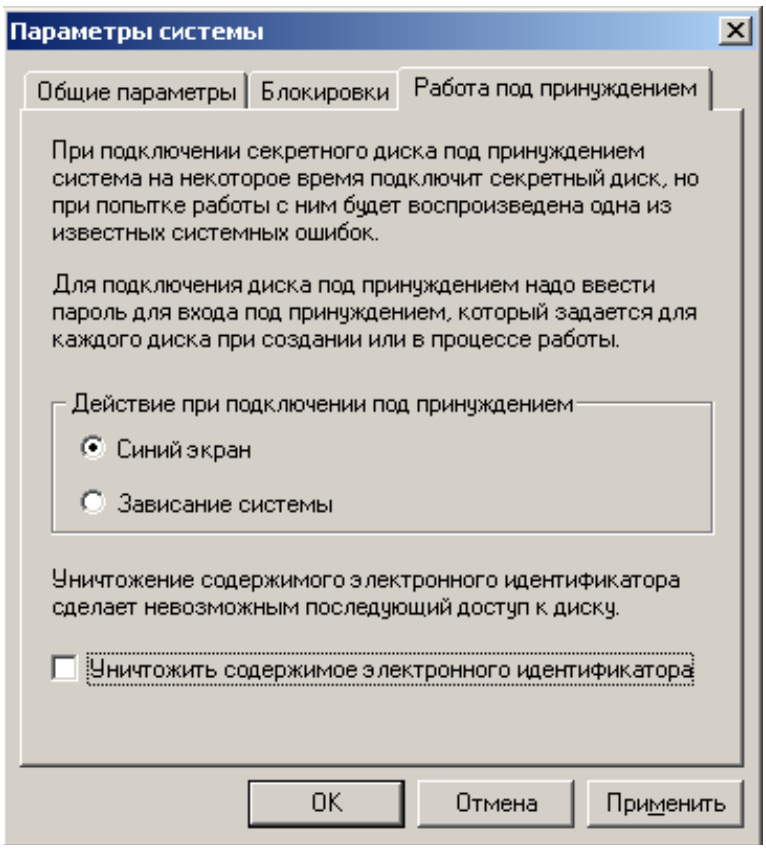

Рисунок 70 - Настройка режима работы под принуждением

Содержание отчета:

1 Название и цель работы.

2 Краткая теоретическая справка.

3 Результаты проделанной работы (этапы, экранные формы, расчеты и т.д.).

4 Выводы по выполненной работе.

5 Список использованных источников.

10 Лабораторная работа № 10. Исследование системы защиты информации от несанкционированного доступа на основе ПО «Страж NT»

Цель работы.

Приобрести навыки в построение системы защиты информации от несанкционированного доступа на основе ПО «Страж NT»

Краткие теоретические сведения.

СЗИ «Страж NT» версии 2.5 (разработчик ЗАО НПЦ «Модуль») представляет собой программно-аппаратный комплекс, способный работать в среде операционных систем фирмы Microsoft Windows NT 4.0, Windows 2000, Windows XP и Windows 2003 и добавляющий к системе безопасности ОС следующие функциональные возможности:

1 Организация доверенной загрузки с возможностью идентификации и аутентификации пользователей при помощи дискет, устройств iButton, USB-ключей eToken R2, eToken Pro, Guardant.

2 Реализация мандатной модели разграничения доступа на основе меток конфиденциальности пользователей, защищаемых ресурсов и прикладных программ.

3 Создание замкнутой программной среды для пользователей путем разрешения запуска ограниченного количества прикладных программ и динамических библиотек.

4 Контроль потоков защищаемой информации.

5 Очистка освобождаемой памяти и дискового пространства.

6 Контроль целостности указанных администратором файлов.

7 Аудит доступа к защищаемым ресурсам.

8 Управление вводом-выводом на отчуждаемые носители.

Запуск и регистрация в системе защиты.

Установка системы защиты должна производиться пользователем из группы администраторов. Политикой безопасности предприятия должен быть предусмотрен один привилегированный пользователь, выполняющий обязанности системного администратора и администратора безопасности. В соответствии с разработанной политикой безопасности установку СЗИ «Страж NT» должен производить именно этот пользователь. Целесообразно использовать в качестве учетной записи встроенную учетную запись Администратора. После инсталляции системы защиты, администратор получит права по настройке и управлению как СЗИ, так и операционной системой. Перед инсталляцией необходимо убедиться, что пароль Администратора не содержит символов кириллицы и специальных знаков, а его длина не превышает 14 символов.

Установка системы производится стандартным образом. В ходе установки необходимо ввести лицензионный номер. После завершения копирования файлов на жесткий диск будет предложено выбрать тип используемого персонального идентификатора и ввести пароль администратора безопасности, после чего будет создан его персональный идентификатор, для чего потребуется «чистый» идентификатор, например, отформатированная дискета.

Практическое освоение средства защиты информации «Страж NT» осуществляется с предварительно установленном экземпляром СЗИ в виде образа системы VMware, в котором по умолчанию имеется только один пользователь – «Администратор». Поскольку у многих современных компьютеров дисковод для флоппи-дисков просто отсутствует, в качестве ключевой дискеты при работе с СЗИ «Страж NT» следует использовать ее электронный образ, хранящийся в одном каталоге вместе с образом самой системы в виде файла с именем «дискета».

Для реализации функций защиты в СЗИ «Страж NT» необходимо настроить

BIOS ПЭВМ на загрузку с жесткого диска, а также установить пароль на изменение параметров BIOS, чтобы эти настройки не могли быть модифицированы пользователями, в противном случае становится возможна загрузка ПК со съемного носителя. Если требуемые установки BIOS не выполнены, СЗИ при запуске системы выведет соответствующее сообщение и приостановит ее дальнейшую работу.

В СЗИ «Страж NT» идентификация и аутентификация пользователя производится до загрузки операционной системы. Это позволяет исключить возможность получения доступа к информации, содержащейся на жестком диске компьютера, не пройдя успешно процедуру аутентификации. Процедура идентификации предполагает сравнение информации, содержащейся на энергонезависимом носителе ключевой информации (дискете), с информацией, записанной на жестком диске компьютера.

Программа идентификации и аутентификации записана в главной загрузочной записи (MBR) жесткого диска и вызывается автоматически после прохождения процедуры POST BIOS: пользователю предлагается предъявить персональный идентификатор и ввести пароль.

Модификация главной загрузочной записи, выполняемая СЗИ при его инициализации, предотвращает попытки НСД при загрузке компьютера с внешнего носителя, так как любая операционная система «повиснет» при попытке монтирования раздела, на котором установлена СЗИ «Страж NT». Таким образом, для злоумышленника исключается несанкционированный доступ к содержимому жесткого диска, несмотря на гипотетическую возможность загрузки ПЭВМ с внешнего носителя или подключения НЖМД к другому ПК.

Порядок выполнения работы:

1 Зарегистрироваться в системе пользователем Администратор, предъявив при включении компьютера (перезагрузке) ключевую дискету (в VMware чтение дискеты будет осуществляться автоматически при загрузке операционной системы, если в свойствах образа ОС заранее указан образ дискеты.) введя пароль «12345».

2 Попытаться загрузить компьютер без ключевой дискеты, затем вставить флешку и три раза подряд неправильно ввести пароль.

Задача № 1. Создание пользователей:

1 В «Страж NT» возможны две стратегии создания учетных записей пользователей. Первая предполагает создание всех требуемых пользователей до установки СЗИ, а вторая – создание пользователей после установки средства защиты. После установки СЗИ все операции по созданию и удалению пользователей, а также по назначению им прав доступа производятся Администратором безопасности с использованием «Менеджера пользователей» программы «Управление СЗИ», которая вызывается командой **Пуск ⇒ Программы ⇒ Страж NT ⇒ Управление СЗИ**. Менеджер пользователей открывается командой меню **Администрирование ⇒ Менеджер пользователей**, как показано на рисунке 71.

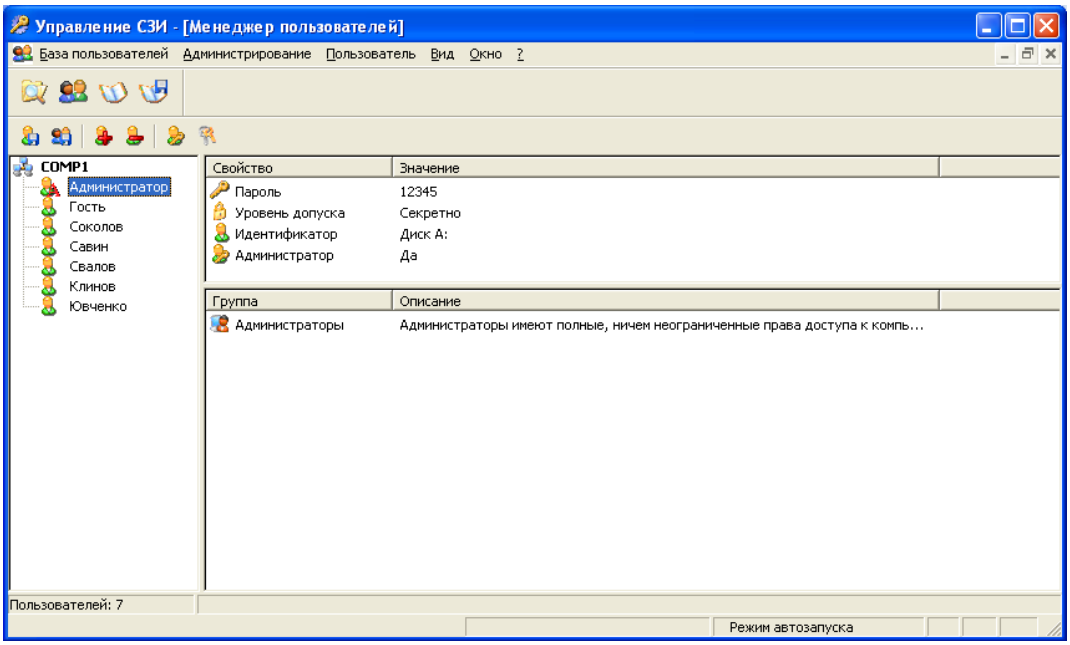

Рисунок 71 - Менеджер пользователей

В случае создания пользователей до установки СЗИ (штатными средствами ОС Windows) после установки необходимо установить уровни допуска для каждого из пользователей, задать пароли и создать персональные идентификаторы (сформировать носители ключевой информации).

3 В рассматриваемом примере построения защищенной системы учетные записи пользователей будут создаваться после установки СЗИ. Чтобы создать учетную запись с использованием «Менеджера пользователей», необходимо выполнить команду меню **Пользователь ⇒ Добавить пользователя**, после чего ввести имя вновь создаваемого пользователя. В правой верхней части окна отображается информация о выделенной учетной записи. Чтобы задать для нее пароль, необходимо щелкнуть на поле «Значение» строки «Пароль», а затем ввести новый пароль и подтвердить его.

При вводе пароля его значение отображается на мониторе в открытом виде (в том числе у Администратора), поэтому существует повышенная опасность его подсматривания, в том числе преднамеренного. Любые изменения в параметрах учетной записи пользователя необходимо сохранять. Пиктограмма учетной записи пользователя, параметры которой изменились, становится красной и сдвигается вправо. Для сохранения параметров нужно выполнить команду меню **База пользователей ⇒ Сохранить** или выбрать «Сохранить» из контекстного меню, появляющегося при щелчке правой клавишей мыши на имени пользователя.

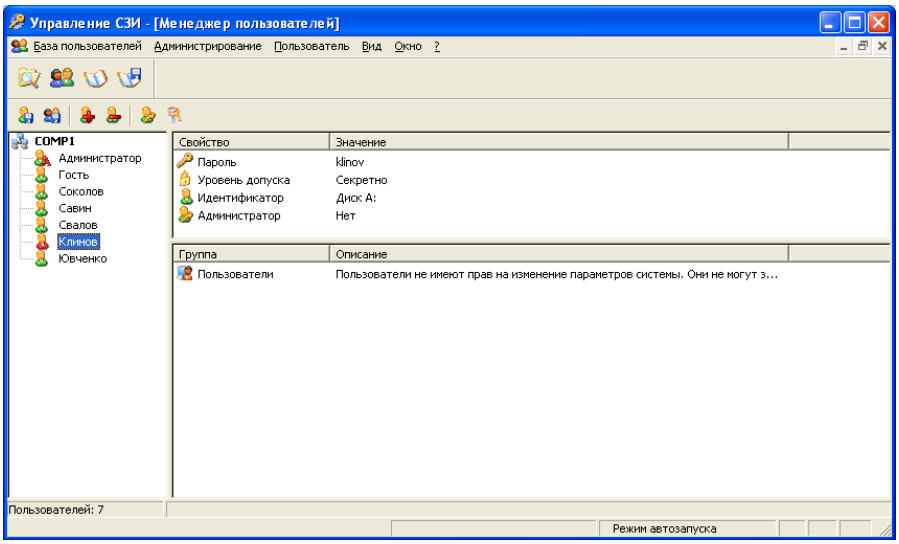

Рисунок 72 - Настройки учетной записи изменены

4 Зарегистрироваться вновь созданным пользователем не удастся, так как

личные каталоги пользователей создаются в Windows после первой регистрации пользователя в системе, а «Страж NT» охраняет каталог Documents and Settings от записи. Чтобы обеспечить возможность создания этих каталогов, необходимо временно приостановить работу механизмов защиты СЗИ «Страж NT», а затем зарегистрироваться новым пользователем в системе, не перезагружая компьютер. Остановка механизмов защиты делается выбором пункта меню «Останов» при нажатии правой кнопкой мыши на иконке СЗИ «Страж NT» в системном «Трее» и действует до следующей перезагрузки компьютера либо до выбора пункта меню «Запуск» там же. Рекомендуется сначала создать всех пользователей, приостановить механизмы защиты, а после этого последовательно зарегистрироваться в системе от имени всех вновь созданных пользователей. Все эти действия может и должен выполнить Администратор системы.

5 После того как учетные записи всех пользователей созданы, необходимо сформировать персональные идентификаторы для каждого из них. Это действие выполняется также с использованием «Менеджера пользователей». Программа «Управление СЗИ» должна находиться в режиме администрирования (команда меню **Администрирование ⇒ Режим администрирования**). Чтобы создать персональный идентификатор, необходимо выбрать пользователя, а затем выполнить команду меню **Пользователь ⇒ Сформировать идентификатор**… Система защиты попросит вставить персональный идентификатор Администратора, затем создать список доступных пользователю компьютеров, и после поместить «чистый» носитель, на который будет записана уникальная ключевая информация, и идентификатор пользователя будет создан.

Изменение уровня допуска пользователя или его пароля требуют повторного создания персональных идентификаторов.

6 Создать учетные записи пользователей и назначить им уровни допуска. Пароли выбрать произвольно. Приостановить функционирование механизмов защиты выбором пункта меню «Останов» при нажатии правой кнопкой мыши на иконке СЗИ «Страж NT» в системном «Трее». Последовательно зарегистрироваться

в системе всеми пользователями.

Задача № 2. Реализация мандатной модели разграничения доступа:

1 Мандатная модель разграничения доступа в СЗИ «Страж NT» реализована посредством назначения защищаемым ресурсам, каждому пользователю системы и прикладным программам меток конфиденциальности и сопоставления их при запросах на доступ. В качестве меток конфиденциальности выступают:

- для защищаемых ресурсов — гриф;
- для пользователей — уровень допуска;
- для прикладных программ — допуск и текущий допуск.

В СЗИ «Страж NT» по умолчанию используются следующие наименования меток конфиденциальности в порядке повышения: несекретно, секретно, совершенно секретно. Чтобы изменить наименования меток (если это не было сделано на этапе установки СЗИ), необходимо, зарегистрировавшись Администратором безопасности, запустить программу настройки СЗИ (**Пуск ⇒ Программы ⇒ Страж NT ⇒ Настройка системы защиты**) и отметить пункт «Изменить наименования меток конфиденциальности информации».

После нажатия кнопки «Далее» будет предложено ввести наименования меток конфиденциальности.

2 Настройка системы защиты в части реализации мандатной модели разграничения доступа заключается в выполнении следующих действий:

– в соответствии с политикой безопасности назначить каждому пользователю уровень допуска при помощи окна «Менеджер пользователей» программы «Управление СЗИ» (это должно быть сделано на этапе создания пользователей до создания их персональных идентификаторов);

– для прикладных программ, предназначенных для обработки защищаемых ресурсов, разрешить режим запуска (см. ниже) и установить значение допуска при помощи окна «Администратор ресурсов» программы «Управление СЗИ» в (рисунок 74);

– в соответствии с политикой безопасности определить защищаемые ресурсы

и присвоить им гриф секретности также при помощи окна «Администратора ресурсов».

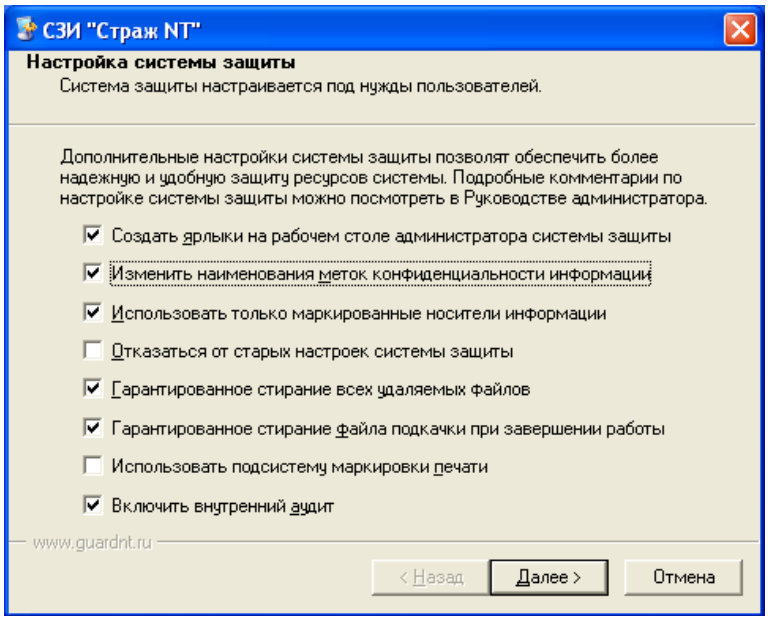

Рисунок 74 - Диалоговое окно «Настройка системы защиты»

З «Администратор ресурсов» открывается из программы «Управление СЗИ» командой меню **Администрирование ⇒ Администратор ресурсов**.

Операции, связанные с изменением прав доступа, могут производиться только в режиме администрирования. Чтобы включить его, необходимо выполнить команду меню **Администрирование ⇒ Режим администрирования**.

Исходно все объекты, участвующие в процессе мандатного управления доступом, имеют метки конфиденциальности «Несекретно». Метки конфиденциальности можно присваивать как отдельным файлам, так и каталогам. Для установки метки конфиденциальности ресурса необходимо в окне «Администратора ресурсов» щелкнуть правой клавишей мыши на файле или каталоге и в раскрывшемся контекстном меню выбрать пункт «Гриф и режим запуска». Будет открыто диалоговое окно, вид которого показан на рисунке 75.

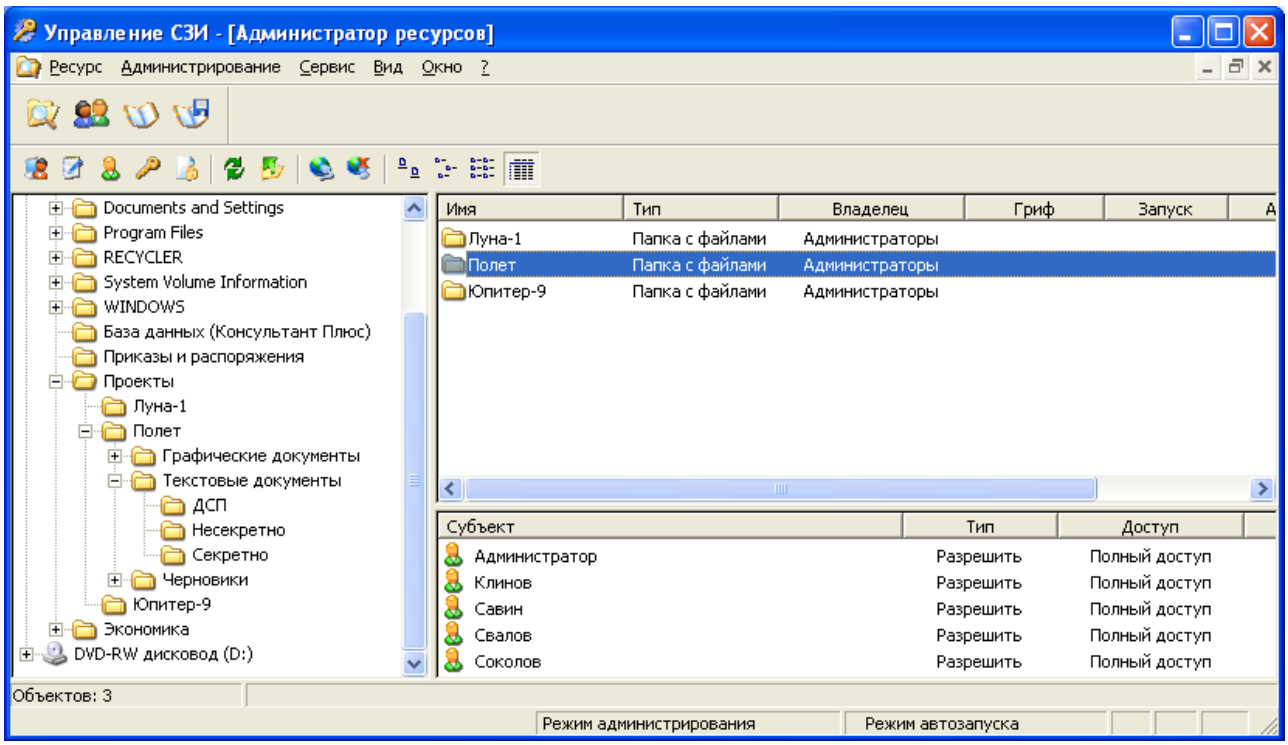

Рисунок 75 Администратор ресурсов

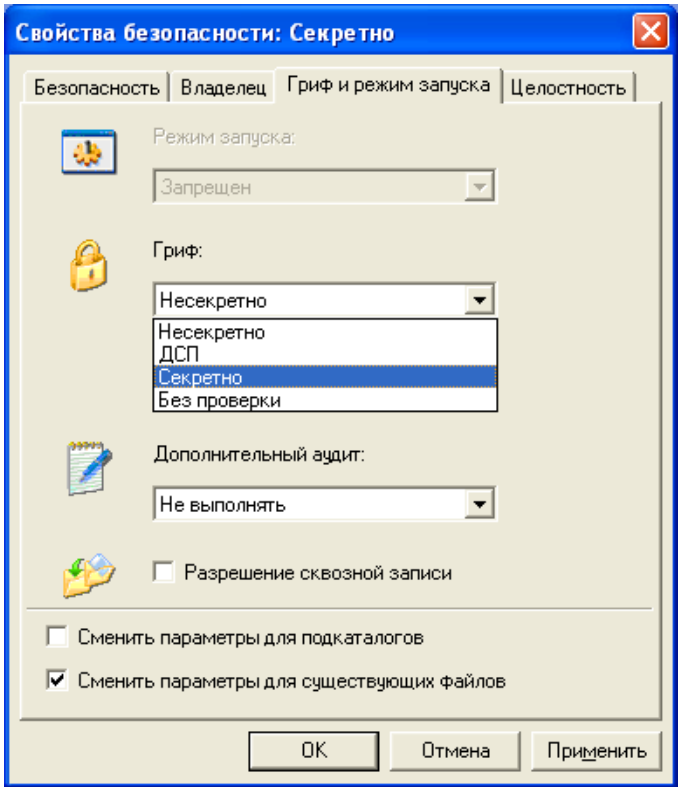

Рисунок 76 - Диалоговое окно «Гриф и режим запуска»

Задача № 3. Реализация дискреционной модели разграничения доступа:

1 Дискреционная модель разграничения доступа реализуется посредством списков доступа, которые представляют собой наборы записей, содержащих код субъекта и маску доступа. Маски доступа определяют права доступа субъекта доступа к защищаемым ресурсам. В целом процедура назначения прав доступа посредством списков доступа в СЗИ «Страж NT» совпадает с соответствующей процедурой, осуществляемой штатными средствами Windows NT для файловой системы NTFS. Устанавливать разрешения на доступ можно только в программе «Управление СЗИ» в окне «Администратора ресурсов».

2 Программа должна быть переведена в режим администрирования (**Администрирование ⇒ Режим администрирования**). Диалоговое окно, в котором производится настройка разрешений, можно открыть, щелкнув правой клавишей мыши на пиктограмме соответствующего ресурса и выбрав пункт «Разрешения и аудит» в контекстном меню. Следует отметить отличия в реализации дискреционного принципа контроля доступа по сравнению с ОС Windows NT. Вопервых, если пользователь не имеет разрешений на чтение ресурса, данный ресурс (кроме устройств и портов) становится для него невидимым. Это справедливо и для администраторов системы защиты. Чтобы администратор увидел такие ресурсы, необходимо запустить «Администратор ресурсов» и включить режим администрирования. Во-вторых, эксклюзивными правами на назначение прав доступа к файлам и каталогам обладает только Администратор безопасности (а не создатель-владелец, как в ОС Windows NT).

3 С помощью «Администратора ресурсов» в режиме администрирования разграничить права доступа пользователей к созданным каталогам. Зарегистрироваться пользователем Ювченко и просмотреть содержимое каталога «С:\Экономика». Убедиться, что каталог «С:\Проекты» для этого пользователя не отображается.

4 Зарегистрироваться пользователем Свалов и просмотреть содержимое каталога «С:\Проекты\Полет\Текстовые документы\Секретно». Убедиться, что

каталог «C:\Экономика» не для него отображается.

5 Создать в каталоге «C:\Приказы и распоряжения» пользователем Клинов короткий текстовый файл «Приказ1.txt» с приказом об увольнении Соколова. Зарегистрироваться Администратором и просмотреть разрешения, которые установлены для вновь созданного файла. Привести эти разрешения в соответствие с разрешениями, установленными для каталога, если они различаются.

6 Убедиться, что Соколов сможет прочитать приказ о своем увольнении, но не сможет изменить его.

Задача № 4. Создание замкнутой программной среды:

1 Замкнутость программной среды в СЗИ «Страж NT» обеспечивается путем установки соответствующих разрешений на запуск для исполняемых файлов (прикладных программ). Существует несколько режимов запуска исполняемых файлов, из которых для рядовых пользователей системы наиболее важными являются:

– запрещен – запуск на выполнение запрещен, кроме администратора системы защиты;

– приложение – запуск исполняемого файла разрешен для всех пользователей системы.

2 Файлы, не имеющие разрешения на запуск, ни при каких условиях не могут быть запущены на выполнение. Разрешение на запуск прикладных программ может производить только Администратор системы защиты. При создании новых исполняемых файлов режим запуска для них устанавливается в значение «запрещен». Файлы, разрешенные на запуск, автоматически становятся доступны только на чтение и выполнение, обеспечивая целостность программной среды.

Кроме того, каждой запущенной программе соответствует текущий допуск, который выбирается пользователем при запуске программы и определяет степень секретности сведений, обрабатывающихся в данный момент. Все документы, сохраняемые программой, имеют гриф, равный текущему уровню допуска в момент сохранения. Увидеть, какой текущий уровень допуска имеет программа, можно в строке заголовка — он отображается в квадратных скобках. Текущий уровень

допуска можно изменить, щелкнув на главном меню программы (пиктограмма в левой части строки заголовка), а затем выбрав пункт «Текущий допуск». В открывшемся диалоговом окне необходимо выбрать требуемый уровень допуска, не превышающий уровень допуска текущего пользователя.

3 Для всех используемых пользователями компьютерной системы программ Администратором должен быть установлен режим запуска «Приложение», а также уровень допуска, соответствующий максимальной степени секретности документов, с которыми разрешено работать данной программе. Это делается в диалоговом окне «Гриф и режим запуска».

Рядовым пользователям запрещен запуск программ, для которых не был установлен соответствующий режим запуска. На пользователей из группы Администраторы данное ограничение не действует, и они вправе запускать любые исполняемые файлы. Изменение файлов, у которых установлен режим запуска «Приложение», запрещено, в том числе Администратору.

Задача № 5. Создание иерархической структуры каталогов:

1 С помощью «Администратора ресурсов» создать иерархическую структуру каталогов, как показано на рисунке 77. Назначить созданным каталогам грифы секретности в соответствии с их названиями.

2 Установить для файла «%SystemRoot%\explorer.exe» режим запуска «Приложение», максимальный уровень допуска и режим запроса текущего уровня допуска «При старте».

3 Установить для файла «%SystemRoot%\system32\notepad.exe» режим запуска «Приложение», максимальный уровень допуска и режим запроса текущего уровня допуска «По умолчанию».

4 Перезагрузить компьютер, зарегистрироваться пользователем Клинов. Далее при загрузке будет выведено диалоговое окно, в котором предлагается выбрать текущий уровень допуска для программы «Проводник». Необходимо выбрать уровень допуска «Секретно». Запустив «Проводник», просмотреть содержимое созданных каталогов.

5 Выйти из системы и зарегистрироваться пользователем Соколов. В

диалоговом окне выбора текущего уровня допуска для программы «Проводник» попытаться выбрать уровень допуска «Секретно».

6 Запустить редактор «Блокнот».

7 Создать короткий текстовый документ «Соколов.txt» и сохранить его в каталоге «C:\Проекты\Полет\Текстовые документы\Несекретно».

8 Зарегистрироваться в системе пользователем Свалов, запустить «Блокнот», установить максимальный текущий допуск («Секретно»), создать короткий текстовый документ «Свалов.txt» и попытаться сохранить его в каталог «C:\Проекты\Полет\Текстовые документы\Несекретно». Получилось ли это? Сохранить документ в каталоге «C:\Проекты\Полет\Текстовые документы\Секретно».

9 Попытаться открыть несекретный документ программой «Блокнот» при установленном уровне допуска «Секретно».

10 Запустить еще один экземпляр редактора «Блокнот» с текущим уровнем допуска «Несекретно», и попытаться скопировать содержимое из секретного документа в несекретный с использованием команд ***Правка ⇒ Копировать*** и ***Правка ⇒ Вставить***.

11 Проверить, может ли пользователь Свалов запустить «Калькулятор» («%SystemRoot%\system32\calc.exe»).

Задача № 6. Контроль целостности.

В СЗИ «Страж NT» реализована возможность контроля со стороны Администратора и ограниченно со стороны пользователей фактов изменения наиболее критичных с точки зрения безопасности файлов (как санкционированного, так и нет), для чего предусмотрена функция контроля целостности файлов.

Включение контроля осуществляется администратором безопасности с использованием «Администратора ресурсов» программы «Управление СЗИ». Программа должна быть переведена в режим администрирования.

Настройка контроля целостности ресурса показана на рисунке 77.

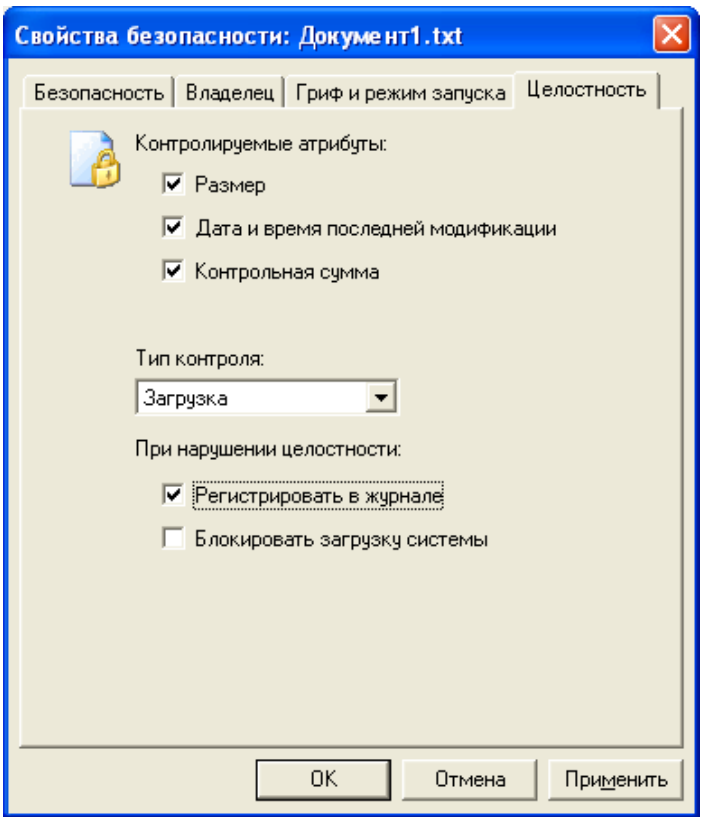

Рисунок 77 - Настройка контроля целостности ресурса

Чтобы вызвать диалоговое окно, в котором производятся настройки контроля целостности файла, нужно выполнить команду меню ***Ресурс ⇒ Целостность*** или воспользоваться контекстным меню.

В качестве контролируемых атрибутов могут выступать: размер, дата и время последней модификации, а также контрольная сумма файла. Проверка контролируемых параметров может производиться в нескольких режимах, который можно установит в раскрывающемся списке «Тип контроля»:

– «Загрузка» — при загрузке операционной системы (только для файлов, находящихся на системном диске);

– «Автомат» — при загрузке операционной системы (для любых файлов);

– «Открытие» — при открытии на чтение файла, целостность которого нарушена, выдается ошибка, и файл не открывается.

В режиме «Загрузка» при обнаружении нарушения целостности можно произвести блокировку дальнейшей загрузки ОС для всех пользователей, исключая

администратора безопасности. Кроме того, в режимах «Загрузка» и «Автомат» есть возможность регистрации факта нарушения целостности файла в «Журнале регистрации событий».

Выполнение работы:

1 Зарегистрироваться в системе пользователем Администратор и настроить контроль целостности всех параметров файла «C:\Проекты\Полет\Текстовые документы\Несекретно\Соколов.txt» в режиме «Автомат» с записью в журнал. Для файла «C:\Проекты\Полет\Текстовые документы\Секретно\Свалов.txt» настроить контроль целостности всех параметров в режиме «Открытие».

2 Выйти из системы и зарегистрироваться пользователем Свалов. Изменить файлы «Соколов.txt» и «Свалов.txt». Перезагрузить компьютер, зарегистрироваться пользователем Клинов.

3 Зарегистрироваться Администратором, открыть «Журнал регистрации событий» в программе «Управление СЗИ» (***Администрирование ⇒ Журнал регистрации событий***) и найти записи журнала, в которых отражено изменение контрольной суммы файла «Соколов.txt».

4 Отключить контроль целостности файлов.

Задача № 7. Регистрация событий.

СЗИ «Страж NT» позволяет использовать стандартные средства регистрации событий, присутствующие в ОС Windows NT. Кроме того, средствами СЗИ дополнительно реализована автоматическая регистрация следующих событий:

– вход в систему (включение компьютера, аутентификация с использованием носителя ключевой информации);

– попытка запуска неразрешенных на выполнение исполняемых файлов;

– факт нарушения целостности ресурса (при условии, что осуществляется контроль целостности этого ресурса).

Окно постановки на учет носителя информации показано на рисунке 78. Журнал регистрации событий показан на рисунке 79.

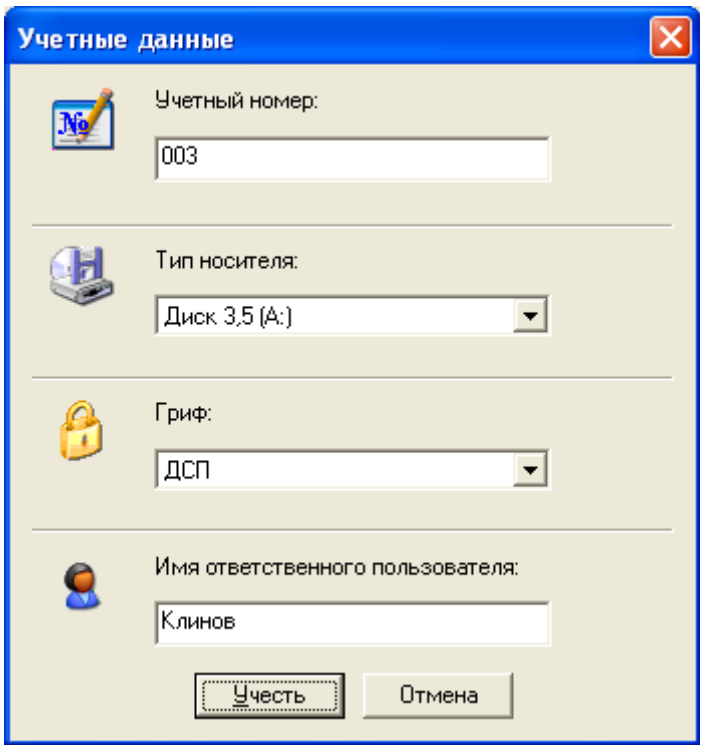

Рисунок 78 - Постановка на учет носителя информации

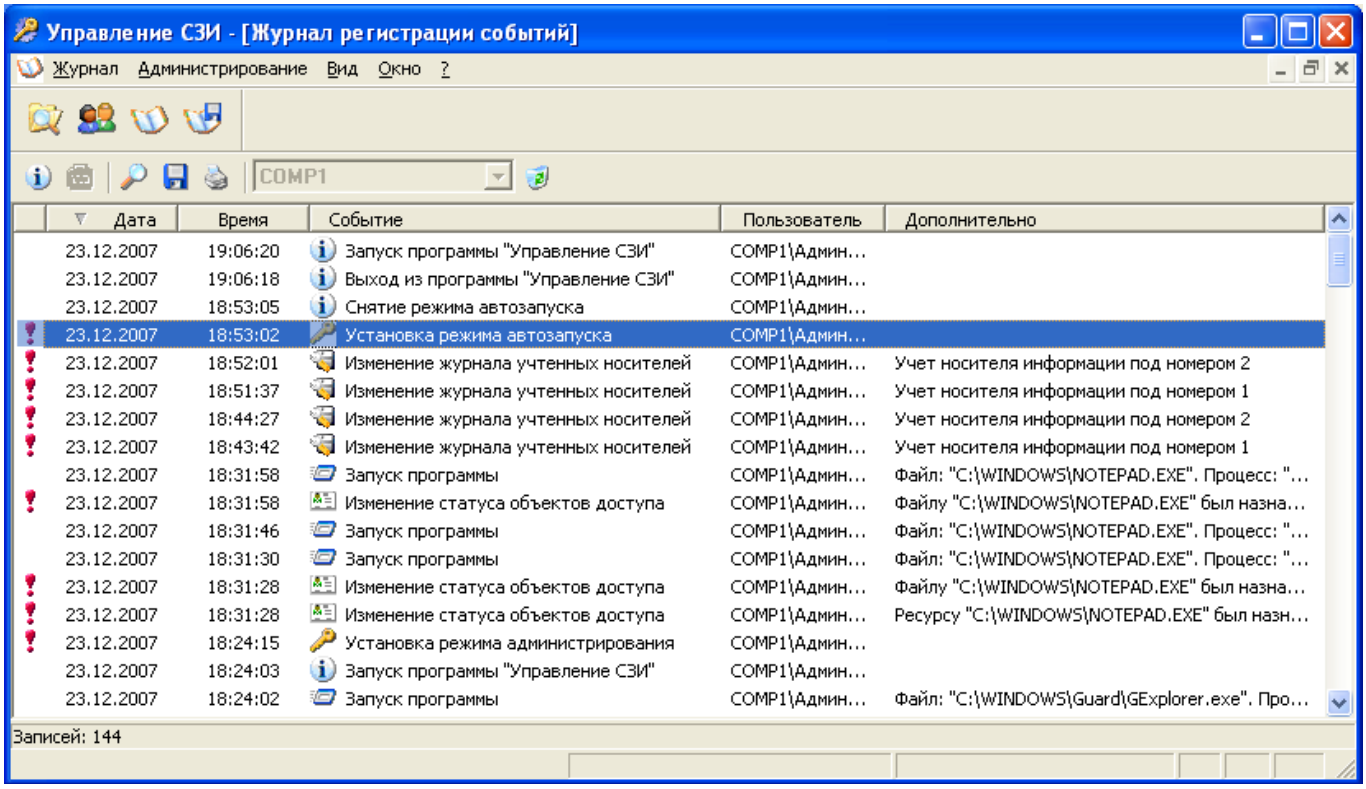

Рисунок 79 - Журнал регистрации событий

Регистрируются также важные с точки зрения безопасности системы действия, выполняемые только пользователем с правами администратора, например такие, как:

– включение режима администрирования;

– изменение грифа ресурсов;

– назначение допуска пользователей;

– изменение паролей пользователей;

– очистка журнала регистрации событий.

Сведения об этих событиях записываются не в системный журнал операционной системы, а в специальный «Журнал регистрации событий» (рисунок 79), который 'E2a открывается командой меню **Администрирование ⇒ Журнал регистрации событий** из программы «Управление СЗИ».

При формировании политик аудита в компьютерной системе кроме событий, фиксируемых СЗИ автоматически, рекомендуется настроить регистрацию следующих категорий событий:

– регистрация пользователей в ОС Windows NT;

– изменения в политике безопасности Windows NT.

Аудит указанных событий, а также событий, связанных с доступом к защищаемым ресурсам (при наличии достаточных для этого оснований), необходимо производить с использованием стандартных средств регистрации Windows NT. Разработчики СЗИ «Страж NT» не рекомендуют регистрировать события, связанные с применениями привилегий пользователей, так как это будет приводить к быстрому переполнению журнала. По умолчанию в ОС Windows NT регистрация всех категорий событий отключена. Чтобы включить ее, необходимо сделать соответствующие изменения в настройках локальной политики безопасности в разделе «Политика аудита» (рисунок 80) (**Панель управления ⇒ Администрирование ⇒ Локальная политика безопасности ⇒ Локальные политики ⇒ Политика аудита**).

Аудит событий доступа к защищаемым ресурсам должен производиться

только при наличии обоснованных подозрений в злоупотреблении полномочиями. Кроме того, в связи с особенностями реализации защитных механизмов в СЗИ «Страж NT», регистрация событий отказа в доступе к ресурсам будет приводить к появлению в журнале большого количества посторонних записей. Поэтому можно рекомендовать устанавливать аудит лишь для событий успешного доступа к ресурсам. Настройка регистрации производится при помощи окна «Администратор ресурсов». Для того чтобы включить регистрацию событий, необходимо щелкнуть правой клавишей мыши на ресурсе (файле, каталоге, диске и т. д.), выбрать пункт контекстного меню «Разрешения и аудит», а затем в открывшемся диалоговом окне нажать кнопку «Дополнительно…». Откроется окно «Параметры управления доступом», вкладка «Аудит» которого отвечает за регистрацию событий, связанных с доступом к выбранному ресурсу, как на рисунке 81.

Выполнение работы:

1 Изменить настройки локальной политики безопасности так, чтобы производилась регистрация следующих категорий событий: вход в систему (успех, отказ), доступ к объектам (успех).

2 С использованием «Администратора ресурсов» в режиме администрирования назначить аудит всех типов событий доступа каталогу «C:\Проекты\Полет\Текстовые документы\Секретно».

3 Перезагрузиться, зарегистрироваться пользователем Свалов и прочитать содержимое указанного выше каталога. После этого выйти из системы и зарегистрироваться пользователем Клинов. Также попытаться прочитать содержимое каталога.

4 Перезагрузиться, зарегистрироваться пользователем Администратор, просмотреть содержимое «Журнала регистрации событий» СЗИ «Страж NT».

5 Открыть «Журнал безопасности» и найти записи, связанные с получением доступа к каталогу «C:\Проекты\Полет\Текстовые документы\Секретно» пользователями Свалов и Клинов.

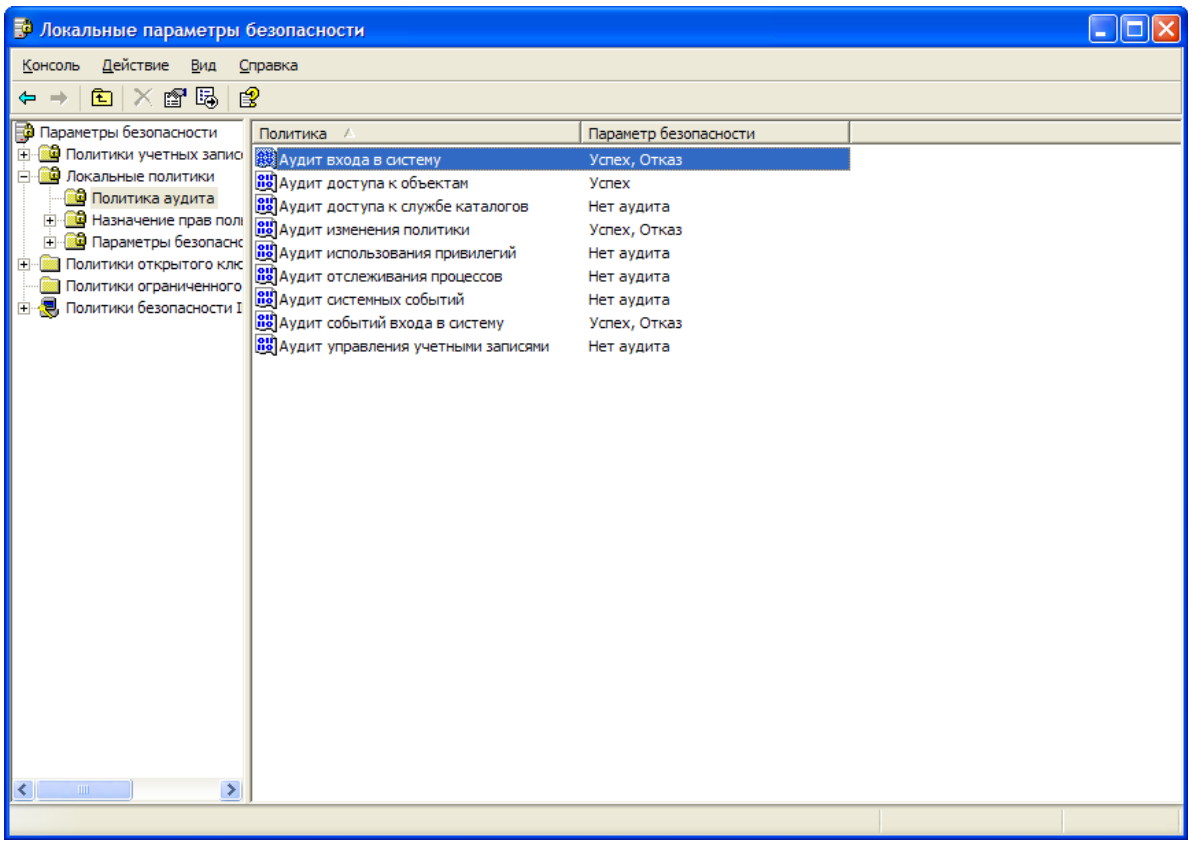

Рисунок 80 - Настройка политики аудита

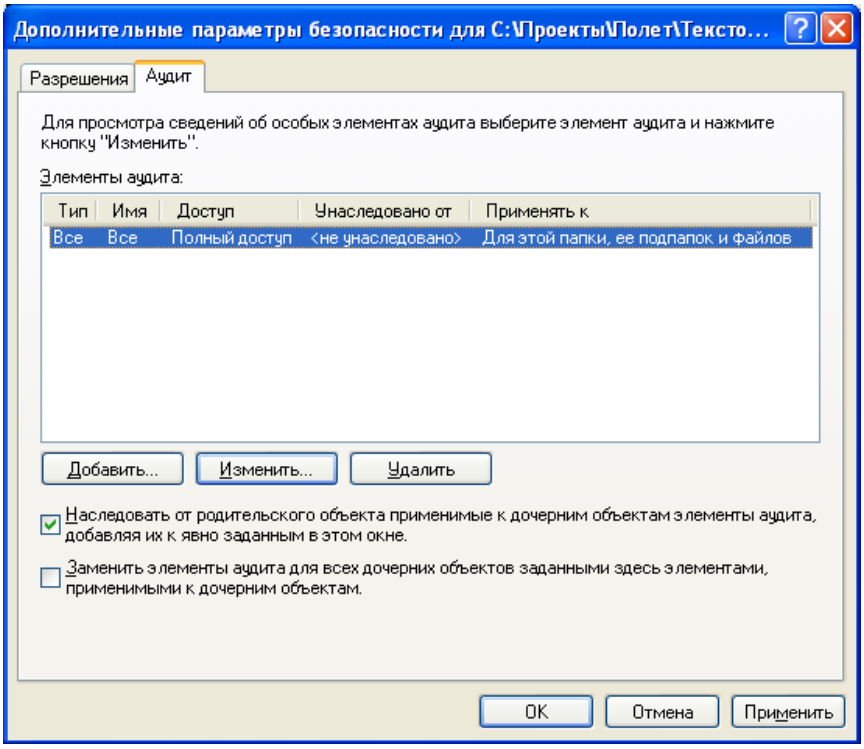

Рисунок 81 - Настройка регистрации событий доступа к ресурсу

Журнал безопасности показан на рисунке 82.

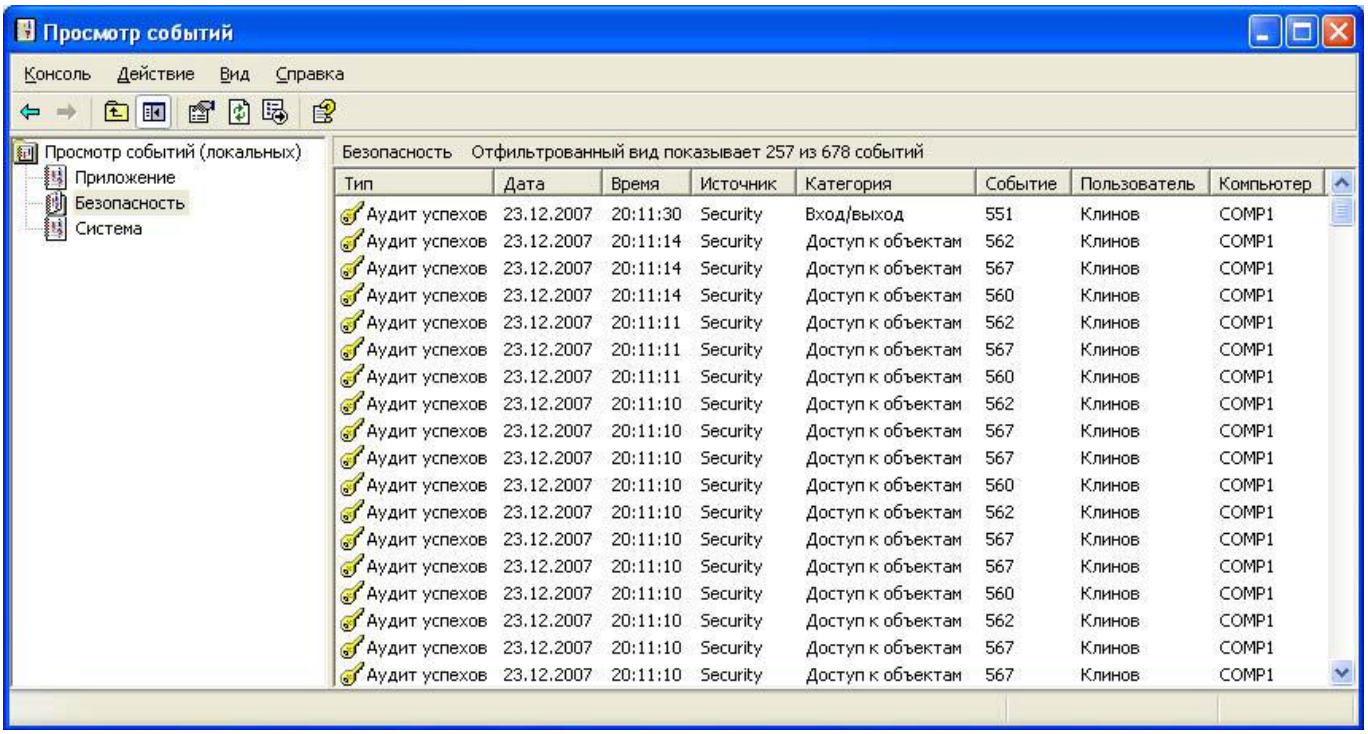

Рисунок 82 - Журнал безопасности

Задача № 8. Гарантированное удаление данных.

СЗИ «Страж NT» соответствует требованиям класса защищенности 3 «РД Гостехкомиссии России. СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации» и кроме всего прочего включает в себя механизм гарантированного стирания всех удаляемых файлов, файла подкачки и критичных областей оперативной памяти. При удалении «грифованных» файлов механизм их гарантированного стирания в СЗИ действует по умолчанию.

Выполнение работы:

1 Работая с пользователем Соколов, создать в каталоге «C:\Проекты\Полет\Текстовые документы\Несекретно» короткий текстовый файл «Соколов2.txt», содержащий произвольную строку символов (запомнить или переписать строку).

2 Зарегистрироваться пользователем Свалов. Создать в каталоге «C:\Проекты\Полет\Текстовые документы\Секретно» текстовый файл «Свалов2.txt», содержащий

произвольную строку символов (запомнить или переписать строку).

3 С использованием редактора WinHEX (или любого другого двоичного редактора), запущенного из основной операционной системы, открыть файл образа диска с установленной СЗИ «Страж NT». Найти и записать смещение, по которому расположены два созданных файла (поиск файловых записей можно вести как по имени файла, так и по содержимому).

4 Удалить файлы «Соколов2.txt» и «Свалов2.txt», воспользовавшись комбинацией <Shift+Delete> в «Страж NT» (пользователем Свалов или Администратор). Попытаться найти содержимое удаленных файлов с использованием редактора WinHEX.

Содержание отчета:

1 Название и цель работы.

2 Краткая теоретическая справка.

3 Результаты проделанной работы (этапы, экранные формы, расчеты и т.д.).

4 Выводы по выполненной работе.

5 Список использованных источников.

Список использованных источников

1 Вайнштейн, Ю. В. Основы информационной безопасности: учебн. пособие/ Ю. В. Вайнштейн - Красноярск: Сибирский федеральный университет, 2007. – 79 с.

2 Каторин, Ю. Ф. Техническая защита информации: лабораторный практикум /под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2013. – 112 с.

3 Колегов, Д. Н. Лабораторный практикум по основам построения защищенных компьютерных сетей/ Д. Н. Колегов. – Томск: Томский государственный университет, 2013. – 140 с.