Департамент образования Вологодской области
бюджетное профессиональное образовательное учреждение
Вологодской области
«ВОЛОГОДСКИЙ СТРОИТЕЛЬНЫЙ КОЛЛЕДЖ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к практическим работам

ПО ДИСЦИПЛИНЕ ОП.15. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специальность 09.02.04 Информационные системы (по отраслям)

2017г.

Рассмотрено на заседании предметной цикловой комиссии общепрофессиональных, специальных дисциплин и дипломного проектирования по специальностям 08.02.01 Строительство и эксплуатация зданий и сооружений, 08.02.07 Монтаж и эксплуатация внутренних сантехнических устройств, кондиционирования воздуха и вентиляции, 43.02.08 Сервис домашнего и коммунального хозяйства.

Данные методические указания предназначены для студентов специальности 09.02.04 Информационные системы (по отраслям) БПОУ ВО «Вологодский строительный колледж» при выполнении практических работ по дисциплине ОП.15. Основы информационной безопасности.

Настоящие методические указания включают в себя краткий теоретический материал, практические задачи, указания к их выполнению.

Автор:

Н.Л.Ингеройнен - преподаватель

СОДЕРЖАНИЕ

Введение

Методические указания разработаны с учётом обязательного минимума содержания образования по дисциплине. В методических указаниях представлены практические задания для выполнения их в тетради или на компьютере по всем разделам рабочей программы и календарно-тематического плана по дисциплине ОП.15. Основы информационной безопасности.

Задания разделены по разделам курса информатики: «Сущность и понятие защиты информации», «Основы защиты информации», «Правовое обеспечение информационной безопасности», «Организационные основы защиты информации»» Обеспечение безопасности автоматизированных систем».

Раздел 2. Сущность и понятие защиты информации

Практическая работа 1. Анализ источников, каналов распространения и каналов утечки информации

Цель работы: формирование навыка работы с нормативными документами по исследуемому вопросу; анализ угроз информационной безопасности
Время выполнения: 2 часа
Оборудование: учебный персональный компьютер.

Теоретические основы

Понятие «информационная безопасность» (ИБ) рассматривается как состояние защищенности потребностей личности, общества и государства в информации, при котором обеспечиваются их существование и прогрессивное развитие независимо от наличия внутренних и внешних информационных угроз. Тогда с позиции обеспечения ИБ можно определить, что под информационной угрозой понимается воздействие дестабилизирующих факторов на состояние информированности, подвергающее опасности жизненно важные интересы личности, общества и государства.

В законе РФ «О безопасности» дано определение угрозы безопасности как совокупности условий, факторов, создающих опасность жизненно важным интересам личности, общества и государства. Под угрозой информации в системах ее обработки понимается возможность возникновения на каком -либо этапе жизнедеятельности системы такого явления или события, следствием которого могут быть нежелательные воздействия на информацию. К настоящему времени известно большое количество разноплановых угроз различного происхождения, таящих в себе различную опасность для информации. Для системного представления их удобно классифицировать по виду, возможным источникам, предпосылкам появления и характеру проявления.

Виды угроз Определив понятие «угроза государству, обществу и личности» в широком смысле, рассмотрим его относительно не посредственного воздействия на конфиденциальную информацию, обрабатываемую на каком-либо объекте (кабине те, предприятии, фирме). Анализируя возможные пути воздействия на информацию, представляемую как совокупность информационных элементов, связанных между собой логическими связями (рис. 1), можно выделить основные нарушения:

— физической целостности (уничтожение, разрушение элементов);

— логической целостности (разрушение логических связей);

— содержания (изменение блоков информации, внешнее навязывание ложной информации);

— конфиденциальности (разрушение защиты, уменьшение степени защищенности информации),

— прав собственности на информацию (несанкционированное копирование, использование).

С учетом этого для таких объектов систем угроза информационной безопасности представляет реальные или потенциально возможные действия или условия, приводящие к овладению конфиденциальной информацией, хищению, искажению, изменению, уничтожению ее и сведений о самой системе, а также к прямым материальным убыткам.

Обобщая рассмотренные угрозы, можно выделить три наиболее выраженные для систем обработки информации:

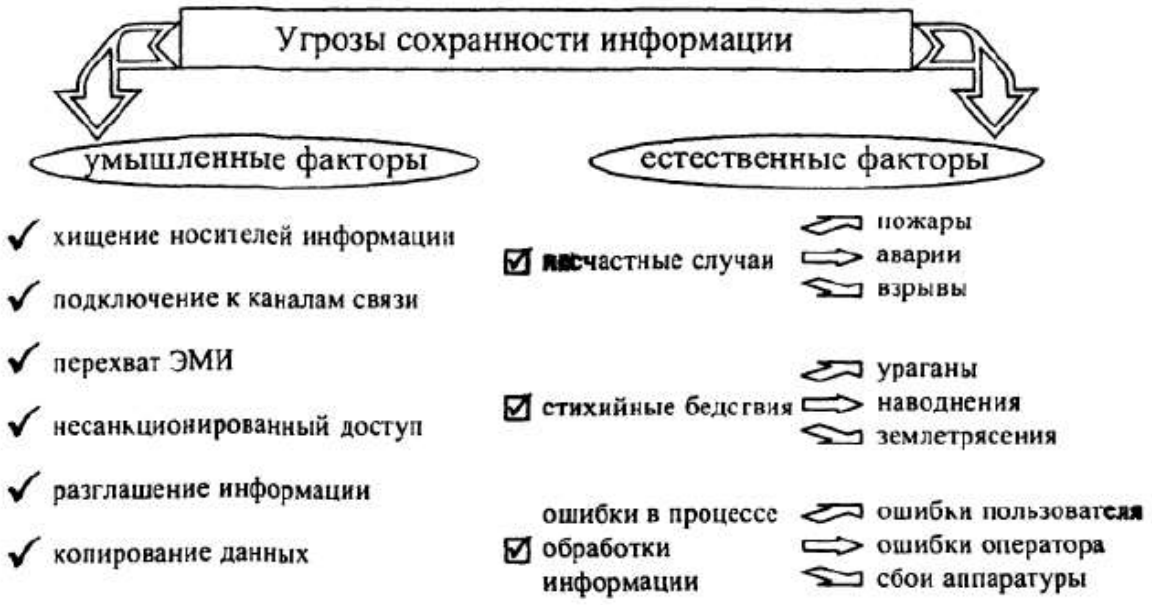
1) подверженность физическому искажению или уничтожению;

2) возможность несанкционированной (случайной или злоумышленной) модификации;

3) опасность несанкционированного (случайного или преднамеренного) получения информации лицами, для которых она не предназначалась.

Кроме того, с точки зрения анализа процесса обработки информации выделяют такую угрозу, как блокирование доступа к обрабатываемой информации.

Угрозы безопасности информации в современных системах ее обработки определяются умышленными (преднамеренные угрозы) и естественными (непреднамеренные угрозы) разрушающими и искажающими воздействиями внешней среды, надежностью функционирования средств обработки информации, а также преднамеренным корыстным воздействием несанкционированных пользователей, целями которых являются хищение, уничтожение, разрушение, несанкционированная модификация и использование обрабатываемой информации. При этом под умышленными, или преднамеренными, понимаются такие угрозы, которые обусловливаются злоумышленными действиями людей. Случайными, или естественными, являются угрозы, не зависящие от воли людей. В настоящее время принята следующая классификация угроз сохранности (целостности)



Под источником угроз понимается непосредственный исполнитель угрозы с точки зрения ее негативного воздействия на информацию. Источники можно разделить на следующие группы:

— люди;

— технические устройства;

— модели, алгоритмы, программы;

— технологические схемы обработки;

— внешняя среда

Предпосылки появления угроз Существуют следующие предпосылки, или причины, появления угроз:

— объективные (количественная или качественная недостаточность элементов системы) — не связанные непосредственно с деятельностью людей и вызывающие случайные по характеру происхождения угрозы;

— субъективные — непосредственно связанные с деятельностью человека и вызывающие как преднамеренные (деятельность разведок иностранных государств, промышленный шпионаж, деятельность уголовных элементов и недобросовестных сотрудников), так и непреднамеренные (плохое психофизиологическое состояние, недостаточная подготовка, низкий уровень знаний) угрозы информации.

Перечисленные разновидности предпосылок интерпретируются следующим образом:

— количественная недостаточность — физическая не хватка одного или нескольких элементов системы обработки, вызывающая нарушения технологического процесса обработки или перегрузку имеющихся элементов;

— качественная недостаточность — несовершенство конструкции (организации) элементов системы, в силу чего может появляться возможность случайного или преднамеренного негативного воздействия на обрабатываемую или хранимую ин формацию;

— деятельность разведорганов иностранных государств — специально организуемая деятельность государственных органов разведки , профессионально ориентированных на добывание необходимой информации всеми доступными способами и средствами;

— промышленный шпионаж: — негласная деятельность отечественны х и зарубежных промышленных организаций (фирм), направленная на по лучение незаконным путем конфиденциальной информации, используемой для достижения промышленных, коммерческих, политических или подрывных целей;

— злоумышленные действия уголовных элементов — хищение информации, средств ее обработки или компьютерных программ в целях наживы или их разрушение в интересах конкурентов;

— плохое психофизиологическое состояние — постоянное или временное психофизиологическое состояние сотрудников, приводящее при определенных нестандартных внешних воздействиях к увеличению ошибок и сбоев в обслуживании систем обработки информации или непосредственно к разглашению конфиденциальной информации;

— недостаточная качественная подготовка сотрудников — уровень теоретической и практической подготовки персонала к выполнению задач по защите информации, недостаточная степень которого может привести к нарушению процесса функционирования системы защиты информации.

В современной литературе и нормативно-правовых актах в области информационной безопасности можно встретить такую классификацию угроз информации, которая делит их на внутренние и внешние. Одной из наиболее принципиальных особенностей проблемы защиты информации является формирование полного множества угроз информации, потенциально возможных на объекте ее обработки. В самом деле, даже одна неучтенная угроза может в значительной мере снизить эффективность защиты.

Возможные пути получения конфиденциальной информации

Анализ рассмотренных видов угроз позволяет сгруппировать их по двум основным областям:

1) угрозы нарушения физической и логической целостности, а также содержания информации (несанкционированная модификация). Их можно объединить в причины нарушения целостности информации (ПНЦИ);

2) угрозы, следствием которых может быть получение защищаемой информации (хищение или копирование) лицами, не имеющими на это полномочий, — в каналы несанкционированного получения информации (КНПИ).

Под действием рассмотренных выше угроз может произойти утечка защищаемой информации, то есть несанкционированное, неправомерное завладение соперником данной информацией и возможность использования ее в своих, в ущерб интересам собственника (владельца) информации, целях. При этом образуется канал утечки информации, под которым понимается физический путь от источника конфиденциальной информации к злоумышленнику. Для его возникновения необходимы определенные пространственные, энергетические и временные условия, а также соответствующие средства восприятия и фиксации информации на стороне злоумышленника .

. В зависимости от используемых соперником сил и средств для получения несанкционированного доступа к носителям защищаемой информации различают каналы агентурные, технические, легальные.

Агентурные каналы утечки информации — это использование противником тайных агентов для получения несанкционированного доступа к носителям защищаемой информации. В случае использования агентами технических средств разведки (направленны х микрофонов, закладных устройств, миниатюрных видеокамер и др.) говорят о ведении агентурно-технической разведки.

Технические каналы утечки информации — совокупность технических средств разведки, демаскирующих признаков объекта защиты и сигналов, несущих информацию об этих признаках. Эти каналы образуются без участи я человека в процессе обработки информации техническими средствами, а поэтому являются одними из наиболее опасны х и требуют отдельного рассмотрения.

Легальные каналы утечки информации — это использование соперником открытых источников информации (литературы, периодических изданий и т. п), обратный инжиниринг, выведывание под благовидным предлогом информации у лиц, располагающих интересующей соперника информацией, и других возможностей. В основу классификации ПНЦИ положен показатель, характеризующий степень участия в этом процессе человека. В соответствии с таким подходом ПНЦИ делятся на два вида (объективные и субъективные) и на следующие классы (рис. 6).

Для предотвращения возможной утечки конфиденциальной информации и нарушения ее целостности на объектах ее обработки разрабатывается и внедряется система защиты информации. Система защиты информации — совокупность взаимосвязанных средств, методов и мероприятий, направленных на предотвращение уничтожения, искажения, несанкционированного получения конфиденциальных сведений, отображенных физическими полями, электромагнитными, световыми и звуковыми волнами или вещественно-материальными носителями в виде сигналов, образов, символов, технических решений и процессов.

Задание

Необходимо провести анализ защищенности объекта защиты информации по следующим разделам:

1. Виды возможных угроз
2. Характер происхождения угроз
3. Классы каналов несанкционированного получения информации
4. Источники появления угроз
5. Причины нарушения целостности информации
6. Потенциально возможные злоумышленные действия
7. Определить класс защищенности автоматизированной системы

Отчет

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

Контрольные вопросы

1. Что такое информационный риск?
2. В чем заключается задача управления информационными рисками?
3. Какие существуют методики оценки рисков и управления ими?
4. Какие формулы используются при количественной оценке информационных рисков?

Практическая работа 2. Проведение анализа информации на предмет целостности

Цель работы изучить понятие целостности информации, проанализировать риски информационной безопасности.

Оборудование: учебный персональный компьютер.

Теоретические основы

Целостность информации условно подразделяется на статическую и динамическую.

Статическая целостность информации предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации.

Динамическая целостность информации включает вопросы корректного выполнения сложных действий с информационными потоками, например, анализ потока сообщений для выявления некорректных, контроль правильности передачи сообщений, подтверждение отдельных сообщений и др.

Целостность является важнейшим аспектом информационной безопасности в тех случаях, когда информация используется для управления различными процессами, например техническими, социальными и т. д.

Так, ошибка в управляющей программе приведет к остановке управляемой системы, неправильная трактовка закона может привести к его нарушениям, точно также неточный перевод инструкции по применению лекарственного препарата может нанести вред здоровью. Все эти примеры иллюстрируют нарушение целостности информации, что может привести к катастрофическим последствиям. Именно поэтому целостность информации выделяется в качестве одной из базовых составляющих информационной безопасности.

Целостность– гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений.

Действия, направленные на нарушение целостности информации, подразделяются на субъективные преднамеренные и объективные преднамеренные.

Субъективные преднамеренные:

- диверсия (организация пожаров, взрывов, повреждений электропитания и др.);
- непосредственные действия над носителем (хищение, подмена носителей, уничтожение информации);
- информационное воздействие (электромагнитное облучение, ввод в компьютерные системы разрушающих программных средств, воздействие на психику личности психотропным оружием).

Объективные непреднамеренные:

- отказы (полный выход из строя) аппаратуры, программ, систем питания и жизнеобеспечения;
- сбои (кратковременный выход из строя) аппаратуры, программ, систем питания и жизнеобеспечения;

- стихийные бедствия (наводнения, землетрясения, ураганы);
- несчастные случаи (пожары, взрывы, аварии);
- электромагнитная несовместимость.

Практическое задание

Составьте таблицу, содержащую причины нарушения целостности информации и мер предосторожности, применяемых для защиты информации от потери целостности.

Отчет

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

Контрольные вопросы

1. Что такое целостность информации?
2. Какие меры можно предпринять для защиты информации?

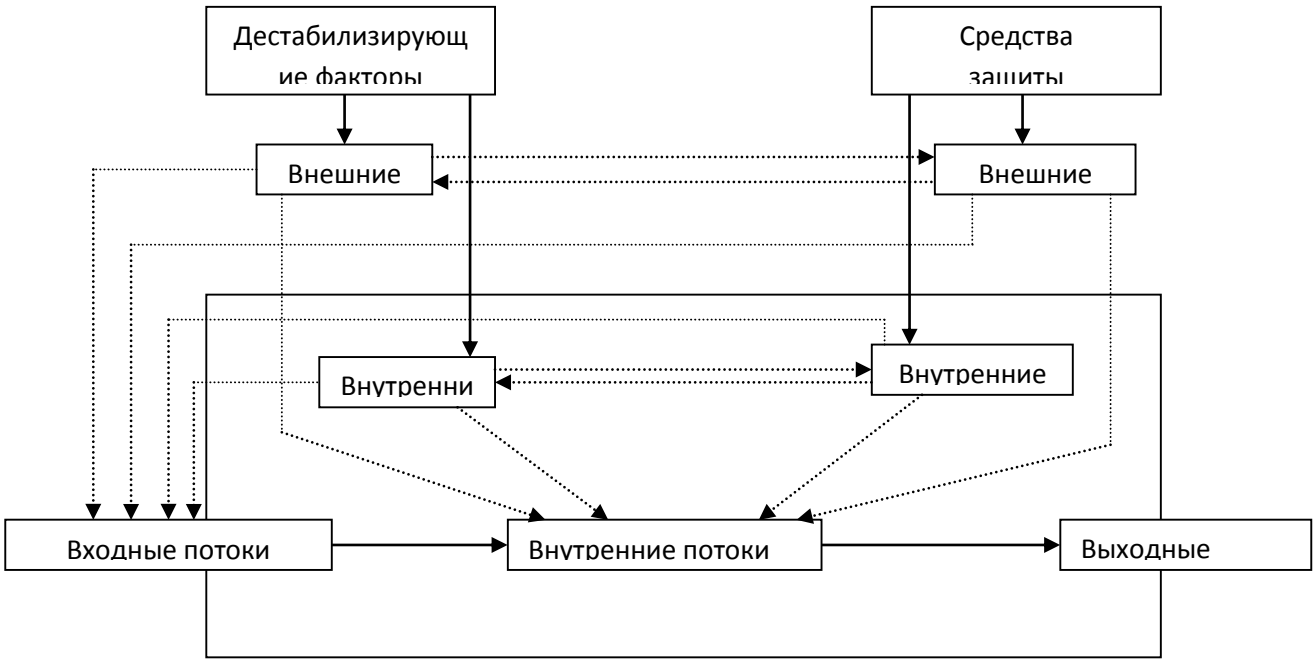
Практическая работа 3. Оценка уязвимости информации

Цель работы: Ознакомиться с алгоритмами оценки уязвимости информационной безопасности.

Оборудование: учебный персональный компьютер.

Теоретические основы

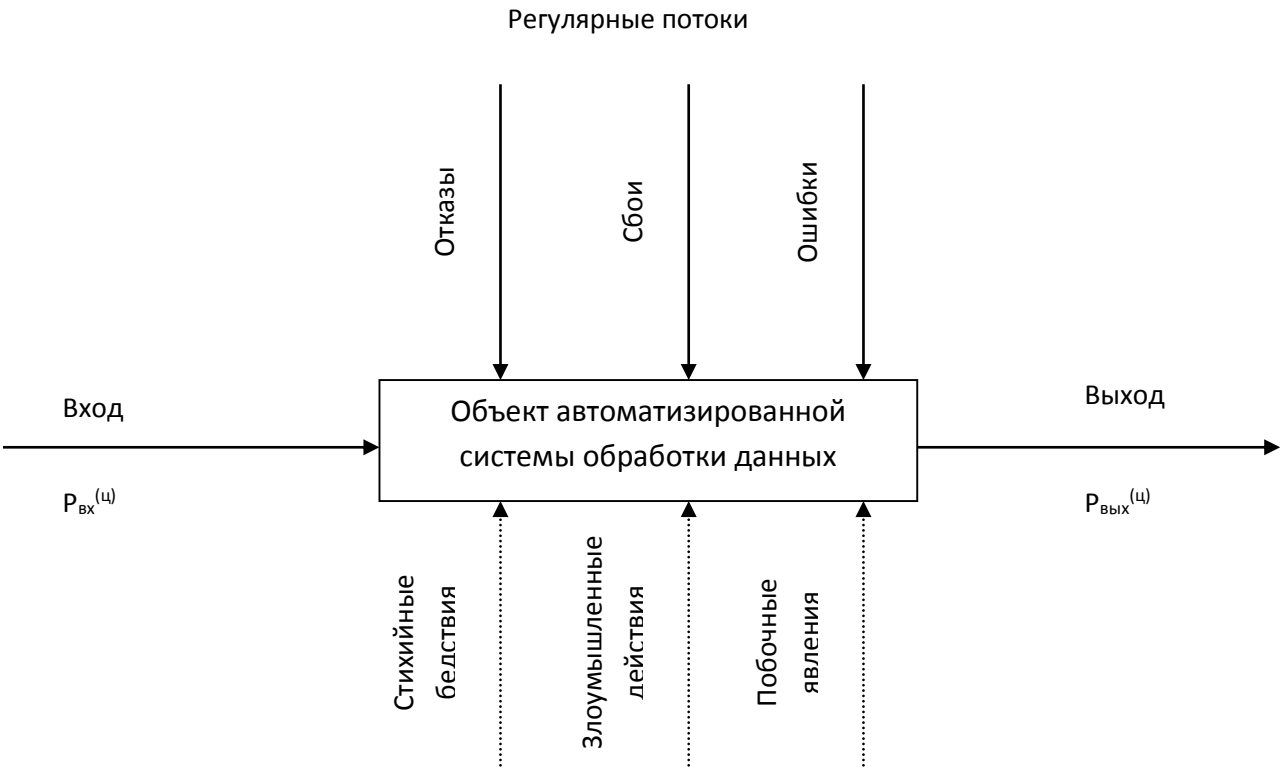
Уязвимость информации есть событие, возникающее как результат такого стечения обстоятельств, когда в силу каких-то причин используемые в автоматизированных системах обработки данных средства защиты не в состоянии оказать достаточного противодействия проявлению дестабилизирующих факторам и нежелательного их воздействия на защищаемую информацию. Модель уязвимости информации в автоматизированных системах обработки данных в общем виде показано.



Данная детализируется при изучении конкретных видов уязвимости информации: нарушения физической или логической целостности, несанкционированной модификации, несанкционированного получения, несанкционированного размножения.

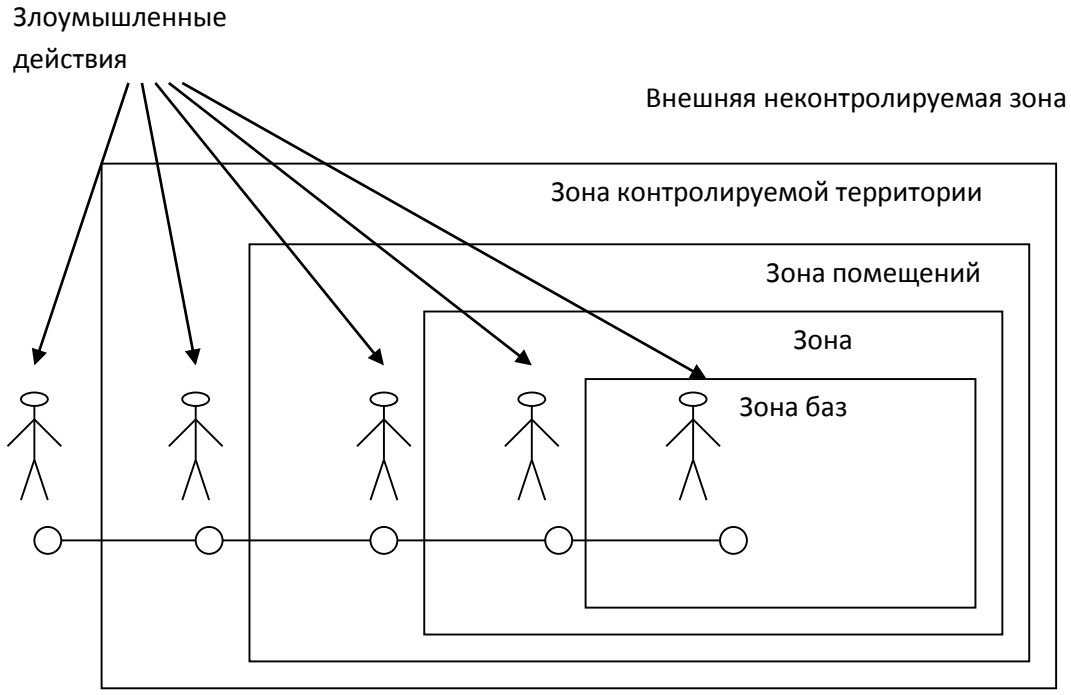
При детализации общей модели основное внимание акцентируется на том, что подавляющее большинство нарушений физической целостности информации имеет место в процессе ее обработки на различных участках технологических маршрутов. При этом целостность информации зависит не только от процессов, происходящих на объекте, но и от целостности информации, поступающей на его вход. Основную опасность представляют случайные дестабилизирующие факторы (отказы, сбои и ошибки компонентов автоматизированных систем обработки данных), которые потенциально могут проявиться в любое время, и в этом отношении можно говорить о регулярном потоке этих факторов. Из стихийных бедствий наибольшую опасность представляют пожары, опасность которых в большей или меньшей степени также является постоянной. Опасность побочных явлений практически может быть сведена к нулю путем надлежащего выбора места для помещений автоматизированной системы обработки данных и их оборудования. Что касается злоумышленных действий, то они связаны, главным образом, с несанкционированным доступом к ресурсам автоматизированной системы обработки данных. При этом наибольшую опасность представляет занесение вирусов.

В соответствии с изложенным общая модель процесса нарушения физической целостности информации на объекте автоматизированной системы обработки данных может быть



представлена схематично.

С точки зрения несанкционированного получения информации принципиально важным является то обстоятельство, что в современных автоматизированных системах обработки данных оно возможно не только путем непосредственного доступа к базам данных, но и многими путями, не требующими такого доступа. При этом основную опасность представляют злоумышленные действия людей. Воздействие случайных факторов непосредственно не ведет к несанкционированному получению информации, оно лишь способствует появлению каналов несанкционированного получения информации, которыми может воспользоваться злоумышленник. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных для самого общего случаю представлена:



Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных

Выделенные зоны определяются следующим образом:

1) внешняя неконтролируемая зона — территория вокруг автоматизированной системы обработки данных, на которой персоналом и средствами автоматизированной системой обработки данных не применяются никакие средства и не осуществляется никакие мероприятия для защиты информации;
2) зона контролируемой территории — территория вокруг помещений автоматизированной системы обработки данных, которая непрерывно контролируется персоналом или средствами автоматизированной системы обработки данных;
3) зона помещений автоматизированной системы обработки данных — внутренне пространство тех помещений, в которых расположена система;
4) зона ресурсов автоматизированной системы обработки данных — та часть помещений, откуда возможен непосредственный доступ к ресурсам системы;
5) зона баз данных — та часть ресурсов системы, с которых возможен непосредственный доступ к защищаемым данным.

Злоумышленные действия с целью несанкционированного получения информации в общем случае возможны в каждой из перечисленных зон. При этом для несанкционированного получения информации необходимо одновременное наступление следующих событий: нарушитель должен получить доступ в соответствующую зону; во время нахождения нарушителя в зоне в ней должен проявиться (иметь место) соответствующий канал несанкционированного получения информации; соответствующий канал несанкционированного получения информации должен быть доступен нарушителю соответствующей категории; в канале несанкционированного получения информации в момент доступа к нему нарушителя должна находиться защищаемая информации.

Рассмотрим далее трансформацию общей модели уязвимости с точки зрения несанкционированного размножения информации. Принципиальными особенностями этого процесса являются:

1) любое несанкционированное размножение есть злоумышленное действие;
2) несанкционированное размножение может осуществляться в организациях-разработчиках компонентов автоматизированной системы обработки данных, непосредственно в автоматизированной системе обработки данных и сторонних организациях, причем последние

могут получать носитель, с которого делается попытка снять копию как законным, так и незаконным путем.

Попытки несанкционированного размножения информации у разработчика и в автоматизированной системе обработки данных есть один из видов злоумышленных действий с целью несанкционированного ее получения и поэтому имитируются приведенной моделью. Если же носитель с защищаемой информацией каким-либо путем (законным или незаконным) попал в стороннюю организацию, то для его несанкционированного копирования могут использоваться любые средства и методы, включая и такие, которые носят характер научных исследований и опытно-конструкторских разработок.

В процессе развития теории и практики защиты информации сформировалось три методологических подхода к оценке уязвимости информации: эмпирический, теоретический и теоретико-эмпирический.

Эмпирический подход к оценке уязвимости информации.

Сущность эмпирического подхода заключается в том, что на основе длительного сбора и обработки данных о реальных проявлениях угроз информации и о размерах того ущерба, который при этом имел место, чисто эмпирическим путем устанавливаются зависимости между потенциально возможным ущербом и коэффициентами, характеризующими частоту проявления соответствующей угрозы и значения имевшего при ее проявлении размера ущерба. Наиболее характерным примером моделей рассматриваемой разновидности являются модели, разработанные специалистами американской фирмы IBM. Рассмотрим развиваемые этих моделях подходы.

Исходной посылкой при разработке моделей является почти очевидное предположение: с одной стороны, при нарушении защищенности информации наносит некоторый ущерб, с другой, обеспечение защиты информации сопряжено с расходованием средств. Полная ожидаемая стоимость защиты может быть выражена суммой расходов на защиту и на потерь от ее нарушения. Совершенно очевидно, что оптимальным решением было бы выделение на защиту информации средств в размере $C_{опт}$, поскольку при этом обеспечивается минимизация общей стоимости защиты информации.

Для того, чтобы воспользоваться данным подходом к решению проблемы, необходимо, во-первых, знать (или уметь определять) ожидаемые потери при нарушении защищенности информации, а во-вторых, в зависимость между уровнем защищенности и средствами, затрачиваемыми на защиту информации.

Решение первого вопроса, т.е. оценки ожидаемых потерь при нарушении защищенности информации, принципиально может быть получено лишь тогда, когда речь идет о защите промышленной, коммерческой и им подобной тайны, хотя и здесь встречаются весьма серьезные трудности. Что касается оценки уровня потерь при нарушении статуса защищенности информации, содержащей государственную, военную и им подобную тайну, то здесь до настоящего времени строгие подходы к их получению не найдены. Данное обстоятельство существенно сужает возможную область использования моделей, основанных на рассматриваемых подходах.

Для определения уровня затрат, обеспечивающих требуемый уровень защищенности информации, необходимо по крайней мере знать, во-первых, полный перечень угроз информации, во-вторых, потенциальную опасность для информации для каждой из угроз и, в третьих, размеры затрат, необходимых для нейтрализации каждой из угроз.

$$R_i = 10^{(S_i + V_i - 4)}$$

Поскольку оптимальное решение вопроса о целесообразном уровне затрат на защиту состоит в том, что этот уровень должен быть равен уровню ожидаемых потерь при нарушении защищенности, достаточно определить только уровень потерь. Специалистами фирмы IBM предложена следующая эмпирическая зависимость ожидаемых потерь от i-й угрозы информации:

Где Si — коэффициент, характеризующий возможную частоту возникновения соответствующей угрозы; Vi — коэффициент, характеризующий значение возможного ущерба при ее возникновении. Предложенные специалистами значения коэффициентов:

Значения коэффициента Si

Ожидаемая (возможная) частота появления угрозы	Предполагаемое значение Si
Почти никогда	0
1 раз в 1000 лет	1
1 раз в 100 лет	2
1 раз в 10 лет	3
1 раз в год	4
1 раз в месяц (примерно, 10 раз в год)	5
12 раза в неделю (примерно 100 раз в год)	6
3 раза в день (1000 раз в год)	7

Возможные значения коэффициента Vi

Значение возможного ущерба при проявлении угрозы (доллары США)	Предполагаемое значение Vi
1	0
10	1
100	2
1 000	3
10 000	4
100 000	5
1 000 000	6
10 000 000	7

Суммарная стоимость потерь определяется формулой

$$R = \sum_{\forall i} R_i$$

Таким образом, если бы удалось собрать достаточное количество фактических данных о проявлениях угроз и их последствиях, то рассмотренную модель можно было бы использовать для решения достаточно широкого круга задач защиты информации, причем, нетрудно видеть, что модель позволяет не только находить нужные решения, но и оценивать их точность. По России такая статистика в настоящее время практически отсутствует. В США же, например, сбору и обработке указанных данных большое внимание уделяет целый ряд учреждений (Стенфордский исследовательский институт и др.). В результате уже получены достаточно представительные данные по целому ряду угроз, которые могут быть положены в основу ориентировочных расчетов и для других стран.

Практическое задание

1. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ.»

2. Ознакомьтесь с **Приложениями C, D** и **E** ГОСТа.

3. Выберите три различных информационных актива организации (см. вариант).

4. Из **Приложения D** ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.

5. Пользуясь **Приложением C** ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

6. Пользуясь одним из методов предложенных в **Приложении E** ГОСТа произведите оценку рисков информационной безопасности.

7. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

Отчет

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

Контрольные вопросы

Дайте определение понятиям:

1. Уязвимости системы защиты информации
2. Угрозы ИБ
3. Оценка рисков

Раздел 3. Основы защиты информации

Практическая работа 4. Требования к безопасности информационных систем.

Цель работы: закрепление теоретических знаний по вопросам сертификации средств защиты информации по требованиям безопасности информации.

Оборудование: учебный персональный компьютер.

Теоретические основы

Минимальные (базовые) требования безопасности формулируются в общем виде, без учета категории, присвоенной ИС. Они задают базовый уровень информационной безопасности, им должны удовлетворять все информационные системы. Результаты категорирования важны при выборе регуляторов безопасности, обеспечивающих выполнение требований, сформулированных на основе анализа рисков.

Организация должна разработать, документировать и обнародовать официальную политику безопасности и формальные процедуры, направленные на выполнение приведенных ниже требований, и обеспечить эффективную реализацию политики и процедур.

В компании необходимо периодически производить оценку рисков, включая оценку угроз миссии, функционированию, имиджу и репутации организации, ее активам и персоналу. Эти угрозы являются следствием эксплуатации ИС и осуществляемых при этом обработки, хранения и передачи данных.

Применительно к закупке систем и сервисов в компании необходимо:

1. выделить достаточный объем ресурсов для адекватной защиты ИС;
2. при разработке систем учитывать требования ИБ;
3. ограничивать использование и установку программного обеспечения;
4. обеспечить выделение внешними поставщиками услуг достаточных ресурсов для защиты информации, приложений и/или сервисов.

В области сертификации, аккредитации и оценки безопасности в организации следует проводить:

1. постоянный мониторинг регуляторов безопасности, чтобы иметь доверие к их эффективности;
2. периодическую оценку регуляторов безопасности, применяемых в ИС, чтобы контролировать их эффективность;

3. разработку и претворение в жизнь плана действий по устранению недостатков и уменьшению или устранению уязвимостей в ИС;
4. авторизацию введения в эксплуатацию ИС и установление соединений с другими информационными системами.

В области кадровой безопасности необходимо:

1. обеспечить надежность (доверенность) должностных лиц, занимающих ответственные посты, а также соответствие этих лиц предъявляемым к данным должностям требованиям безопасности;
2. обеспечить защиту информации и информационной системы при проведении дисциплинарных акций, таких как увольнение или перемещение сотрудников;
3. применять соответствующие официальные санкции к нарушителям политики и процедур безопасности.

Организация должна обеспечить информирование и обучение сотрудников:

1. чтобы руководители и пользователи ИС знали о рисках, связанных с их деятельностью, и о соответствующих законах, нормативных актах, руководящих документах, стандартах, инструкциях и т.п.;
2. чтобы персонал имел должную практическую подготовку для выполнения обязанностей, связанных с информационной безопасностью.

В области планирования необходимо разработать, документировать, периодически изменять и реализовать планы обеспечения безопасности ИС, описывающие регуляторы безопасности (имеющиеся и планируемые) и правила поведения персонала, имеющего доступ к ИС.

С целью планирования бесперебойной работы в компании следует установить, поддерживать и эффективно реализовать планы реагирования на аварийные ситуации, резервного копирования, восстановления после аварий, чтобы обеспечить доступность критичных информационных ресурсов и непрерывность функционирования в аварийных ситуациях.

В плане реагирования на нарушения информационной безопасности организация должна:

1. создать действующую структуру для реагирования на инциденты, имея в виду адекватные подготовительные мероприятия, выявление, анализ и локализацию нарушений, восстановление после инцидентов и обслуживание обращений пользователей;
2. обеспечить прослеживание, документирование и сообщение об инцидентах соответствующим должностным лицам организации и уполномоченным органам.

С целью физической защиты организация должна:

1. предоставлять физический доступ к ИС, оборудованию, в производственные помещения только авторизованному персоналу;
2. физически защищать оборудование и поддерживающую инфраструктуру ИС;
3. обеспечить должные технические условия для функционирования ИС;
4. защищать ИС от угроз со стороны окружающей среды;
5. обеспечить контроль условий, в которых функционирует ИС;
6. обеспечить управление доступом, предоставив доступ к активам ИС только авторизованным пользователям, процессам, действующим от имени этих пользователей, а также устройствам (включая другие ИС) для выполнения разрешенных пользователям транзакций и функций.

Для обеспечения протоколирования и аудита необходимо:

1. создавать, защищать и поддерживать регистрационные журналы, позволяющие отслеживать, анализировать, расследовать и готовить отчеты о незаконной, несанкционированной или ненадлежащей активности;
2. обеспечить прослеживаемость действий в ИС с точностью до пользователя (подотчетность пользователей).

В плане управления конфигурацией в компании следует:

1. установить и поддерживать базовые конфигурации;
2. иметь опись (карту) ИС, актуализируемую с учетом жизненного цикла, в которую входят аппаратура, программное обеспечение и документация;

3. установить и обеспечить практическое применение настроек для конфигурирования средств безопасности в продуктах, входящих в ИС.

В области идентификации и аутентификации необходимо обеспечить идентификацию и аутентификацию пользователей ИС, процессов, действующих от имени пользователей, а также устройств как необходимое условие предоставления доступа к ИС.

Кроме того, необходимо:

Применительно к сопровождению:

1. осуществлять периодическое и своевременное обслуживание ИС;
2. обеспечить эффективные регуляторы для средств, методов, механизмов и персонала, осуществляющих сопровождение.

Для защиты носителей:

1. защищать носители данных как цифровые, так и бумажные;
2. предоставлять доступ к данным на носителях только авторизованным пользователям;
3. санировать или уничтожать носители перед выводом из эксплуатации или перед передачей для повторного использования.

С целью защиты систем и коммуникаций:

1. отслеживать, контролировать и защищать коммуникации (то есть передаваемые и принимаемые данные) на внешних и ключевых внутренних границах ИС;
2. применять архитектурные и аппаратно-программные подходы, повышающие действующий уровень информационной безопасности ИС.

Для обеспечения целостности систем и данных:

1. своевременно идентифицировать дефекты ИС и данных, докладывать о них и исправлять;
2. защищать ИС от вредоносного программного обеспечения;
3. отслеживать сигналы о нарушениях безопасности и сообщения о новых угрозах для информационной системы и должным образом реагировать на них.

Практическое задание

Пользуясь учебником, опишите:

1. Виды и схемы сертификации средств защиты информации.
2. Функции ФСТЭК в области сертификации средств защиты информации.
3. Функции органов сертификации средств защиты информации.
4. Функции испытательных лабораторий (центров).
5. Функции заявителей.
6. Порядок проведения сертификации и контроля.
7. Перечень средств защиты информации, подлежащих сертификации.

Отчет

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

Контрольные вопросы

1. Сформулируйте цели системы сертификации средств защиты информации по требованиям безопасности информации.
2. Организационная структура системы сертификации средств защиты информации по требованиям безопасности информации.
3. Назовите виды и схемы сертификации средств защиты информации.

Практическая работа 5. Требования к безопасности информационных систем в России.

Цель работы: закрепление теоретических знаний в области правового обеспечения информационной безопасности.

Оборудование: учебный персональный компьютер.

Теоретические основы

Подход к безопасности реализован в руководящем документе Государственной технической комиссией при Президенте РФ «Классификация автоматизированных систем и требований по защите информации», выпущенном в 1992 г. Требования всех приведенных ниже документов обязательны для исполнения только для тех государственных либо коммерческих организаций, которые обрабатывают информацию, содержа-щую государственную тайну. Для остальных коммерческих структур документы носят рекомендательный характер. В данном документе выделено 9 классов защищенности автоматизированных систем от несанкционированного доступа к информации, а для каждого класса определен минимальный состав необходимых механизмов защиты и требования к содержанию защитных функций каждого из механизмов в каждом из классов систем.

Классы систем разделены на три группы, причем основным критерием деления на группы приняты специфические особенности обработки информации, а именно:

третья группа — системы, в которых работает один пользователь, до-пущенный ко всей обрабатываемой информации, размещенной на носи-телях одного уровня конфиденциальности; к группе отнесены два класса, обозначенные ЗБ и ЗА;

вторая группа — системы, в которых работает несколько пользовате-лей, которые имеют одинаковые права доступа ко всей информации, обрабатываемой и/или хранимой на носителях различного уровня конфи-денциальности; к группе отнесены два класса, обозначенные 2Б и 2А;

первая группа — многопользовательские системы, в которых одно-временно обрабатывается и/или хранится информация разных уровней конфиденциальности, причем различные пользователи имеют разные права на доступ к информации; к группе отнесено 5 классов: 1Д, 1Г, 1В, 1Б и 1А.

Требования к защите растут от систем класса ЗБ к классу 1 А.

Все механизмы защиты разделены на 4 подсистемы следующего назначения:

- управления доступом;
- регистрации и учета;
- криптографического закрытия;
- обеспечения целостности.

Содержание средств для каждой группы систем приведено в документе. Приведенная в руководящем документе Гостехкомиссии методика распространяется на защиту от несанкционированного доступа к инфор-мации, находящейся непосредственно в ЗУ ЭВМ и на сменных машино-читаемых носителях. Значительно раньше, в 1978 г., Гостехкомиссией были выпущены руководящие документы, определяющие требования к защите информации в автоматизированных системах от утечки по побоч-ным электромагнитным излучениям и наводкам. При разработке назван-ных требований учитывались следующие факторы:

1. Доля грифованной информации в общем объеме обрабатываемой информации.

2. Интенсивность обработки грифованной информации, выражаемая относительной долей времени ее обработки в течение суток.

3. Условия расположения аппаратуры автоматизированной системы.

Наличие рассмотренных методик и закрепление их в официальных документах создает достаточно надежную базу для защиты информации на регулярной основе. Однако нетрудно видеть, что с точки зрения современной постановки задачи защиты информации имеющиеся методики являются недостаточными по ряду причин, а именно:

1) методики ориентированы на защиту информации только в средствах ЭВТ, в то время как имеет место устойчивая тенденция органическо-го сращивания автоматизированных и традиционных технологий об-работки информации;

2) учитываются далеко не все факторы, оказывающие существенное влияние на уязвимость информации, а поэтому и подлежащие учету при определении требований к защите;

3) в научном плане они обоснованы недостаточно за исключением требований к защите информации от утечки по техническим каналам.

Практическое задание.

1. Воспользуйтесь поиском для получения таблицы характеристик классов подсистем защищенности
2. Проанализируйте данную таблицу
3. Выпишите основные требования к информационной безопасности.
4. На основе полученных данных сформулируйте рекомендации по информационной безопасности.

Отчет

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

Контрольные вопросы

1. Сколько классов защищённости существует?
2. Обязательно ли выполнение всех требований изученного документа?
3. Учтены ли в изученном документе новые методы получения доступа?

Практическая работа 6. Оценка состояния безопасности ИС США.

Цель работы изучить Стандарт США "Критерии оценки гарантировано защищенных вычислительных систем в интересах министерства обороны США".

Оборудование: учебный персональный компьютер.

Теоретические основы

Наиболее известным документом, четко определяющим критерии, по которым должна оцениваться защищенность вычислительных систем, и те механизмы защиты, которые должны использоваться в системах обработки секретной (конфиденциальной — в более общей постановке) информации, является так называемая "Оранжевая книга", представляющая собой стандарт США "Критерии оценки гарантировано защищенных вычислительных систем в интересах министерства обороны США" (Trusted Computer Systems Evaluation Criteria — TCSEC), принятый в 1983 году. Его принятию предшествовали пятнадцатилетние исследования, проводившиеся специально созданной рабочей группой и национальным бюро стандартов США.

Стандартом предусмотрено шесть фундаментальных требований, которым должны удовлетворять те вычислительные системы, которые используются для обработки конфиденциальной информации. Требования разделены на три группы: стратегия, подотчетность, гарантии — в каждой группе по два требования следующего содержания.

1. **Стратегия.**

Требование 1 — стратегия обеспечения безопасности: необходимо иметь явную и хорошо определенную стратегию обеспечения безопасности.

Требование 2 — маркировка: управляющие доступом метки должны быть связаны с объектами.

2. **Подотчетность.**

Требование 3 — идентификация: индивидуальные субъекты должны идентифицироваться.

Требование 4 — подотчетность: контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность.

3. **Гарантии.**

Требование 5 — гарантии: вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет достаточного уровня гарантий того, что система обеспечивает выполнение изложенных выше требований (с первого по четвертое).

Требование 6 — постоянная защита: гарантировано защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от "взламывания" и/или несанкционированного внесения изменений.

В зависимости от конкретных значений, которым отвечают автоматизированные системы, они разделены на четыре группы (D, C, B, A), которые названы так:

D — минимальная защита;

C — индивидуальная защита;

B — мандатная защита;

A — верифицированная защита.

Группы систем делятся на классы, причем все системы, относимые к группе D, образуют один класс (D), к группе C — два класса (C1 и C2), к группе B — три класса (B1, B2 и B3), к группе A — один класс (A1 с выделением части систем вне класса).

Ниже рассмотрим названия и краткую характеристику перечисленных классов:

D — минимальная защита — системы, подвергнутые оцениванию, но не отвечающие требованиям более высоких классов;

C1 — защита, основанная на индивидуальных мерах — системы, обеспечивающие разделение пользователей и данных. Они содержат внушающие доверие средства, способные реализовать ограничения по доступу, накладываемые на индивидуальной основе, т.е. позволяющие пользователям иметь надежную защиту их информации и не дающие другим пользователям считывать или разрушать их данные. Допускается кооперирование пользователей по уровням секретности;

C2 — защита, основанная на управляемом доступе — системы, осуществляющие не только разделение пользователей как в системах C1, но и разделение их по осуществляемым действиям;

B1 — защита, основанная на присваивании имен отдельным средствам безопасности — системы, располагающие всеми возможностями систем класса C, и дополнительно должны быть формальные модели механизмов обеспечения безопасности, присваивания имен защищаемым данным (включая и выдаваемые за пределы системы) и средства мандатного управления доступом ко всем поименованным субъектам и объектам;

B2 — структурированная защита — системы, построенные на основе ясно определенной и формально задокументированной модели, с мандатным управлением доступом ко всем субъектам и объектам, располагающие усиленными средствами тестирования и средствами управления со стороны администратора системы;

B3 — домены безопасности — системы, монитор обращений которых контролирует все запросы на доступ субъектов к объектам, не допускающие несанкционированных изменений. Объем монитора должен быть небольшим вместе с тем, чтобы его состояние и работу можно было сравнительно легко контролировать и тестировать. Кроме того должны быть предусмотрены: сигнализация о всех попытках несанкционированных действий и восстановление работоспособности системы;

A1 — верификационный проект — системы, функционально эквивалентные системам класса B3, но верификация которых осуществлена строго формальными методами. Управление системой осуществляется по строго определенным процедурам. Обязательно введение администратора безопасности.

Практическое задание

1. Проанализируйте стандарт "Критерии оценки гарантировано защищенных вычислительных систем в интересах министерства обороны США".

2. Согласно требованиям, предоставленным в стандарте, составьте характеристику вычислительной системы для обработки конфиденциальной информации.
3. Обоснуйте свой выбор решений по защите информации.

Отчет

Отчет должен содержать:
1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

Контрольные вопросы

1. Что такое политика безопасности?
2. Какие элементы включает в себя политика безопасности?
3. Что такое классы безопасности и уровни доверия?
4. Какие требования определяются классами C1 и C2?
5. Какие требования определяются классами B1, B2 и B3?
6. Какие требования определяются классом A1?

Практическая работа 7. Определение классов защищенности средств вычислительной техники от несанкционированного доступа.

Цель работы: изучить и проанализировать руководящий документ "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации".
Оборудование: учебный персональный компьютер.

Теоретические основы

Теоретические основы представлены в руководящем документе "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации"

Практическое задание

1. Изучить документ "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации"
2. Укажите, какие типы НСД рассмотрены в документе.
3. Составить презентацию на тему «Классы защищённости СВТ»

Отчет

Отчет должен содержать:
1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

Контрольные вопросы

1. Как проводится оценка защищённости от НСД?
2. Какие типы документации необходимы СВТ?
3. Чем отличаются классы защищённости СВТ?

Практическая работа 8. **Определение требований к защите информации**

Цель работы: изучить требования, предъявляемые к защите информации, изучить документацию по защите информации.

Оборудование: учебный персональный компьютер.

Теоретические основы

С позиций системного подхода для реализации приведенных принципов процесс, да и сама система защиты информации должны отвечать некоторой совокупности **требований.**

Защита информации должна быть:

- ***централизованной***;

необходимо иметь в виду, что процесс управления всегда централизован, в то время как структура системы, реализующей этот процесс, должна соответствовать структуре защищаемого объекта;

- ***плановой***;

планирование осуществляется для организации взаимодействия всех подразделений объекта в интересах реализации принятой политики безопасности; каждая служба, отдел, направление разрабатывают детальные планы защиты информации в сфере своей компетенции с учетом общей цели организации;

- ***конкретной и целенаправленной***;

защите подлежат абсолютно конкретные информационной ресурсы, могущие представлять интерес для конкурентов;

- ***активной***;

защищать информацию необходимо с достаточной степенью настойчивости и целеустремленности. Это требование предполагает наличие в составе системы информационной безопасности средств прогнозирования, экспертных систем и других инструментариев, позволяющих реализовать наряду с принципом «обнаружить и устранить» принцип «предвидеть и предотвратить»;

- ***надежной и универсальной***, охватывать весь технологический комплекс информационной деятельности объекта;

методы и средства защиты должны надежно перекрывать все возможные каналы утечки информации и противодействовать способам несанкционированного доступа независимо от формы представления информации, языка ее выражения и вида носителя, на котором она закреплена;

- ***нестандартной***(по сравнению с другими организациями), разнообразной по используемым средствам;

- ***открытой*** для изменения и дополнения мер обеспечения безопасности информации;

- ***экономически эффективной***;

затраты на систему защиты не должны превышать размеры возможного ущерба

Практическое задание

1. Воспользуйтесь поиском для составления сводной таблицы документов, регламентирующих требования к информационной безопасности
2. Укажите, какие документы необходимо учитывать при проектировании защиты документации на электронном носителе.
3. Смоделируйте последовательность действий для защиты от копирования информации.

Отчет

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;

6. вывод о проделанной работе.

Контрольные вопросы

1. Перечислите виды защиты информации.
2. Назовите объекты защиты информации и дайте их определения.
3. Назовите способы защиты информации.
4. Назовите свойства информации, составляющие модель информационной безопасности.
5. Назовите основные принципы информационной безопасности.
6. Перечислите условия и требования к защите информации.
7. Дайте определения политики безопасности на объекте и сформулируйте требования, предъявляемые к плану защиты информации

Раздел 4. Правовое обеспечение информационной безопасности

Практическая работа 9. Анализ терминов и определений информационной безопасности

Цель работы проанализировать ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения..

Оборудование: учебный персональный компьютер.

Теоретические основы

Теоретические сведения предоставлены в ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

Практическое задание

1. Изучить ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации.
2. Изучить основные термины и определения
3. Составить глоссарий для памятки по информационной безопасности.

Отчет

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

Контрольные вопросы

1. Как называется умышленно искаженная информация?
2. Как называется информация, к которой ограничен доступ?
3. Какими путями может быть получена информация?
4. Как называются компьютерные системы, в которых обеспечивается безопасность информации?
5. Основной документ, на основе которого проводится политика информационной безопасности?

Практическая работа 10. Работа с ГОСТами в области информационной безопасности

Цель работы на основе ГОСТ Р 53114-2008 получить навыки составления документации в области информационной безопасности.

Оборудование: учебный персональный компьютер.

Практическое задание

1. На основе ГОСТ Р 53114-2008 составить памятку об информационной безопасности для заведения, использующего электронный документооборот.
2. Обосновать достаточность предлагаемых пунктов безопасности.
3. На примере продемонстрировать необходимость соблюдения правил информационной безопасности.

Отчет

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

Контрольные вопросы

1. Какие стандарты включены в ГОСТ Р 53114-2008?
2. Что такое приемлемость уровня риска?

Раздел. 5. Организационные основы защиты информации

Практическая работа 11. Составление инструкции по обработке и хранению конфиденциальных документов

Цель работы составление алгоритма для работы с конфиденциальной информацией.

Оборудование: учебный персональный компьютер.

Теоретические основы

С появлением новых технологий (компьютеры и оргтехника) защитить информацию становится все труднее. Множество конкурентов не упустят малейшей возможности получить конфиденциальную информацию фирмы-конкурента и использовать ее в своих целях. Для того чтобы избежать утечки информации, составляющей тайну фирмы, создаются службы по контролю за документами конфиденциального характера, их передвижением и хранением в организации.

Безопасность ценной документируемой информации определяется степенью ее защищенности от последствий экстремальных ситуаций, в том числе стихийных бедствий, а также пассивных и активных попыток злоумышленника создать потенциальную или реальную угрозу несанкционированного доступа к документам с использованием организационных и технических каналов, в результате чего могут произойти хищение и неправомерное использование злоумышленником информации в своих целях, ее модификация, подмена, фальсификация, уничтожение.

Злоумышленник – это недобросовестный конкурент, лицо, действующее в интересах конкурента, противника или в личных корыстных интересах (агенты иностранных спецслужб, промышленного и экономического шпионажа, криминальных структур, отдельные преступные элементы, психически больные лица и др.). Понятие «злоумышленник» тесно связано с понятием

«постороннее лицо», то есть любое лицо, не имеющее непосредственного отношения к деятельности фирмы (работники коммунальных служб, экстремальной помощи, прохожие и др.), посетители фирмы, работники других организационных структур, а также сотрудники данной фирмы, не имеющие права доступа в определенные помещения, к конкретному документу, информации, базе данных.

Документируемая информация, используемая предпринимателем в бизнесе и управлении предприятием, организацией, банком, компанией или другой структурой (далее – фирма), является его собственной или частной информацией, представляющей для него значительную ценность, его интеллектуальной собственностью.

Ценность информации может быть стоимостной категорией, характеризующей конкретный размер прибыли при ее использовании или размер убытков при ее утрате. Информация часто становится ценной ввиду ее правового значения для фирмы или развития бизнеса, например учредительные документы, программы и планы, договоры с партнерами и посредниками и т. д. Ценность информации может также отражать ее перспективное научное, техническое или технологическое значение.

Информация, имеющая интеллектуальную ценность для предпринимателя, обычно разделяется на два вида:

техническая, технологическая: методы изготовления продукции, программное обеспечение, производственные показатели, химические формулы, результаты испытаний опытных образцов, данные контроля качества и т. п.;

деловая: стоимостные показатели, результаты исследования рынка, списки клиентов, экономические прогнозы, стратегия действий на рынке и т. п.

Ценная информация охраняется нормами гражданского, патентного и авторского права или включается в категорию информации, составляющую тайну фирмы.

Выявление и регламентация реального состава информации, представляющей ценность для предпринимателя и составляющей тайну фирмы, – основополагающие части системы защиты информации. Состав ценной информации фиксируется в специальном перечне, определяющем срок и уровень (гриф) ее конфиденциальности (то есть недоступности для всех), список сотрудников фирмы, которым предоставлено право использовать эти сведения в работе. Перечень, основу которого составляет типовой состав защищаемых сведений фирм данного профиля, является постоянным рабочим материалом руководства фирмы, служб безопасности и конфиденциальной документации. Он представляет собой классифицированный список типовой и конкретной ценной информации о проводимых работах, производимой продукции, научных и деловых идеях, технологических новшествах. В перечень включаются действительно ценные сведения о каждой работе фирмы.

Дополнительно может составляться перечень документов, в которых эти сведения отражаются (документируются). В перечень включаются также документы, не содержащие защищаемую информацию, но представляющие ценность для фирмы и подлежащие охране.

Перечни формируются индивидуально каждой фирмой в соответствии с рекомендациями специальной комиссии и утверждаются первым руководителем фирмы. Эта же комиссия регулярно вносит текущие изменения в перечни в соответствии с динамикой выполнения фирмой конкретных работ.

Коммерческая ценность информации, как правило, недолговечна и определяется временем, необходимым конкуренту для выработки той же идеи или ее хищения и воспроизводства, опубликования и перехода информации в категорию общеизвестных. Степень ценности информации и надежность ее защиты находятся в прямой зависимости.

Документы, содержащие ценную информацию, входят в состав информационных ресурсов фирмы, которые могут быть: а) открытыми (доступными для работы персонала без специального разрешения) и б) ограниченными для доступа к ним персонала (отнесенными к одному из видов тайны – государственной или негосударственной). Документы, содержащие сведения, которые

составляют негосударственную тайну (служебную, коммерческую, банковскую, тайну фирмы и др.) или содержат персональные данные, именуются конфиденциальными.

Несмотря на то, что конфиденциальность является синонимом секретности, этот термин широко используется исключительно для обозначения информационных ресурсов ограниченного доступа, не отнесенных к государственной тайне. Конфиденциальность отражает ограничение, которое накладывает собственник информации на доступ к ней других лиц, то есть собственник устанавливает правовой режим этой информации в соответствии с законом. Вместе с тем к конфиденциальным документам нельзя относить учредительные документы, уставы предпринимательских структур, финансовую документацию, сведения о заработной плате персонала и другую документированную информацию, необходимую правоохранительным и налоговым государственным органам.

Под конфиденциальным документом понимается необходимым образом оформленный носитель документированной информации, содержащий сведения, которые относятся к негосударственной тайне и составляют интеллектуальную собственность юридического или физического лица. Обязательным признаком конфиденциального документа является наличие в нем информации, подлежащей защите. К конфиденциальным относятся следующие документы:

в государственных структурах – документы, проекты документов и сопутствующие материалы, относимые к служебной информации ограниченного распространения (называемые в чиновничьем обиходе документами для служебного пользования), содержащие сведения, отнесенные к служебной тайне, имеющие рабочий характер и не подлежащие опубликованию в открытой печати;

в предпринимательских структурах и направлениях подобной деятельности – документы, содержащие сведения, которые их собственник или владелец в соответствии с законодательством имеет право отнести к коммерческой (предпринимательской) тайне, тайне фирмы, тайне мастерства;

независимо от принадлежности – документы и базы данных, фиксирующие любые персональные (личные) данные о гражданах, а также содержащие профессиональную тайну, технические и технологические новшества (до их патентования), тайну предприятий связи, сферы обслуживания и т. п.

Называть конфиденциальные документы секретными или ставить на них гриф секретности не допускается. Особенностью конфиденциального документа является то, что он одновременно представляет собой:

массовый носитель ценной, защищаемой информации;

основной источник накопления и объективного распространения этой информации, а также ее неправомерного разглашения или утечки;

обязательный объект защиты.

Конфиденциальность документов всегда имеет значительный разброс по срокам ограничения свободного доступа к ним персонала фирмы (от нескольких часов до многих лет). Следует учитывать, что основная масса конфиденциальных документов после окончания их исполнения или работы с ними теряет свою ценность и конфиденциальность. Например, переписка до заключения контракта может иметь гриф конфиденциальности, но после его подписания этот гриф с письменного разрешения первого руководителя фирмы снимается.

Оставшиеся конфиденциальными исполненные документы, сохраняющие ценность для деятельности фирмы, формируются в дела в соответствии с номенклатурой дел. Период нахождения конфиденциальных документов в делах может быть кратковременным или долговременным в зависимости от ценности информации, содержащейся в документах дела. Период конфиденциальности документов определяется по указанному выше перечню конфиденциальных сведений и зависит от специфики деятельности фирмы. Например, производственные, научно-исследовательские фирмы обладают более ценными документами, чем торговые, посреднические и др.

Документы долговременного периода конфиденциальности (программы и планы развития бизнеса, технологическая документация ноу-хау, изобретения до их патентования и др.) имеют усложненный вариант обработки и хранения, обеспечивающий безопасность информации и ее носителя.

Документы кратковременного периода конфиденциальности, имеющие оперативное значение для деятельности фирмы, обрабатываются и хранятся по упрощенной схеме и могут не выделяться из технологической системы обработки открытых документов при наличии в этой системе минимальных защитных, контрольных и аналитических элементов.

Практическое задание

Вариант 1

Вы руководитель фирмы Вам необходимо организовать процесс формирования «Перечня сведений конфиденциального характера». Опишите процесс организации.

Вариант 2

Вы руководитель фирмы Вам необходимо организовать конфиденциальное делопроизводство. Опишите процесс организации.

Вариант 3

Вы руководитель фирмы Вам необходимо организовать процесс осуществления защитных мер в отношении документопотоков. Опишите процесс организации.

Вариант 4
Вы руководитель фирмы и Вам необходимо организовать технологическую систему обработки конфиденциальных документов. Опишите процесс организации.

Отчет

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

Контрольные вопросы

1. Где фиксируется состав ценной информации?
2. Сформулируйте определение конфиденциальных документов?
3. Какие документы не относятся к конфиденциальным документам?
4. Что является обязательным признаком конфиденциального документа?
5. Какие документы относятся к конфиденциальным?

Практическая работа 12. Определение коэффициента важности, полноты, адекватности, релевантности, толерантности информации

Цель работы: работа в тестовой программе (Aida или CPU-z); основные настройки базовой системы ввода вывода.

Оборудование: учебный персональный компьютер.

Теоретические основы

Информация разнообразна по содержанию и виду обслуживаемой ею человеческой деятельности. Каждый вид информации имеет свои особенные технологии обработки, смысловую ценность, формы представления, требования точности и оперативности отражения явлений и процессов.

Однако для любого вида информации можно указать три объекта взаимодействия: источник информации, приемник (потребитель) информации и объект, который данная информация отражает.

С точки зрения потребителя выделяют следующие свойства информации:

релевантность — способность информации соответствовать запросу потребителя;

точность — степень близости информации к реальному состоянию объекта, процесса, явления;

своевременность — способность информации соответствовать запросам потребителя в нужный момент времени;

достоверность — свойство информации не иметь скрытых ошибок;

доступность — свойство, характеризующее возможность ее получения данным потребителем;

защищенность — свойство, характеризующее невозможность несанкционированного доступа к информации;

эргономичность — удобство формы или объема информации для данного потребителя. Если вести речь о научной информации, то здесь наиболее важным свойством является адекватность — однозначное соответствие отображаемому объекту. Данное определение характеризует не взаимоотношение «информация — потребитель», а «информация — отображаемый объект».

Среди внутренних свойств информации важнейшими являются количество информации, ее внутренняя организация и структура. По способу внутренней организации информация делится на две группы: данные, или простой, логически неупорядоченный набор сведений, и логически упорядоченный, организованный набор данных.

К свойствам информации, связанным с ее хранением, относятся:

живучесть — свойство сохранять качество с течением времени;

актуальность — степень соответствия информации текущему моменту времени. оценка достоверности информации

Информация, используемая в процессе оценки, должна отвечать требованиям:

достоверности;

точности;

комплексности;

Используемая информация должна достоверно отражать ситуацию, точно соответствовать целям оценки и комплексно учитывать внешние условия.

Выделяют следующие свойства, характеризующие качество информации:

Объективность информации характеризует её независимость от чьего-либо мнения или сознания, а также от методов получения. Более объективна та информация, в которую методы получения и обработки вносят меньший элемент субъективности. Полнота. Информацию можно считать полной, когда она содержит минимальный, но достаточный для принятия правильного решения набор показателей. Как неполная, так и избыточная информация снижает эффективность принимаемых на основании информации решений.

Достоверность — свойство информации быть правильно воспринятой. Объективная информация всегда достоверна, но достоверная информация может быть как объективной, так и субъективной.

Достоверность — несомненная верность чего-либо. Достоверность следует отличать от истины. Достоверностью являются сведения для субъекта, который их воспринимает. Достоверность становится истиной, если она проверена на опыте и соответствует действительности.

Адекватность — степень соответствия реальному объективному состоянию дела.

Доступность информации — мера возможности получить ту или иную информацию.

Актуальность информации — это степень соответствия информации текущему моменту времени.

Эмоциональность — свойство информации вызывать различные эмоции у людей. Это свойство информации используют производители Медиа-информации. Чем сильнее вызываемые эмоции, тем больше вероятности обращения внимания и запоминания информации.

В информатике понятие достоверности связывается с понятием информация - сведениями о людях, предметах, фактах, событиях т процессах независимо от формы их представления, а под достоверностью информации - соответствии этих сведений реальной действительности.

Особое значение достоверность имеет в отношении информации. Достоверная информация воспринимается как истина, а недостоверная информация - как ложь. Мы говорим, что информация достоверна, если мы имеем возможность использовать ее без дополнительной проверки.

Для принятия решений по ней также необходимы такие качества информации как полнота, актуальность, ценность и др. В случае неполной, недостоверной, противоречивой, неактуальной информации принятие решений по ней затруднительно. В этом случае, выполняются работы по увеличению достоверности, полноты и ценности информации и попытки принятия решений в условиях неопределенности. Во многих областях деятельности добиться полноты и достоверности информации невозможно.

Причинами недостоверности могут быть:

- преднамеренное искажение (дезинформация);
- непреднамеренное искажение субъективного свойства;
- искажение в результате воздействия помех;
- ошибки фиксации информации;

В общем случае достоверность информации достигается:

- указанием времени свершения событий, сведения о которых передаются;
- сопоставлением данных, полученных из различных источников;
- своевременным вскрытием дезинформации;
- исключением искажённой информации и др.

Практическое задание

Оцените результат поиска в сети Интернет и ответьте на вопросы:

1. Какую поисковую систему ты использовал?
2. Адрес сайта, который ты изучал.
3. Название сайта.
4. Долго ли загружается страница?
5. Привлекательно ли она выглядит?
6. Легко ли читается?
7. Есть ли изображения? Какого качества?
8. Несут ли изображения дополнительную информацию?
9. Указаны ли имя и адрес электронной почты автора сайта?
10. Есть ли указание, когда был подготовлен (обновлен) сайт?
11. Есть ли возможность при переходе на следующие страницы автоматически вернуться на первую?
12. Достаточно ли полно заглавие сайта раскрывает его содержание?
13. Смог бы ты получить больше информации из печатного справочника?
14. Во всем ли ты согласен с автором?
15. Не попадалась ли тебе неверная информация?
16. Достаточно ли актуальна предложенная информация?
17. Есть ли на сайте отсылки к другим сайтам с похожей информацией?

Отчет

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

Контрольные вопросы

1. Назовите причины недостоверности информации?

2. Каким требованиям должна соответствовать оценочная информация?

Практическая работа 13. Оценка безопасности информации на объектах ее обработки

Цель работы ознакомиться с проблемами реализации политик безопасности в компьютерных системах.

Оборудование: учебный персональный компьютер.

Теоретические основы

Под политикой безопасности понимают набор норм, правил и практических приемов, регулирующих управление, защиту и распределение ценной информации. Политика безопасности задает механизмы управления доступа к объекту, определяет как разрешенные, так и запрещенные доступы.

Политика безопасности реализуется посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты. Для конкретной организации политика безопасности должна носить индивидуальный характер и зависеть от конкретной технологии обработки информации и используемых программных и технических средств.

Политика безопасности определяется способом управления доступом, который задаёт порядок доступа к объектам системы. Различают два основных вида политики безопасности: избирательную и полномочную.

Избирательная политика безопасности основана на избирательном способе управления доступом. Избирательное (или дискреционное) управление доступом характеризуется заданным администратором множеством разрешенных отношений доступа (например, в виде троек объект – субъект – тип доступа). Обычно для описания свойств избирательного управления доступом применяют математическую модель на основе матрицы доступа.

Матрица доступа представляет собой матрицу, в которой столбец соответствует объекту системы, а строка – субъекту. На пересечении столбца и строки матрицы указывается тип разрешенного доступа субъекта к объекту. Обычно выделяют такие типы доступа субъекта к объекту, как «доступ на чтение», «доступ на запись», «доступ на исполнение» и т.п. Матрица доступа является самым простым подходом к моделированию систем управления доступом. Однако она служит основой для сложных моделей, более адекватно описывающих реальные автоматизированные системы обработки информации (АСОИ).

Избирательная политика безопасности широко применяется в АСОИ коммерческого сектора, так как её реализация соответствует требованиям коммерческих организаций по разграничению доступа и подотчетности, а также имеет приемлемую стоимость.

Полномочная политика безопасности основана на полномочном (мандатном) способе управления доступом. Полномочное (или мандатное) управление доступом характеризуется совокупностью правил предоставления доступа, определенных на множестве атрибутов безопасности субъектов и объектов, например, в зависимости от метки конфиденциальности информации и уровня допуска пользователя. Полномочное управление доступом подразумевает, что:

1) все субъекты и объекты системы однозначно идентифицированы;

2) каждому объекту системы присвоена метка конфиденциальности информации, определяющая ценность содержащейся в нем информации;

3) каждому субъекту системы присвоен определенный уровень допуска, определяющий максимальное значение метки конфиденциальности информации объектов, к которым субъект имеет доступ.

Чем важнее объект, тем выше его метка конфиденциальности. Поэтому наиболее защищенными оказываются объекты с наиболее высокими значениями метки конфиденциальности.

Основное назначение полномочной политики безопасности – регулирование доступа субъектов системы к объектам с различными уровнями конфиденциальности, предотвращение

утечки информации с верхних уровней должностной иерархии на нижние, а также блокирование возможных проникновений с нижних уровней на верхние.

При выборе и реализации политики безопасности в компьютерной системе, как правило, работают следующие шаги:

1. В информационную структуру вносится структура ценностей (определяется ценность информации) и проводится анализ угроз и рисков для информации и информационного обмена.

2. Определяются правила использования для любого информационного процесса, права доступа к элементам информации с учетом данной оценки ценностей.

Реализация политики безопасности должна быть четко продумана. Результатом ошибочного или бездумного определения правил политики безопасности, как правило, является разрушение ценности информации без нарушения политики.

Практическое задание

Необходимо провести анализ защищенности объекта защиты информации по следующим разделам:

1. Виды возможных угроз
2. Характер происхождения угроз
3. Классы каналов несанкционированного получения информации
4. Источники появления угроз
5. Причины нарушения целостности информации
6. Потенциально возможные злоумышленные действия
7. Определить класс защищенности автоматизированной системы

Отчет

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

Контрольные вопросы

1. Что понимается под политикой безопасности в компьютерной системе?
2. В чем заключается модель политики безопасности в компьютерной системе?

Раздел 6. Обеспечение безопасности автоматизированных систем.

Практическая работа 14. Классификация автоматизированных систем обработки информации по классу защиты информации

Цель работы закрепление знаний основного понятийного аппарата, применяемого в области защиты информации, формирование навыка работы с нормативными документами по исследуемому вопросу.

Оборудование: учебный персональный компьютер.

Теоретические основы

Система защиты информации (СЗИ) в самом общем виде может быть определена как организованная совокупность всех средств, методов и мероприятий, выделяемых (предусматриваемых) на объекте информатизации (ОИ) для решения в ней выбранных задач по защите. Введением понятия СЗИ определяется тот факт, что все ресурсы, выделяемые для защиты информации, должны объединяться в единую, целостную систему, которая является

функционально самостоятельной подсистемой любого ОИ. Таким образом, важнейшим концептуальным требованием к СЗИ является требование адаптируемости, то есть способности к целенаправленному приспособлению при изменении структуры, технологических схем или условий функционирования ОИ. Важность требования адаптируемости обусловливается, с одной стороны, возможностью изменяться перечисленным факторам, а с другой — отношением процессов защиты информации к слабоструктурированным, то есть имеющим высокий уровень неопределенности. Управление же слабоструктурированными процессами может быть эффективным лишь при условии адаптируемости системы управления. Помимо общего концептуального требования, к СЗИ предъявляется еще целый ряд более конкретных, целевых требований, которые могут быть разделены на:

— функциональные;
— эргономические;
— экономические;
— технические;
— организационные.

Сформированная к настоящему времени система включает следующий перечень общеметодологических принципов:

— концептуальное единство;
— адекватность требованиям;
— гибкость (адаптируемость);
— функциональная самостоятельность;
— удобство использования;
— минимизация предоставляемы х прав;
— полнота контроля;
— адекватность реагирования;
— экономичность.

Концептуальное единство означает, что архитектура, технология, организация и обеспечение функционирования как СЗИ в целом, так и составных ее компонентов должны рассматриваться и реализовываться в строгом соответствии с основными положениями е диной концепции защиты информации. Адекватность требованиям означает, что СЗИ должна строиться в строгом соответствии с требованиями к за щите, которые, в свою очередь, определяются категорией соответствующего объекта и значениями параметров, влияющих на защиту информации.

Гибкость (адаптируемость) системы защиты означает такое построение и такую организацию ее функционирования, при которых функции защиты осуществлялись бы достаточно эффективно при изменении в некотором диапазоне структуры ОИ, технологических схем или условий функционирования каких-либо ее компонентов. Функциональная самостоятельность предполагает, что СЗИ должна быть самостоятельной обеспечивающей подсистемой системы обработки информации и при осуществлении функций защиты не должна зависеть от других подсистем. Удобство использования означает, что СЗИ не должна создавать дополнительных неудобств для пользователей и персонала ОИ. Минимизация предоставляемых прав означает, что каждому пользователю и каждому лицу из состава персонала ОИ должны предоставляться лишь те полномочия на доступ к ресурсам ОИ и находящейся в ней информации, которые ему действительно необходимы для выполнения своих функций в процессе автоматизированной обработки информации. При этом предоставляемые права должны быть определены и утверждены заблаговременно в установленном порядке. Полнота контроля предполагает, что все процедуры автоматизированной обработки защищаемой информации должны контролироваться системой защиты в полном объеме, причем основные результаты контроля должны фиксироваться в специальных регистрационных журналах. Активность реагирования означает, что СЗИ должна реагировать на любые попытки несанкционированных действий. Характер реагирования может быть различным и включает: просьбу повторить действие; отключение структурного элемента, с которого осуществлено несанкционированное действие; исключение нарушителя из числа зарегистрированных пользователей; подачу специального сигнала и др. Экономичность СЗИ означает, что при условии соблюдения основных требований всех предыдущих принципов расходы на СЗИ должны быть минимальными.

Практическое задание

Необходимо предложить анализ увеличения защищенности объекта защиты информации по следующим разделам:

1. Определить требования к защите информации
2. Классифицировать автоматизированную систему
3. Определить факторы, влияющие на требуемый уровень защиты информации
4. Выбрать или разработать способы и средства защиты информации
5. Построить архитектуру систем защиты информации
6. Сформулировать рекомендации по увеличению уровня защищенности

Отчет

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

Контрольные вопросы

1. Что такое гибкость системы?
2. В чём она выражается?
3. Как определяют требования к защите информации?

Практическая работа 15. Планирование, создание и изменение учетных записей пользователей.

Цель работы *познакомиться с основами администрирования операционной системы Windows*.

Оборудование: учебный персональный компьютер.

Теоретические основы

Для входа в систему Windows нужно иметь заранее созданную учетную запись. Если рабочая станция включена в рабочую группу, а не в домен, эта учетная запись должна храниться на этой станции. Чтобы войти в домен, необходима учетная запись в этом домене (или в доверенном домене).

Учетная запись содержит не только имя и другие данные, идентифицирующие пользователя, но и определяет, каким образом пользователь регистрируется, когда он может входить в систему, какие ресурсы ему доступны и каков его уровень доступа к этим ресурсам. Другими словами, учетная запись определяет все аспекты доступа к компьютеру и в сеть. Кроме того, каждая учетная запись содержит пароль, обеспечивающий ее безопасное использование.

Права пользователя определяются не только учетной записью, но и членством в группах. **Группа** – это совокупность пользователей, выполняющих сходную работу и имеющих примерно одинаковые потребности в ресурсах.

Windows поддерживает два типа групп.

– **Глобальные группы.** Глобальная группа может содержать учетные записи пользователей только того домена, где она создана. Права доступа к ресурсам других доменов глобальные группы получают в рамках доверительных отношений между доменами.

– **Локальные группы.** Локальная группа может иметь в своем составе как индивидуальных пользователей, так и глобальные группы. Это позволяет объединять в одной локальной группе пользователей из различных доменов и управлять ими коллективно. Права локальной группы распространяются только на тот домен, где она создана.

В подавляющем большинстве группы используются, чтобы упростить контроль за доступом к общим ресурсам. Сначала создается группа и задается ей право доступа к

конкретному ресурсу, а затем включается сюда пользователь, которому этот ресурс необходим. Позже, когда потребуется изменить уровень доступа к ресурсу (например, наложить ограничения на его изменение), будет достаточно модифицировать права группы, и все ее члены наследуют новые права на общий ресурс. Это значительно легче, чем изменять привилегии каждой индивидуальной учетной записи в группе.

4.1.2. Доверительные отношения

Доверительным называют особые логические отношения между доменами, при которых один домен доверяет пользователям другого домена. Домен-доверитель открывает пользователям доверенного домена доступ к своим ресурсам. Если, например, домен А является доменом-доверителем, а домен Б – доверенным доменом, то пользователь домена Б может работать и с ресурсами домена А. Доверительные отношения могут быть как односторонними, так и двусторонними. То, что домен А доверяет домену Б, вовсе не означает, что домен Б доверяет домену А. Для установления двусторонних доверительных отношений необходимо явно указать, что домен А доверяет домену Б.

4.1.3. Встроенные группы

Windows XP содержит целый ряд встроенных учетных записей и групп. Одна из них – учетная запись администратора, которая создается при установке операционной системы. Учетную запись администратора нельзя удалить или отключить, ее можно только переименовать. В число встроенных входит и учетная запись гостя, которую также нельзя удалить, но можно переименовать или отключить. Эта запись применяется для регистрации в компьютере без использования специально созданной учётной записи. Она не требует ввода пароля и по умолчанию заблокирована.

Администраторы (Administrators). Члены группы “Администраторы” получают практически неограниченный доступ к ресурсам домена, сервера или рабочей станции, где находится группа, и полную власть над ними. Они могут также использовать любые файлы и каталоги раздела FAT, однако полного доступа к каталогам файловой системы NTFS автоматически не получают. Право доступа им должен предоставить владелец файла или каталога, в противном случае даже администратор не может использовать этот ресурс. Правда, за администратором остается право присвоить себе любой ресурс и тем самым получить к нему полный доступ.

Операторы архива (Backup Operators). Эта локальная группа создана специально для архивирования файлов. Пользователи, входящие в группу “Операторы архива”, получают право проводить резервное копирование и восстановление файлов, локально входить в систему и завершать ее работу. Однако операторы архива лишены возможности изменять параметры безопасности и выполнять другие административные задачи.

Опытные пользователи (Power Users). Опытные пользователи – это пользователи, которым предоставлены некоторые административные привилегии. Они могут создавать новые учетные записи и вносить изменения в те, которые создали сами. Кроме того, они могут включать учетные записи в группы пользователей, гостей и опытных пользователей, а также разрешать или запрещать совместное использование файлов и принтеров на локальных рабочих станциях и серверах.

Пользователи (Users). Это самая многочисленная группа. Члены этой группы могут выполнять большинство пользовательских функций, например, запускать приложения, пользоваться локальным или сетевым принтером, завершать работу системы или блокировать рабочую станцию. Они могут также создавать локальные группы и регулировать состав их членов.

Гости (Guests). Члены этой группы обладают ограниченными правами на доступ к ресурсам системы и могут завершать работу системы. В отличие от пользователей гостям запрещен локальный вход на сервер, хотя они могут регистрироваться на нем через сеть.

Репликаторы (Replicator). Эта специальная группа создана, чтобы упростить тиражирование файлов и каталогов.

Главное в концепции учетных записей и групп состоит в том, что они упрощают администрирование ресурсов и доступ к ним. Вместо того чтобы задавать конкретные права

каждому пользователю, можно создать группу с этими правами, а затем по мере необходимости включать в нее пользователей. Важно понимать, что пользователь может быть членом нескольких групп и что одна группа способна включать в себя другую.

Практическое задание

1. Откройте Панель управления с помощью меню Пуск, щелкните кнопкой мыши на ссылке Добавление и удаление учетных записей пользователей и подтвердите действия в окне UAC.

2. В окне Учетные записи пользователей щелкните кнопкой мыши на ссылке Создание учетной записи.

3. В появившемся окне введите имя учетной записи, оставьте переключатель типа учетной записи в положении Обычный доступ и нажмите кнопку Создание учетной записи.

4. Выйдите из системы. Для этого нажмите кнопку Пуск, щелкните кнопкой мыши на стрелке рядом с кнопкой Блокировка и выполните команду Выход из системы.

5. На экране приветствия щелкните кнопкой мыши на значке новой учетной записи и дождитесь входа в систему.

6. Снова откройте окно Учетные записи пользователей, щелкнув кнопкой мыши на значке учетной записи в меню Пуск.

7. Перейдите по ссылке Создание пароля своей учетной записи, в появившемся окне введите один и тот же пароль в поля Новый пароль и Подтверждения пароля, по сле чего нажмите кнопку Создать пароль. Подсказка о пароле не является обязательной, но она может помочь вспомнить забытый пароль.

8. Щелкните кнопкой мыши на ссылке Изменение своего рисунка и выберите другое изображение для значка учетной записи.

9. Попробуйте выполнить настройки, которые запрещены для обычных пользователей, изменить системное время. Должно появиться окно, в котором нужно ввести пароль для одной из учетных записей с правами администратора.

10. Создайте текстовый документ или рисунок в личной папке Документы и скопируйте его в папку Общие. Значок папки Общие можно найти на панели Избранные ссылки программы Проводник.

11. Выйдите из системы и снова войдите с использованием учетной записи, обладающей правами администратора.

12. Попробуйте открыть ранее скопированный документ из папки Общие и внести в него изменения.

13. Попробуйте открыть личную папку ранее созданной учетной записи, которая находится по адресу C:ПользователиИмя_пользователя. Доступ к ней будет запрещен, однако после подтверждений в окнах UAC вы сможете получить доступ к файлам других пользователей.

14. Откройте окно Учетные записи пользователей и удалите ранее созданную учетную запись. Будет предложено сохранить личные файлы удаляемой учетной записи на Рабочем столе. Вы можете согласиться или удалить их окончательно.

Отчет

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

Контрольные вопросы

1. Перечислите способы создания учетных записей пользователей на ПК
2. Опишите технологию создания учетной записи с помощью панели управления
3. Перечислите действия, которые можно выполнять с созданной учетной записью
4. Как установить членство в группе?

Практическая работа 16. Создание и администрирование групп пользователей.

Цель работы научиться создавать группы и изменять их области действия.
Оборудование: учебный персональный компьютер.

Теоретические основы

Пользователи, группы и компьютеры — ключевые объекты в службе каталогов Active Directory, так как они позволяют всем, кто использует компьютер в сети, идентифицировать себя в качестве участника безопасности. Без такой идентификации персонал не сможет получить доступ к компьютерам, программам и данным, необходимым для повседневной работы. Хотя для минимальной идентификации достаточно знать имя пользователя и компьютера, управление участниками безопасности для отдельного пользователя серьезно усложнится, если не организовать пользователей в группы. На определенном этапе назначать разрешения каждому из множества пользователей станет просто невозможно, однако при разумном использовании групп назначение разрешений и управление ими сильно упрощается.

В Windows существует два типа групп, каждая из которых может иметь три области действия. Понимание их структуры в рамках соответствующей области действия гарантирует оптимальное распределение административных ресурсов при управлении правами доступа к ресурсам. Возможности конструкции группы также зависят от того, в каком режиме работает их родительский домен или лес Windows Server 2003: основном, промежуточном или смешанном. В Windows несколько групп уже созданы предварительно, или встроены. Вы можете создать дополнительно столько групп, сколько пожелаете.

Группы (groups) — это контейнеры, содержащие объекты пользователей и компьютеров. Если разрешения безопасности для группы заданы в таблице управления доступом (access control list, ACL) для некоего ресурса, то их получают все члены группы.

В Windows существует два типа групп: безопасности и распространения. Группы безопасности (security groups) используют для назначения разрешений доступа к сетевым ресурсам. Группы распространения (distribution groups) применяются для объединения пользователей в списки рассылки электронной почты. Группу безопасности можно использовать в качестве группы распространения, но не наоборот. Правильное планирование структуры групп влияет на производительность и масштабируемость, особенно в корпоративных средах, содержащих множество доменов.

Совет Хотя в таблицах ACL можно задавать параметры для отдельных участников безопасности (пользователей и компьютеров), эта практика должна быть скорее исключением из общего правила. Если вы обнаружите, что задаете в ACL слишком много исключений для пользователя какой-либо группы, пересмотрите его членство в этой группе.

Область действия группы (group scope) определяет, каким образом участникам группы назначаются разрешения. В Windows и группы безопасности, и группы распространения классифицируют по трем областям действия: локальная доменная, глобальная и универсальная.

Примечание Хотя локальные группы не классифицируются по области действия Windows, они включены для полноты картины.

Локальные группы (local groups), или локальные группы компьютеров, используются в основном для обратной совместимости с Windows NT 4. На компьютерах с Windows существуют локальные пользователи и группы, сконфигурированные как рядовые серверы. Контроллеры доменов не используют локальные группы.

• Локальные группы могут содержать участников из любого домена в пределах леса, из доверенных доменов в других лесах и более низкого уровня.

• Локальная группа действует в пределах конкретного компьютера и может предоставлять разрешения для ресурсов только на этом компьютере.

Локальные группы домена (domain local groups) главным образом используются для назначения глобальным группам разрешений на доступ к локальным ресурсам домена.

Характерные черты локальных групп домена таковы.

• Существуют во всех режимах работы доменов и лесов — смешанном, промежуточном и основном.

• Локальная группа домена функционирует подобно локальной группе на контроллере домена, пока домен работает в смешанном режиме.

• Могут содержать участников из любого домена в пределах леса, из доверенных доменов в других лесах и более низкого уровня.

• Действуют в пределах домена в основном режиме Windows и могут использоваться для предоставления прав на ресурсы на любом компьютере с Windows в том домене, где определена группа.

Глобальные группы (global groups) чаще используются для предоставления категоризированного членства в локальных группах доменов для отдельных участников безопасности и для прямого назначения разрешений (в частности, в доменах смешанного или промежуточного режимов). Часто глобальные группы применяются для объединения пользователей или компьютеров в одном домене и совместного исполнения одной работы, роли или функции. Характеристики глобальных групп таковы.

• Существуют во всех режимах работы доменов и лесов — смешанном, промежуточном и основном.

• Могут содержать только членов из своего домена.

• Могут сами являться членами локальной группы компьютера или домена.

• Могут содержать другие глобальные группы.

Универсальные группы (universal groups) в основном применяют для предоставления доступа к ресурсам во всех доверенных доменах. Однако такие группы могут использоваться только как участники безопасности (то есть как группы безопасности) в доменах, работающих в основном режиме Windows 2000 или в режиме Windows Server 2003.

• Универсальные группы могут содержать участников из любого домена в лесу.

• универсальным группам могут предоставляться разрешения в любом домене, включая доверенные домены в других лесах.

Совет Универсальные группы помогают представить и объединить группы, которые распределены по разным доменам и выполняют типичные функции в рамках вашей организации. Рекомендуется делать универсальными широко используемые и редко изменяемые группы.

Преобразование групп.

Консоль Active Directory — пользователи и компьютеры (Active Directory Users And Computers) является основным средством, которое вы будете использовать для управления объектами (пользователями, группами и компьютерами) в домене. При создании групп вы будете указывать область действия, тип и состав. Также с помощью этой консоли вы сможете изменить состав существующих групп.

Обычно группы создают из консоли Active Directory — пользователи и компьютеры (Active Directory Users And Computers), ярлык которой расположен в группе программ Администрирование (Administrative Tools). В окне консоли щелкните правой кнопкой в правой панели контейнера, где вы хотите создать группу, и выберите Создать (New)\Группа (Group). Затем определите тип и область действия создаваемой группы.

Практическое задание.

Задание1 . Создание и изменение группы

В этом упражнении вы измените тип группы и ее область действия.

1. В консоли *Active Directory — пользователи и компьютеры* раскройте контейнер Users и создайте в нем глобальную группу распространения Agents.

2. Щелкните правой кнопкой группу Agents и выберите **Свойства (Properties).** Можете ли вы изменить область действия и тип этой группы? Почему?

Если вы не можете изменить тип и область действия группы, ваш домен работает в смешанном режиме Windows 2000 или в промежуточном режиме Windows Server 2003. Чтобы изменить тип

или область действия группы, необходимо перевести домен в основной режим Windows 2000 или в режим Windows Server 2003.

Задание 2. Вложенные группы

В этом упражнении вы познакомитесь со вложенными группами, а также изучите возможные комбинации членства.

1. Домен должен работать в режиме Windows Server 2003. Если это не так, измените режим домена в консоли *Active Directory — пользователи и компьютеры.*
2. Создайте три глобальные группы в ОП Users: Group1, Group2 и Group3.
3. Добавьте три учетные записи пользователей: User1, User2 и User3.
4. Добавьте User1, User2 и User3 в группу Group1.
5. Добавьте Group1 в группу Group2.

Какие группы теперь можно преобразовать в универсальные? Проверьте свои теоретические знания (вы должны без проблем преобразовать две из трех этих групп).

Отчет

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

Контрольные вопросы

1. Какой тип доменной группы больше всего похож на локальную группу на рядовом сервере? В чем их сходство?
2. Вы используете универсальные группы в своем домене или в лесу, и вам нужно предоставить санкционированный доступ членам универсальной группы. Какая конфигурация необходима для использования универсальной группы?
3. На какой вкладке в окне свойств группы можно добавить в нее пользователей?

Практическая работа 17. Планирование и установка разрешений NTFS для файлов, папок отдельным пользователям и группам.

Цель работы научиться использовать общие папки для предоставления доступа к сетевым ресурсам

Оборудование: учебный персональный компьютер.

Теоретические основы

Общие папки (shared folders) обеспечивают доступ полномочных пользователей сети к файловым ресурсам.

Разрешения доступа к общей папке

Общая папка может содержать приложения, данные или личную папку пользователя (home folder). Каждый тип данных требует различных разрешений доступа.

Поскольку разрешения доступа применяются ко всей общей папке, а не к отдельным файлам, они предоставляют менее избирательную защиту, чем разрешения NTFS.

Разрешения доступа к общей папке не ограничивают доступ пользователей, работающих на компьютере, где расположена эта папка. Они применяются только к тем, кто обращается к папке по сети.

Разрешения доступа к общей папке — единственный способ обеспечить безопасность сетевых ресурсов на томе FAT. Разрешения NTFS на томах FAT недоступны.

По умолчанию группа Everyone (Все) получает разрешение Full Control(Полный доступ) для всех новых общих папок.

Разрешения доступа к общим папкам

Разрешение	Позволяет

Изменение	Создавать папки, добавлять к ним файлы, изменять и добавлять данные в файлах, изменять атрибуты файла, удалять папки (файлы) и выполнять действия, допускаемые разрешением Read.
(Чтение)	Просматривать список папок и файлов, содержание файлов и их атрибуты; запускать программы и изменять папки, вложенные в общую папку.
(Полный доступ)	Изменять разрешения для файлов, вступать во владение (Полный доступ) файлами и выполнять все действия, допускаемые разрешением Change.

Можно предоставлять (отменять) разрешения доступа к общей папке. Обычно удобнее назначать разрешения группе, чем отдельным пользователям. Отменять же разрешения следует, только чтобы предотвратить применение нежелательных разрешений. Обычно это происходит, когда в полномочную группу включен пользователь, для которого надо ограничить доступ. Чтобы запретить все виды доступа к общей папке, отмените разрешение Full Control.

Применение разрешений доступа к общей папке

Вид доступа к общей папке зависит от разрешений, назначенных учетным записям пользователей и групп. Далее рассматриваются последствия применения разных разрешений.

• Несколько разрешений совмещаются. Пользователь может участвовать в нескольких группах, каждая из которых имеет разные разрешения с разными уровнями доступа к общей папке. Действующие разрешения пользователя являются комбинацией разрешений его собственных группы, членом которой он является. Например, имея разрешение Read (Чтение) и, будучи членом группы, с разрешением Change (Изменить), пользователь будет обладать разрешением Change, включающим в себя Read.

• Запрет приоритетнее разрешения. Если пользователю запрещен доступ к общей папке, он не будет иметь его, даже если это разрешено группе, к которой он принадлежит.

• Для доступа к ресурсам на томах NTFS требуются разрешения NTFS. Разрешений общей папки достаточно, чтобы получить доступ к ресурсам на томе FAT, но не на томе NTFS. Для доступа к общей папке на диске NTFS помимо разрешения доступа к общей папке требуются и соответствующие разрешения NTFS для каждого общего файла и папки.

• Общий доступ к скопированным или перемещенным папками прекращается. При копировании общей папки, общим останется оригинал, но не копия. Перемещенная папка перестает быть общей.

Основные правила назначения разрешений на доступ к общей папке

Основные правила назначения разрешений на доступ к общей папке можно сформулировать следующим образом.

• Определите группы, которым необходим доступ к данному ресурсу и требуемый уровень доступа. Составьте документацию по группам и их разрешениям для каждого ресурса.

• Назначайте разрешения группам, а не отдельным учетным записям пользователей.

• Назначайте для ресурса максимально строгие разрешения, позволяющие пользователям выполнять только необходимые задачи. Например, если пользователям нужно только читать информацию в папке, а не удалять или создавать в ней файлы, назначьте разрешение Read.

• Папки с одинаковыми требованиями безопасности должны принадлежать одной папке. Скажем, если пользователям требуется разрешение Read для нескольких папок приложения, поместите их в одну и предоставьте к ней совместный доступ (вместо предоставления доступа для каждой папки в отдельности).

Планирование общих папок

Продуманная структура общих папок позволяет централизовать администрирование и упростить доступ к данным. Общие папки могут содержать программы и данные и позволяют создать места для централизованного хранения пользователями своих данных.

Общие папки программ применяют для серверных приложений, к которым может обращаться компьютер клиента. Главный плюс общих приложений в том, что вам не нужно устанавливать и поддерживать их компоненты на каждом компьютере. В то время как файлы программ для приложений могут храниться на сервере, данные о конфигурации большинства сетевых программ, как правило, хранятся на компьютерах клиентов. Способ открытия доступа к

папкам программ во многом зависит от конкретного приложения, параметров сети и организации работы на предприятии.

• Создав одну папку и разместив в ней все ваши программы, вы устанавливаете единое место для размещения и модернизации ПО.

• Назначьте группе Administrators (Администраторы) разрешение Full Control (Полный доступ) для папки программ, чтобы группа могла управлять прикладным ПО и контролировать разрешения пользователей.

• Отмените разрешение Full Control для группы Everyone (Все) и назначьте разрешение Read (Чтение) для группы Users (Пользователи). Это повысит безопасность, так как группа Users включает только созданные вами учетные записи, а группа Everyone — любого, кто получил доступ к сетевым ресурсам, в том числе учетную запись Guest(Гость).

Для обмена по сети рабочими и общими данными служат папки данных. Папки данных лучше хранить на отдельном томе, где не установлена ОС или приложения. Файлы данных рекомендуется регулярно архивировать, и если они будут храниться на отдельном томе, этот процесс упростится. Кроме того, том с папками данных не будет затронут, если потребуется переустановить ОС.

Предоставляя доступ к папкам общих данных: используйте централизованные папки данных, чтобы было легче их архивировать; назначьте группе Users разрешение Change (изменение)— это обеспечит пользователям единое общедоступное место для хранения данных, которыми они хотят обмениваться; пользователи также смогут получать доступ к папкам, читать, создавать или изменять в них файлы. Открывая доступ к папке рабочих файлов, необходимо: назначить группе (Администраторы) разрешение (Полный доступ) для главной папки данных, чтобы администраторы могли централизованно выполнять ее обслуживание; предоставить доступ к вложенным папкам данных, задав разрешение (Изменение) соответствующим группам.

Открытие доступа к папкам

Открыть доступ к ресурсам можно, сделав общими содержащие их папки. Для этого вы должны быть членом одной или нескольких групп, в зависимости от роли компьютера, на котором находятся общие папки. Доступом к папке и ее содержимому можно управлять, ограничивая количество пользователей, которые могут одновременно к ней обращаться, и назначая разрешения отдельным пользователям и группам. Вы можете изменить параметры общей папки: закрыть к ней доступ, изменить ее сетевое имя, а также разрешения пользователей и групп.

Открыть доступ к папкам в Windows 2000 Professional вправе только члены встроенных групп Administrators (Администраторы) и Power Users (Опытные пользователи). Какие другие группы могут это делать, и на каких машинах, зависит от того, входят они в рабочую группу или домен, а также от типа компьютера, хранящего общие папки.

• В домене Windows 2000 участникам групп Administrators и Server Operators (Операторы сервера) разрешено открывать доступ к папкам на любой машине домена. Power Users могут открыть доступ к папкам только на изолированном сервере или компьютере Windows 2000 Professional, где зарегистрирована эта группа.

• В рабочей группе Windows 2000 участникам групп Administrators и Power Users разрешено открывать доступ к папкам на изолированном сервере с Windows 2000 Server или на компьютере с Windows 2000 Professional, где зарегистрирована эта группа.

Для доступа к папке на томе NTFS требуется минимум разрешение Read (Чтение).

Windows 2000 автоматически открывает доступ к административным папкам. Эти папки обозначаются знаком доллара ($), который скрывает общие папки от пользователей, просматривающих содержание компьютера. Корневая папка каждого тома, системная папка и местоположение драйверов принтеров — все это скрытые общие папки, к которым можно получить доступ по сети.

Ресурс	Административные общие папки
C$, D$, E$ и т. д.	К корневой папке на каждом жестком диске автоматически открыт доступ, причем имя совместно используемого ресурса — это имя диска со значком доллара ($). Подключившись к этой папке, вы получите доступ ко всему диску. Административные ресурсы используются для удаленного администрирования компьютеров.

	Windows 2000 назначает группе Administrators (администраторы) разрешение (Полный доступ). Windows 2000 автоматически открывает доступ к приводам CD-ROM, имя этого ресурса состоит из буквы диска и знака доллара.
Admins$	Главная системная папка, по умолчанию C:\Winnt, открыта для доступа под именем Admin$. Члены группы Administrators могут обращаться к ней, не зная, где на самом деле она находится. Windows 2000 назначает группе Administrators разрешение Full Control.
Prints$	Когда вы установите первый общий принтер, папка systemroot\System32\Spool\Drivers будет открыта для доступа под именем Print$; она позволяет клиентам обращаться к файлам драйвера принтера. Члены групп Administrators, Server Operators (Операторы сервера) и Print Operators (Операторы печати) имеют разрешение Full Control, а группы Everyone (Все) - Read (Чтение).

Перечень скрытых общих папок не ограничивается теми, которые система создает автоматически. Можно открыть доступ к другим папкам, а если добавить ($) в конце их сетевого имени, к ней смогут обратиться только пользователи, знающие имя папки и имеющие разрешение на доступ к ней.

Открытие доступа к папке

Чтобы открыть доступ к папке, выполните следующие действия

1. Войдите в систему с учетной записью, полномочной открывать доступ к папкам.
2. Щелкните правой кнопкой нужную папку и выберите в контекстном меню команду Properties (Свойства).
3. На вкладке Sharing (Доступ) окна свойств задайте нужные параметры.

Параметры вкладки Доступ

Параметр	Описание
Сетевое имя	По этому имени пользователи будут обращаться к данной общей папке. Это обязательный параметр.
Комментарии	Дополнительное описание для сетевого имени, выводится, когда пользователи просматривают общие папки на сервере. Комментарий может быть использован для описания содержимого общей папки.
Предельное число пользователей	Число пользователей, одновременно обращающихся к данной общей папке. Если выбран переключатель Maximum Allowed (максимально возможное), Windows 2000 Professional ограничит доступ к папке десятью соединениями. Windows 2000 Server может предоставить неограниченное количество соединений в зависимости от числа клиентских лицензий доступа
разрешения	Разрешения общей папки, применяемые, только когда к папке подключаются по сети. По умолчанию группе Everyone (Все) назначается разрешение Full Control (Полный доступ) для всех новых общих папок.
кэширование	Параметры доступа в автономном режиме к этой общей папке.

Назначение разрешений доступа к общей папке

Открыв доступ к папке, надо назначить соответствующие разрешения учетным записям пользователей и группам.

1. На вкладке Sharing (Доступ) диалогового окна свойств папки щелкните кнопку Permissions (Разрешения).
2. В диалоговом окне Разрешения проверьте, что выбрана группа (Все), и щелкните кнопку Remove (Удалить).
3. В диалоговом окне Permissions щелкните кнопку Add (Добавить)
4. В диалоговом окне Пользователи, Компьютеры или Группы щелкните учетные записи (группы), которым хотите назначить разрешения.

5. Щелкните кнопку Add (Добавить), чтобы добавить учетные записи (группы) в список доступа к данной папке; повторите это для всех нужных учетных записей (групп).

6. Щелкните ОК.

7. В окне Permissions (Разрешения) для общей папки щелкните учетную запись (группу) и, пометив флажок Allow (Разрешить) или Deny (Запретить), укажите нужное разрешение.

Подключение к общей папке

Подключаться к общей папке можно с помощью команды Run (Выполнить), значка (Мое сетевое окружение) или мастера (Подключение сетевого диска).

Подключение к общей папке посредством команды Run (Выполнить) осуществляется так.

1. В меню Start (Пуск) выберите команду Run и в поле Open (Открыть) введите \\имя_компьютера.

2. Появится список общих папок на этом компьютере. Дважды щелкните подключаемую папку.

Также можно подключать папки с помощью значка (Мое сетевое окружение).

1. Дважды щелкните значок Мое сетевое окружение.

2. Найдите компьютер, на котором находится нужная папка.

3. Дважды щелкните подключаемую папку.

Сочетание разрешений общей папки и разрешений NTFS

На томе FAT обеспечить безопасность общей папки можно, только задав разрешения доступа. В случае диска NTFS пользователям и группам можно назначать разрешения NTFS. При сочетании разрешений доступа к общей папке и разрешений NTFS приоритет имеет более строгое ограничение

Основные методы

Один из способов открыть доступ к ресурсам на томе NTFS — открыть доступ к папке с разрешениями по умолчанию и скорректировать их через разрешения NTFS. При этом разрешения доступа к общей папке и разрешения NTFS комбинируются, обеспечивая нужный уровень безопасности.

Возможности разрешений доступа к общей папке ограничены, разрешения NTFS значительно гибче. Последние применяются как локально, так и при доступе по сети.

При открытии доступа к папке на томе NTFS действуют следующие правила.

o •К файлам и папкам в общей папке можно применять разрешения NTFS, в том числе разные разрешения к разным файлам и папкам.

o Кроме разрешений доступа к общей папке, пользователи должны иметь разрешения NTFS для доступа к ее содержимому. На томах FAT нет других разрешений доступа к содержащимся в общей папке файлам, вложенным папкам, кроме разрешений доступа к самой папке.

o При сочетании разрешений доступа к общей папке и разрешений NTFS приоритет всегда имеет более строгое ограничение.

Практическое задание

1. Назначение разрешений

Упражнение 1: назначение разрешений для групп пользователей

1. User101 — член групп Group1, Group2 и Group3. Для папки ПапкаA у Group1 есть разрешение Read (Чтение), у Group3 — Full Control (Полный доступ), а для Group2 разрешений не назначено. Какими результирующими разрешениями будет обладать User101 для ПапкиA?

2. User101 также является членом группы Sales, которой назначено разрешение Read для ПапкаB. Для User101 как отдельного пользователя, отменено разрешение Full Control для ПапкаB. Какие результирующие разрешения будет иметь User101 для ПапкаB?

2. управление доступом к общим папкам

Определите результирующие разрешения пользователей, спланируйте совместное использование папок и разрешений доступа к ним, назначьте разрешения доступа к папке, подключитесь к ней, закройте к ней доступ и проверьте эффекты от сочетания разрешений доступа к общей папке и разрешений NTFS.

Упражнение 1: сочетание разрешений

Общие папки на томе NTFS содержат вложенные папки, которым назначены разрешения NTFS(см задания к упражнению). Определите результирующие разрешения пользователей в каждом случае.

Задание 1: определите результирующие разрешения пользователей

1. Открыт доступ к папке Data. Группа Sales имеет для нее разрешение read (Чтение), а для вложенной в нее папки Sales — NTFS-разрешение Full Control (Полный доступ).

Каким будет результирующее разрешение группы Sales для доступа к папке Sales при подключении по сети к папке Data?

2. Папка Users (Пользователи) содержит личные папки пользователей. Каждая личная папка содержит данные, доступные только пользователю, именем которого она названа. Папка Users доступна группе Users с разрешением Full Control (Полный доступ). Userl и User2 имеют разрешения NTFS Full Control только для своих личных папок: никаких разрешений NTFS для остальных. Эти пользователи — члены группы Users.

Какими разрешениями доступа к папке Userl будет обладать Userl при подключении к общей папке Users? Какими будут его разрешения для папки User2?

Упражнение 2: планирование общих папок

Спланируйте доступ к ресурсам на серверах главного офиса предприятия •(см задание к упражнению). Выполнив упражнение, занесите ваши решения в таблицу.

Сделайте ресурсы на этих серверах доступными пользователям ЛВС компании, определив, к каким папкам открыть доступ и какие разрешения назначить группам, в том числе встроенным.

Ваши решения должны удовлетворять следующим критериям:

Членам группы Managers надо читать и вносить исправления в документы в папке Management. Больше никто не должен иметь доступ к этой папке.

- Администраторы должны иметь полный доступ ко всем общим папкам, кроме папки Management.
- Отделу по работе с клиентами требуется отдельное место в сети для хранения рабочих файлов. Все сотрудники этого отдела — члены группы Customer Service.
- Всем сотрудникам компании требуется место в сети для обмена информацией.
- Всем сотрудникам нужны такие приложения, как электронные таблиц и текстовые процессоры.
- Только члены группы Managers должны иметь доступ к ПО управления проектами предприятия.
- Члены группы CustomerDBFull должны читать и вносить информацию в БД клиентов.
- Члены группы CustomerDBRead должны только читать информацию из БД клиентов.

Каждый пользователь сети должен иметь собственное место в сети для хранения файлов, доступное только ему.

Имена общих ресурсов должны быть доступны с компьютеров Windows 2000/NT/98/95, а также с альтернативных платформ.

Запишите свои ответы в следующую таблицу.

Имя папки	Общее имя	Группы и разрешения
Например: Management	Mgmt	Managers: Полный доступ

Упражнение 3: открытие доступа к папкам

Задание 1: откройте доступ к папке

1. Зарегистрируйтесь как (Администратор).
2. Запустите (Проводник), создайте папку C:\Dostup щелкните ее правой кнопкой и выберите в контекстном меню команду (Свойства).
3. В диалоговом окне свойств папки Dostup перейдите на вкладку (Доступ).
4. Щелкните переключатель Share This Folder (Открыть общий доступ к этой папке), щелкните ОК.

Windows Explorer изменил значок папки Dostup, добавив снизу изображение руки, значит, папка стала общей.

Упражнение 4: назначение разрешений доступа к общей папке

Определите текущие разрешения доступа к общей папке и назначьте разрешения группам в вашем домене.

Задание 1: определите текущие разрешения для общей папки Dostup

1. В окне Проводник щелкните правой кнопкой мыши папку C:\Dostup и выберите в контекстном меню команду Свойства.
2. Перейдите на вкладку Доступ и щелкните кнопку Permissions (Разрешения).

По умолчанию группе Everyone (Все) для этой папки назначено разрешение (Полный доступ).

Задание 2: аннулируйте разрешения для группы

1. Убедитесь, что выбрана группа Everyone
2. Щелкните кнопку Remove (Удалить).

Задание 3: назначьте разрешение Full Control группе Administrators

1. Щелкните кнопку Add (Добавить). Откроется диалоговое окно (Выбор: Пользователи, Компьютеры или Группы).
2. Убедитесь, что имя вашего компьютера (Comp1) выведено в поле (Искать в). В поле Name (Имя) щелкните Administrators (Администраторы), а затем — кнопку Add.

Группа Administrators добавится в список групп, имеющих разрешения.

Какой вид доступа будет назначен этой группе по умолчанию?

3. В столбце Allow (Разрешить) окна Permissions (Разрешения) пометьте флажок Full Control.

Почему также включилось разрешение Change (Изменение)?

4. Щелкните ОК, чтобы закрыть окно Разрешение для папки Dostup.
5. Щелкните ОК, чтобы закрыть окно свойств папки Dostup.
6. Закройте (Проводник).

Упражнение 5: прекращение совместного использования папки

Закройте доступ к папке.

Задание 1: закройте доступ к папке

1. Войдите в систему на Comp1 как администратор и запустите Проводник.
2. Щелкните правой кнопкой папку C:\Dostup и выберите в контекстном меню команду (Свойства).
3. В диалоговом окне свойств папки перейдите на вкладку (Доступ).

Щелкните переключатель (Не открывать общий доступ к этой папке), затем — ОК.

Под Dostup больше нет «руки», означавшей, что папка была общей. Возможно, вам сначала понадобится обновить экран — в этом случае нажмите клавишу F5.

4. Закройте (Проводник).

Упражнение 6: назначение разрешений NTFS и открытие доступа к папкам

Назначьте разрешения NTFS папкам Dostup, Public и Manuals и откройте к ним доступ.

Чтобы назначить разрешения NTFS, создайте с помощью Проводника папки и назначьте им разрешения NTFS согласно таблице. Не допускайте наследования разрешений для вложенных объектов и снимите все ранее существовавшие разрешения NTFS.

Папки переданы в совместное пользование, назначены разрешения доступа к ним. Откройте доступ к папкам и назначьте разрешения пользователям сети согласно таблице. Снимите все остальные разрешения сетевого доступа.

Путь	Группа	Разрешения NTFS
C:\Dostup	Администраторы Users(Пользователи)	Полный доступ Чтение и выполнение
C:\Dostup\ Manuals	Администраторы Users	Полный доступ Чтение и выполнение
C:\Dostup\ Public	Администраторы Users	Полный доступ Полный доступ

Отчет

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

Контрольные вопросы

1. Общая папка расположена на томе FAT, и пользователь имеет для нее разрешение Full Control (Полный доступ). К каким объектам в папке он получит доступ?
2. Перечислите разрешения доступа к общей папке.
3. Какие разрешения назначаются общей папке по умолчанию?
4. Общая папка расположена на томе NTFS, и пользователь имеет для нее разрешение Full Control. К каким объектам в этой папке получит доступ пользователь?
5. Почему рекомендуется централизованно хранить общие папки данных?
6. Как лучше обеспечить безопасность общих файлов и папок на NTFS?

Практическая работа 18. Наследование разрешений в NTFS.

Цель работы Определить параметры наследования разрешений NTFS.
Оборудование: учебный персональный компьютер.

Теоретические основы

Разрешения NTFS позволяют явно указать, какие пользователи и группы имеют доступ к файлам и папкам и какие операции с содержимым этих файлов или папок им разрешено выполнять. Разрешения NTFS применимы только к томам, отформатированным с использованием файловой системы NTFS. Они не предусмотрены для томов, использующих файловые системы FAT или FAT32. Система безопасности NTFS эффективна независимо от того, обращается ли пользователь к файлу или папке, размещенным на локальном компьютере или в сети.

Разрешения, устанавливаемые для папок, отличаются от разрешений, устанавливаемых для файлов. Администраторы, владельцы файлов или папок и пользователи с разрешением «Полный доступ» имеют право назначать разрешения NTFS пользователям и группам для управления доступом к этим файлам и папкам. **Список управления доступом**

В NTFS хранится ***список управления доступом*** (access control list —**ACL)** для каждого файла и папки на томе NTFS. В этом списке перечислены пользователи и группы, для которых установлены разрешения для файла или папки, а также сами назначенные разрешения. Чтобы пользователь получил доступ к ресурсу, в ACL должна быть запись, называемая ***элемент списка управления доступом*** (access control entry — ACE) для этого пользователя или группы, к которой он принадлежит. Эта запись назначит запрашиваемый тип доступа (например, **Чтение)** пользователю. Если в ACL нет соответствующей ACE, то пользователь не получит доступ к ресурсу.

Множественные разрешения NTFS

Вы можете установить несколько разрешений пользователю и всем группам, членом которых он является. Для этого вы должны иметь представление о правилах и приоритетах, по которым в NTFS назначаются и объединяются множественные разрешения и о наследовании разрешений NTFS.

Эффективные разрешения. Эффективные разрешения пользователя для ресурса — это совокупность разрешений NTFS, которые вы назначаете отдельному пользователю и всем группам, к которым он принадлежит. Если у пользователя есть разрешение «Чтение» для папки, и он входит в группу, у которой есть разрешение «Запись» для той же папки, значит, у этого пользователя есть оба разрешения.

Установка разрешений NTFS и особых разрешений

Вы должны руководствоваться определенными принципами при установке разрешений NTFS. Устанавливайте разрешения согласно потребностям групп и пользователей, что включает

в себя разрешение или предотвращение наследования разрешений родительской папки подпапками и файлами, содержащимися в родительской папке.

Если вы уделите немного времени на планирование ваших разрешений NTFS и будете соблюдать при планировании несколько принципов, то обнаружите, что разрешениями легко управлять.

• Для упрощения процесса администрирования сгруппируйте файлы по папкам следующих типов: папки с приложениями, папки с данными, личные папки. Централизуйте общедоступные и личные папки на отдельном томе, не содержащем файлов операционной системы и других приложений. Действуя таким образом, вы получите следующие преимущества:

— сможете устанавливать разрешения только папкам, а не отдельным файлам;

— упростите процесс резервного копирования, так как вам не придется делать резервные копии файлов приложений, а все общедоступные и личные папки находятся в одном месте.

- Устанавливайте для пользователей только необходимый уровень доступа. Если необходимо чтение файла, установите пользователю разрешение Чтение для этого файла. Это уменьшит вероятность случайного изменения файла или удаления важных документов и файлов приложений пользователем.
- Создавайте группы согласно необходимому членам группы типу доступа, затем установите соответствующие разрешения для группы. Назначайте разрешения отдельным пользователям только в тех случаях, когда это необходимо.
- При установке разрешений для работы с данными или файлами приложений установите разрешение Чтение и выполнение для групп Пользо**ватели** и Администраторы. Это предотвратит случайное удаление файлов приложений или их повреждение вирусами или пользователями.
- При установке разрешений для папок с общими данными назначьте разрешения Чтение и выполнение и Запись группе Пользователи и разрешение Полный доступ для группы Создатель-владелец. По умолчанию пользователь, создавший документ, также является его владельцем. Владелец файла может дать другому пользователю разрешение на владение файлом. Пользователь, который принимает такие права, в этом случае становится владельцем файла. Если вы установите разрешение Чтение и выполнение и Запись группе Пользователи и разрешение Полный доступ группе Создатель-владелец, то пользователи получат возможность читать и изменять документы, созданные другими пользователями, а также читать, изменять и удалять файлы и папки, создаваемые ими.
- Запрещайте разрешения, только если необходимо запретить отдельный тип доступа определенному пользователю или группе.
- Поощряйте пользователей в установке разрешений для файлов и папок, которые они создают, и научите их это делать самостоятельно.

Администраторы, пользователи с разрешением Полный доступ и владельцы файлов и папок могут устанавливать разрешения для отдельных пользователей и групп.

Дополнительно Позволяет получить доступ к дополнительным возможностям поиска, включая возможность поиска удаленных учетных записей пользователей, учетных записей с неустаревшими паролями и учетных записей, по которым не подключались определенное количество дней.

Назначение или запрещение особых разрешений

Щелкните кнопку **Дополнительно,** чтобы открыть диалоговое окно **Дополнительные параметры безопасности,** где перечислены группы и пользователи и установленные для них разрешения для этого объекта. В поле **Элементы разрешений** также указано, от какого объекта разрешения унаследованы и к каким объектам применимы. Вы можете воспользоваться диалоговым окном **Дополнительные параметры безопасности** для изменения разрешений, установленных для пользователя или группы. Для изменения разрешений, установленных для пользователя или группы, выделите пользователя и щелкните кнопку **Изменить.** Откроется диалоговое окно **Элемент разрешения для.** Затем выделите или отмените определенные разрешения, которые вы хотите изменить.

Практическая работа.

1. Загрузить виртуальную машину Windows и создать новую учетную запись uir.

2. Загрузить виртуальную машину Windows с учетной записью uir.
3. Определение разрешений NTFS по умолчанию для только что созданной папки.
4. Запустить **Проводник,** создать папки **C:\FoIderl** и **C:\FoIderl\Folder2.** Просмотреть разрешения, установленные для созданных папок, щелкнув по вкладке **Безопасность** диалогового окна свойств папки. Обратить внимание на наследование разрешений папкой **Folder2** от родительской папки **Folder 1.**
5. Если на экране не видна вкладка **Безопасность,** вам следует уточнить два вопроса:
   1) Раздел вашего диска отформатирован как NTFS или как FAT? Только на разделах NTFS используются разрешения NTFS, и, таким образом, только на разделах NTFS видна вкладка **Безопасность.**
   2) Используете вы простой общий доступ к файлам или нет? Щелкните кнопку **Отмена,** чтобы закрыть диалоговое окно свойств папки. **В** пункте меню **Сервис** выберите пункт **Свойства папки.** В диалоговом окне **Свойства папки** перейдите на вкладку **Вид.** В списке **Дополнительные параметры** снимите флажок **Использовать простой общий доступ к файлам (рекомендуется)** и щелкните **ОК.**
6. Определить для какой группы установлены особые разрешения. Щелкнуть кнопку **Дополнительно,** выделить эту группу и просмотреть установленные разрешения.
7. Закрыть диалоговое окно свойств папки. Закрыть окно **Проводник** и завершить сеанс.

Отчет

Отчет должен содержать:
1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

Контрольные вопросы

1. Что такое эффективные разрешения пользователя для ресурса?
2. Какие объекты по умолчанию наследуют разрешения, установленные для родительской папки?
3. Чем отличается разрешение «Удаление» от разрешения «Удаление подпапок и файлов»?
4. Какое разрешение NTFS для файлов следует установить для файла, если вы позволяете пользователям удалять файл, но не позволяете становиться владельцами файла?
5. Если вы хотите, чтобы пользователь или группа не имела доступ к определенной папке или файлу, следует ли запретить разрешения для этой папки или файла?

Практическая работа 19. Изменение параметров учетных записей пользователей.

Цель работы: освоение средств администратора операционной системы MS Windows.

Оборудование: учебный персональный компьютер.

Теоретические основы

Идентификацию и аутентификацию можно считать основой программно-технических средств безопасности, поскольку остальные сервисы рассчитаны на обслуживание именованных субъектов. Идентификация и аутентификация – это первая линия обороны, "проходная" информационного пространства организации.

Идентификация позволяет субъекту назвать себя (сообщить свое имя). Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. В качестве синонима слова "аутентификация" иногда используют словосочетание "проверка подлинности".

Идентификация — присвоение субъектам и объектам идентификатора и / или сравнение идентификатора с перечнем присвоенных идентификаторов.

Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной). Пример односторонней аутентификации – процедура входа пользователя в систему.

Аутентификация — проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

В сетевой среде, когда стороны идентификации/аутентификации территориально разнесены, у рассматриваемого сервиса есть два основных аспекта:

• что служит аутентификатором (то есть используется для подтверждения подлинности субъекта);

• как организован (и защищен) обмен данными идентификации/аутентификации.

Субъект может подтвердить свою подлинность, предъявив по крайней мере одну из следующих сущностей:

• нечто, что он знает (пароль, личный идентификационный номер, криптографический ключ и т.п.);

• нечто, чем он владеет (личную карточку или иное устройство аналогичного назначения);

• нечто, что есть часть его самого (голос, отпечатки пальцев, то есть свои биометрические характеристики).

Современные средства идентификации/аутентификации должны поддерживать концепцию единого входа в сеть. Единый вход в сеть – это, в первую очередь, требование удобства для пользователей. Если в корпоративной сети много информационных сервисов, допускающих независимое обращение, то многократная идентификация/аутентификация становится слишком обременительной. К сожалению, пока нельзя сказать, что единый вход в сеть стал нормой, доминирующие решения пока не сформировались.

Таким образом, необходимо искать компромисс между надежностью, доступностью по цене и удобством использования и администрирования средств идентификации и аутентификации.

Скрыть объявление

Нужно отметить, что сервис идентификации / аутентификации может стать объектом атак на доступность. Если система сконфигурирована так, что после определенного числа неудачных попыток устройство ввода идентификационной информации (такое, например, как терминал) блокируется, то злоумышленник может остановить работу легального пользователя буквально несколькими нажатиями клавиш.

Задания для выполнения

1. Освоить средства регистрации пользователей:

• открыть список зарегистрированных пользователей (Панель управления | Администрирование | Управление компьютером | Локальные пользователи и группы | Пользователи);

• с помощью команды контекстного меню (Новый пользователь) создать для себя учетную запись с произвольным логическим именем, введя в качестве строки описания текст «Студент группы XY-Z»);

включить в отчет о лабораторной работе

a) копию экранной формы создания новой учетной записи,

b) копию экранной формы со списком зарегистрированных пользователей,

c) список команд контекстного меню (при отсутствии выделения имени пользователя в списке),

d) а также объяснения смысла четырех дополнительных параметров создаваемой учетной записи;

• выделить имя вновь зарегистрированного пользователя и с помощью команды контекстного меню (Свойства) просмотреть ее свойства;

• включить в отчет о лабораторной работе копию экранной формы со свойствами учетной записи на вкладке «Общие» и объяснение разницы между отключением и блокировкой учетной записи (см. справочный материал – кнопка «Справка» окна свойств пользователя);

• включить в отчет о лабораторной работе копию экранной формы со свойствами учетной записи на вкладке «Членство в группах» и ответ на вопрос, в какую группу по умолчанию включается вновь созданный пользователь

• с помощью кнопок «Добавить», «Дополнительно» и «Поиск» включить вновь созданного пользователя также в группу «Опытные пользователи»;

• выбрать имя созданного пользователя, в контекстном меню выбрать пункт «Задать пароль» и изменить текущий пароль этого пользователя.

• включить в отчет о лабораторной работе список команд контекстного меню при выбранном имени учетной записи вместе с пояснениями их смысла, а также ответы на вопросы:

a) когда должна применяться команда «Задать пароль»,

b) в чем опасность ее применения,

c) как должна происходить смена пароля пользователем

2. Освоить средства работы с группами:

• открыть список групп (Панель управления | Администрирование | Управление компьютером | Локальные пользователи и группы | Группы)

• включить в отчет сведения об автоматически создаваемых группах пользователей, их именах и характеристиках прав их членов;

• создать новую группу в системе с именем «Начинающие пользователи» и включить в отчет о лабораторной работе копию используемого при этом экрана и сведения о порядке создания в системе новых групп пользователей, а также ответ на вопрос, в чем целесообразность разбиения множества пользователей на группы;

3. Освоить порядок назначения прав пользователям:

• открыть окно настройки прав пользователей (Панель управления | Администрирование | Локальная политика безопасности | Локальные политики | Назначение прав пользователя);

• исключить группу пользователей «Все» из числа групп, обладающих правом «Доступ к компьютеру из сети»;

• исключить пользователя «Гость» из числа пользователей, обладающих правом «Локальный вход в систему»;

• добавить группу «Начинающие пользователи» к списку пользователей, обладающих правом «Локальный вход в систему»;

• включить в отчет о лабораторной работе копии экранов, используемых при назначении прав пользователям, и сведения о порядке выполнения этих действий;

• с помощью раздела справки Windows «Назначение прав пользователя» включить в отчет о лабораторной работе пояснения отдельных привилегий пользователей системы. Обязательно ответить на вопрос, почему использование данного права должно быть ограничено.

4. Освоить определение параметров политики безопасности, относящихся к аутентификации и авторизации пользователей при интерактивном входе:

• открыть окно определения параметров безопасности для паролей (Панель управления | Администрирование | Локальная политика безопасности | Политики учетных записей | Политика паролей);

• включить в отчет о лабораторной работе сведения о порядке назначения максимального и минимального сроков действия паролей и ответ на вопрос о смысле подобных ограничений;

• включить в отчет о лабораторной работе сведения о порядке назначения минимальной длины и ограничений на сложность паролей, а также ответы на вопросы, какие и почему требования по сложности предъявляются к паролям в операционной системе Windows (с помощью справочной подсистемы);

• включить в отчет о лабораторной работе сведения о назначении параметров «Требовать неповторяемости паролей» и «Хранить пароли всех пользователей в домене, используя обратимое шифрование» (с помощью справки Windows);

• включить в отчет о лабораторной работе копии экранных форм, используемых при определении параметров политики безопасности, относящихся к паролям;

• открыть окно определения параметров безопасности для политики блокировки учетных записей (Панель управления | Администрирование | Локальная политика безопасности | Политики учетных записей | Политика блокировки учетных записей);

Отчет

Отчет должен содержать:
1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

Контрольные вопросы

1. Кому может быть разрешен доступ по чтению и по записи к базе учетных записей пользователей?
2. Как должны храниться пароли в базе учетных записей пользователей?
3. В чем смысл объединения пользователей в группы?

Практическая работа 20. Настройка политики учетных записей.

Цель работы: настроить политику учётных записей и минимальную длину пароля для пользователя.

Оборудование: учебный персональный компьютер.

Теоретические основы

Настройка политики паролей

Политика паролей позволяет повысить безопасность системы путем упорядочения процесса создания и обновления паролей. Вы можете задать периодичность изменения пароля. Смена пароля снижает вероятность несанкционированного доступа к системе. Даже если злоумышленник узнает имя и пароль учетной записи пользователя, после очередной обязательной смены пароля он не сможет войти в систему.

Кроме этого можно задать минимальную длину пароля. Чем длиннее пароль, тем сложнее его подобрать. Еще один метод — ведение истории паролей. Если его применить, пользователь не сможет завести себе два пароля и вводить их попеременно.

Для настройки политики паролей на компьютере с Windows служат оснастки Group Policy (Групповая политика) и Local Security Policy (Локальная политика безопасности). Для настройки политики паролей в консоли Групповые политики необходимо:

1. Создать в MMC (Microsoft Management Console) дополнительную оснастку Group Policy.
2. Последовательно развернуть папки Local Computer Policy (Локальная политика безопасности), Computer Configuration (Управление компьютером), Windows Settings (Параметры Windows), Security Settings (Параметры безопасности), Account Policies (Политики учетных записей), а затем щелкнуть Password Policy (Политика паролей).
3. Выбрать параметры, которые необходимо задать, и затем в меню Action (Действие) щелкнуть Security (Безопасность).

В правой области окна показаны текущие значения параметров политики паролей.

Параметр	Описание
Enforce Password History (Включить ведение истории паролей)	Задает число паролей, хранимых в истории, и принимает значения в диапазоне от 0 до 24. Значение 0 (по умолчанию) указывает, что ведение истории паролей отключено. Значения, отличные от 0, указывают, сколько новых паролей должен выбрать пользователь, прежде чем повторно использовать старый.
Maximum Password Age (Максимальный срок Действия пароля)	Указывает, сколько дней можно пользоваться паролем, не меняя его. Значение этого параметра по умолчанию — 42, а диапазон допустимых значений — от 0 до 999. 0 указывает, что пароль менять не обязательно.

Minimum Password Age (Минимальный срок Действия пароля)	Указывает, сколько дней пользователь может вводить пароль, прежде чем получит право снова его сменить. Это нужно для того, чтобы после обновления пароля пользователь не мог тут же заменить его старым. Диапазон допустимых значений — от 0 до 999. Значение 0 (по умолчанию) указывает, что пароль можно сменить немедленно. Если история паролей не ведется, задавать значение 0 нельзя. Минимальный срок действия пароля должен быть меньше максимального срока действия.
Minimum Password Length (Минимальная длина пароля)	Задает минимальное количество знаков в пароле. Допустимые значения — от 0 до 14 включительно. Значение 0 (по умолчанию) указывает, что пароль не требуется.
Passwords Must Meet Complexity Requirements (Пароли должны отвечать требованиям сложности)	Принимает одно из двух значений: включен (по умолчанию) или отключен. Если параметр включен, длина пароля должна быть равна или больше минимальной длины, а сам пароль — соответствовать конфигурации истории паролей и состоять из заглавных букв, цифр или знаков пунктуации. Кроме того, пароль не может содержать имен учетной записи и пользователя.
Store Password Using Reversible Encryption For All Users In The Domain (Хранить пароли всех пользователей в домене, используя обратимое шифрование	Принимает одно из двух значений: включен или отключен (по умолчанию). Хранение паролей с применением обратимого шифрования для всех пользователей домена позволяет Windows использовать их, например в протоколе CHAP (Challenge Handshake Authentication Protocol), обратимое шифрование) Возможность существует только на компьютерах с Windows Professional, включенных в состав домена.

Для выбранного параметра откроется диалоговое окно Local Security Policy Setting (Параметры локальной политики безопасности).

Настройка политики блокировки учетных записей

Повысить безопасность системы позволяет также политика блокировки учетных записей, которая закрывает пользователю доступ к учетной записи при наступлении определенных условий.

Эту политику можно настраивать из оснастки Групповая политика, либо в окне Local Security Policy Settings — как при настройке политики паролей.

Параметр	Описание
Account Lockout Duration (Продолжительность блокировки учетной записи)	Указывает, сколько минут учетная запись будет блокирована. Если значение равно 0, учетная запись пользователя будет блокирована в течение неопределенного времени, пока администратор не разблокирует ее. Допустимые значения — от 0 до 99999 мин. (максимальной значение, равное 99999 мин., что составляет примерно 69,4 дня).
Account Lockout Threshold (Максимальное число неудачных попыток)	Количество неудачных попыток, по достижении которого все дальнейшие попытки будут отклоняться. Значение 0 отключает механизм блокировки, то есть учетная запись никогда не блокируется, независимо от числа неудачных попыток войти в систему.

Reset Account Lockout Counter After (Частота сброса счетчика неудачных попыток)	Задает срок (в мин.), по истечении которого сбрасывается счетчик неудачных попыток. Допустимые значения — от 1 до 99999.

Настройка параметров безопасности

1. **Выключение компьютера, не требующее входа в систему**

По умолчанию в Windows Professional, чтобы выключить компьютер пользователю не обязательно входить в систему. Впрочем, параметры регистрации позволяют отменить такое поведение и потребовать, чтобы пользователи вошли в систему перед тем, как выключить компьютер. Получить доступ к параметрам безопасности можно в оснастке Group Policy (Групповая политика), так же как при настройке параметров политики учетных записей. Открыв оснастку Group Policy, последовательно раскройте узлы (Политика локальной безопасности), затем Computer Configuration (Параметры компьютера), Windows Settings (Параметры Windows), Security Settings (Параметры безопасности), Local Policies (Локальные политики), а затем Security Options (Параметры безопасности).

2. **Очистка страничного файла виртуальной памяти при выключении системы.**

По умолчанию при выключении системы Windows Professional не очищает страничный файл виртуальной памяти. В некоторых организациях это рассматривается как нарушение правил безопасности, поскольку доступ к данным этого файла могут получить пользователи, не допущенные к ним. Чтобы отключить эту возможность, откройте оснастку Group Policy (Групповая политика), последовательно раскройте узлы Local Computer Policy (Локальная политика безопасности), затем Computer Configuration (Параметры компьютера), Windows Settings (Параметры Windows), Security Settings (Параметры безопасности), Local Policies (Локальная политика), а затем Security Option (Параметры безопасности). Правой кнопкой мыши щелкните Clear Virtual Memory Pagefile When System Shuts Down (Очистка страничного файла виртуальной памяти при завершении работы) и в контекстном меню выберите Security (Безопасность). Этот параметр может быть либо включен, либо отключен.

3. **Регулирование нажатия клавиш CTRL+ALT+DEL для входа в систему**

По умолчанию Windows Professional не требует, чтобы пользователи нажимали Ctrl+Alt+Del для входа в систему. Повысить безопасность системы можно, изменив такое поведение. Нажатие Ctrl+Alt+Del — сочетания клавиш, которое распознается только Windows, гарантирует, пароль попадет именно в систему Windows, а не в троянскую программу, которая может перехватить пароль. Изменить поведение системы можно в оснастке Group Policy (Групповая политика). Лучше всего отключить необязательность нажатия Ctrl+Alt+Del, чтобы при входе в систему пользователи всегда нажимали это сочетание клавиш.

4. **Скрытие имени последнего успешно вошедшего в систему пользователя**

По умолчанию Windows Professional отображает имя последнего вошедшего в систему пользователя в диалоговом окне Windows Security (Безопасность Windows) или Log On To Windows (Вход в Windows). Это может создать угрозу безопасности, так как имя учетной записи становится доступным постороннему пользователю, при этом несанкционированно проникновение в систему существенно облегчается.

Чтобы включить эту функцию и предотвратить отображение пользователя, в оснастке Group Policy последовательно раскройте узлы (Локальная политика безопасности), затем Computer Configuration (Параметры компьютера), Windows Settings (Параметры Windows), Security Settings (Параметры безопасности), Local Policies (Локальная политика), а затем Security Options (Параметры безопасности). В правой области окна щелкните правой кнопкой Do Not Display Last User Name In Logon Screen (*Не отображать последнего имени пользователя в диалоге входа*) и в контекстном меню выберите Security (*Безопасность*), а затем отключите эту функцию.

Практическая часть:

1. Настройте политику учетных записей на компьютере и убедитесь, что: данные параметры вступили в силу.
2. Настройте минимальную длину пароля, а затем поэкспериментируйте с длиной пароля, чтобы убедиться, что выбранные параметры вступили в силу.

Задание 1: настройка минимальной длины пароля

1. Войдите в систему под учетной записью Administrator (Администратор)
2. В консоли MMC создайте дополнительную консоль с оснасткой Group Policy (Групповая политика).
3. Открыв консоль Group Policy, последовательно щелкните узлы: (Локальная политика безопасности), (Параметры компьютера), Windows Settings (ПараметрыWindows), Security Settings (Параметры безопасности) и (Политики учетных записей).
4. В дереве консоли щелкните Password Policy (Политика паролей).
5. В правой панели щелкните правой кнопкой мыши Minimum Password Length (Минимальная длина пароля) и выберите в контекстном меню Security (Безопасность).
6. В поле Characters (Длина пароля) **введите 6** и щелкните ОК.
7. Закройте окно Local Security Settings (Параметры локальной безопасности).

Задание 2: проверьте, изменилась ли минимальная длина пароля

1. Нажмите Ctrl+Alt+Delete, а затем в диалоговом окне Windows Security (Безопасность Windows) щелкните Change Password (Изменить пароль).
2. В поле Old Password (Старый пароль) введите password, а в поля New Password (Новый пароль) и Confirm Password (Подтверждение) введите **water.**

Информационное окно Change Password (Изменение пароля) сообщит, что новый пароль должен содержать не менее шести символов. Таким образом, параметр Minimum Password Length настроен верно.

Задание 3: Настройте отдельные параметры политики учетных записей, а затем проверьте правильность настройки.

1. С помощью оснастки Group Policy (Групповая политика) задайте параметры политики учетных записей:
   - пользователь должен сменить минимум пять паролей, прежде чем повторно применить старый;
   - после обновления пароля пользователь может его снова сменить не ранее, чем через 24 часа;
   - пользователь должен менять пароль каждые три недели.

Какие параметры вам понадобились, чтобы выполнить требования этого списка?

2. Закройте оснастку Group Policy.

Задание 4: убедитесь, что новые параметры политики учетных записей работают

1. Войдите в систему под именем User4 и паролем User4. Примечание: Если диалоговое окно Logon Message (Сообщение системы) сообщит об отмене пароля через определенный промежуток времени и предложит сменить пароль, щелкните No (Нет).
2. Измените пароль на waters. Получилось ли это? Объясните почему? Измените пароль на papers. Получилось ли это? Объясните почему? Закройте все окна и выйдите из системы.

Задание 5: Настройте параметры политики блокировки учетных записей и убедитесь, что изменения вступили в силу.

1. Войдите в систему под учетной записью Administrator (Администратор).
2. Раскройте меню Пуск\Программы\Администрирование, а затем щелкните Group Policy (Групповая политика).
3. В дереве консоли Group Policy последовательно раскройте узлы: (Локальная политика безопасности), (Управление компьютером), Windows Settings (Параметры Windows), Security Settings (Параметры безопасности), а затем Policies (Политики учетных записей).
4. Щелкните Account Lockout Policy (Политика блокировки учетных записей).
5. Настройте параметры Account Lockout Policy так, чтобы: учетная запись пользователя блокировалась после четырех неудачных попыток войти в систему;
6. разблокировать учетную запись мог только администратор.
7. Выйдите из системы.

Задание 6: проверьте вступление в силу новых параметров политики блокировки учетных записей

1. Четыре раза попробуйте войти в систему как User4 с паролем **papers.** Информационное окно сообщит о блокировке учетной записи.
2. Щелкните ОК и войдите, в систему под учетной записью администратора.

Задание 7: настройте и проверьте параметры безопасности

1. Войдите в систему по учетной записи Administrator (Администратор).
2. Раскройте меню Пуск\Программы\Администрирование и щелкните Group Policy (Групповая политика).
3. В дереве консоли Group Policy по мере необходимости, последовательно раскройте узлы Local Computer Policy\Computer Configuration\Windows Settings\Security Settings (Локальная политика безопасности\ Параметры компьютера\ Параметры Windows\ параметры безопасности),а затем — Account Policies (Политики учетных записей).
4. Настройте политику безопасности на компьютере так, чтобы пользователи:
   - должны были входить в систему, чтобы иметь возможность выключить компьютер;
   - должны были нажимать Ctrl+Alt+Delete для входа в систему;
   - не смогли увидеть в окне Windows Security имя последнего пользователя.
5. Выйдите из системы.
6. Обратите внимание, что теперь для регистрации нужно нажать Ctrl+Alt+Delete.
7. Нажмите Ctrl+Alt+Delete.
8. В диалоговом окне Log On To Windows (Вход в Windows) поле User Name (Пользователь) пустое и кнопка Shutdown (Выключить) неактивна. Если вы не видите кнопку Shutdown, щелкните Options (Параметры).

Отчет

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

Контрольные вопросы

1. Зачем заставлять пользователей менять пароль?
2. Зачем проверять длину паролей?
3. Для чего нужна блокировка учетных записей?
4. Почему желательно требовать, чтобы пользователи нажимали, Ctrl+Alt+Delete перед входом в систему?
5. Как предотвратить отображение имени последнего пользователя в диалоговых окнах Windows Security (Безопасность Windows) и Log On To Windows (Вход в Windows)?

Практическая работа 21. Настройка параметров безопасности операционных систем.

Цель работы установить в BIOS Setup параметры, обеспечивающие безопасность системы.

Оборудование: учебный персональный компьютер.

Теоретические основы

BIOS. После включения компьютера процессор начинает считывать и выполнять микропрограммы, которые хранятся в микросхеме BIOS (Basic Input/Output System – базовая система ввода/вывода). Прежде всего начинает выполняться программа тестирования POST (Power On Self Test), которая проверяет работоспособность основных устройств компьютера: процессора, видеоадаптера, оперативной памяти, последовательных и параллельного портов, дисководов, контроллеров жестких дисков и клавиатуры.

В случае обнаружения неисправностей выдаются последовательности коротких и длинных звуковых сигналов, а после инициализации видеоадаптера процесс тестирования отображается на экране монитора.

Практическое задание 1.3. «BIOS и загрузка операционной системы». Включить компьютер и наблюдать процесс загрузки операционной системы. С помощью программы BIOS Setup произвести установку новых параметров конфигурации компьютера.

В некоторых случаях появление сообщения об ошибке связано с забывчивостью пользователя. Например, в случае появления сообщения *Invalid Boot Diskette* (Невозможно загрузить операционную систему с дискеты) для продолжения загрузки необходимо просто извлечь несистемную дискету из дисковода.

В процессе тестирования BIOS сравнивает получаемые данные о конфигурации компьютера с информацией, хранящейся в CMOS – специальной микросхеме памяти, расположенном на системной плате. Если данные не совпадают, то появляется сообщение CMOS *System Option Not Set*. В этом случае необходимо с помощью утилиты BIOS Setup установить новые конфигурационные параметры.

Для правильной установки даты, времени и параметров жестких и гибких дисков необходимо использовать панель *STANDARD CMOS SETUP* (Стандартная установка).

С помощью панели *BIOS FEATURES SETUP* (Полная установка) можно установить защиту от заражения вирусом загрузочного сектора системного диска. Будет заблокировано любое изменение загрузочного сектора и, поэтому, при переустановке или установке операционной системы защиту необходимо снимать.

Для предохранения данных от несанкционированного доступа можно с помощью BIOS Setup установить пароль для входа в систему или в установку конфигурационных параметров. Обязательно хорошо запомните или запишите пароль, т.к. в случае его утери вход в систему становится невозможным (сброс пароля возможен только аппаратно, путем отключения микросхемы CMOS от источника питания – аккумулятора).

Загрузка операционной системы. После того как POST-тестирование успешно завершается, BIOS приступает к поиску программы-загрузчика Master Boot операционной системы. Современные версии BIOS позволяют загружать операционную систему не только с гибких и жестких дисков, но и с дисководов CD-ROM, ZIP и LS-120. Если программа-загрузчик найдена, она помещается в оперативную память, и начинает процесс загрузки файлов операционной системы.

Системная конфигурация и загрузка драйверов устройств производится путем последовательной обработки конфигурационных файлов. Сначала обрабатываются файлы config.sys и autoexec.bat, оставшиеся в операционной системе Window 95/98 от MS-DOS. Затем обрабатываются файлы system.ini и win.ini, которые остались от операционной системы Windows 3.x. Далее загружаются элементы, находящиеся в меню Автозагрузка.

Практическое задание

1. Включить компьютер. Наблюдать процесс тестирования компьютера. В случае возникновения звуковых сигналов или сообщений об ошибке устранить неисправность.
2. Для входа в BIOS Setup в процессе тестирования нажать клавишу {Del}. Утилита имеет интерфейс в виде системы иерархического меню, перемещение по которому производится с помощью клавиш со стрелками.
3. Установить курсор на пункт меню STANDARD CMOS SETUP и нажать клавишу {Enter}.
4. На появившейся панели установить курсор на элемент конфигурационных данных (выделяется цветом) и с помощью клавиш {PageUp} и {PageDown} установить требуемое значение параметра.
5. Установить курсор на пункт меню BIOS FEATURES SETUP и нажать клавишу {Enter}.
6. На появившейся панели установить курсор на элемент конфигурационных данных Anti-Virus Protection и установить значение Enable.
7. На панели BIOS FEATURES SETUP выбрать пункт Security Option и установить значение System или Setup.

8. Открыть панель SUPERVISOR PASSWORD.
9. На появившейся панели ENTER PASSWORD ввести пароль и нажать клавишу {Enter}.
10. Повторно ввести пароль для подтверждения его правильности.
11. Запустить служебную программу Windows Сведения о системе.
12. В окне приложения ввести команду [Сервис-Программа настройки системы].
13. На вкладке Общие можно отключить обработку конфигурационных файлов, а на других вкладках ознакомиться с их содержанием.

Отчет

Отчет должен содержать:
1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

Контрольные вопросы

1. Что такое BIOS?
2. Какие параметры отвечают за безопасность?
3. Что такое конфигурационные файлы?

Практическая работа 22. Настройка параметров безопасности Windows.

Цель работы: Ознакомиться с механизмами аутентификации и идентификации, локальными политиками безопасности, встроенными в ОС Windows XP..

Оборудование: учебный персональный компьютер.

Теоретические основы

В соответствии с сертификационными требованиями к системам безопасности операционных систем при подключении пользователей должен реализовываться механизм аутентификации и/или идентификации. Идентификация и аутентификация применяются для ограничения доступа случайных или незаконных субъектов (пользователей, процессов) к информационной системе, объектам – ресурсам (аппаратным, программным, информационным).

Идентификация – присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

Аутентификация (установление подлинности) – проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он сам себя выдаёт.

Настройка параметров аутентификации в ОС Windows XP выполняется в рамках локальной политики безопасности. Вкладка «Локальная политика безопасности» используется для изменения политики учетных записей и локальных политик безопасности на компьютере. При помощи вкладки «Локальная политика безопасности» можно определить:

- Кто имеет доступ к компьютеру;
- Какие ресурсы могут использовать пользователи на компьютере;
- Включение и выключение записи действий пользователей или группы пользователей в журнале событий.

Задание: Настроить параметры локальной политики безопасности операционной системы Windows XP.

Алгоритм выполнения работы:

Для просмотра и изменения параметров аутентификации пользователей выполните следующие действия:

1. Выберите кнопку Пуск на панели задач.
2. Откройте меню Настроить – Панель управления.

3. В открывшемся окне выберите ярлык Администрирование – Локальная политка безопасности (рис. 1).

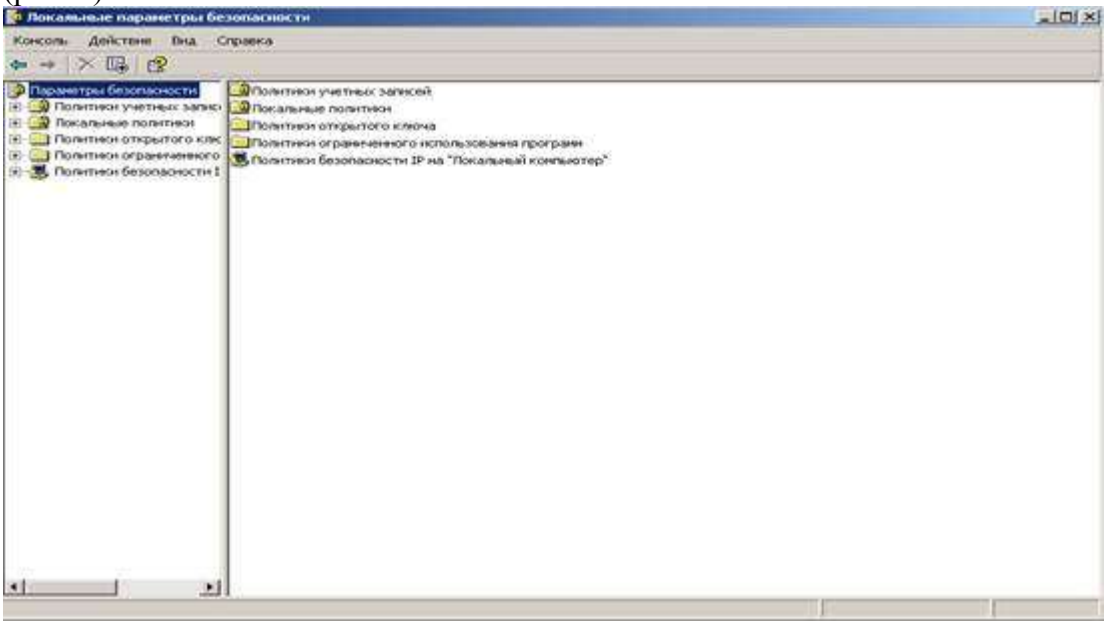


Рис. 1

4. Выберите пункт **Политика учетных записей** (этот пункт включает два подпункта: **Политика паролей** и **Политика блокировки учетной записи**).

5. Откройте подпункт Политика паролей. В правом окне появится список настраиваемых параметров (рис. 2).

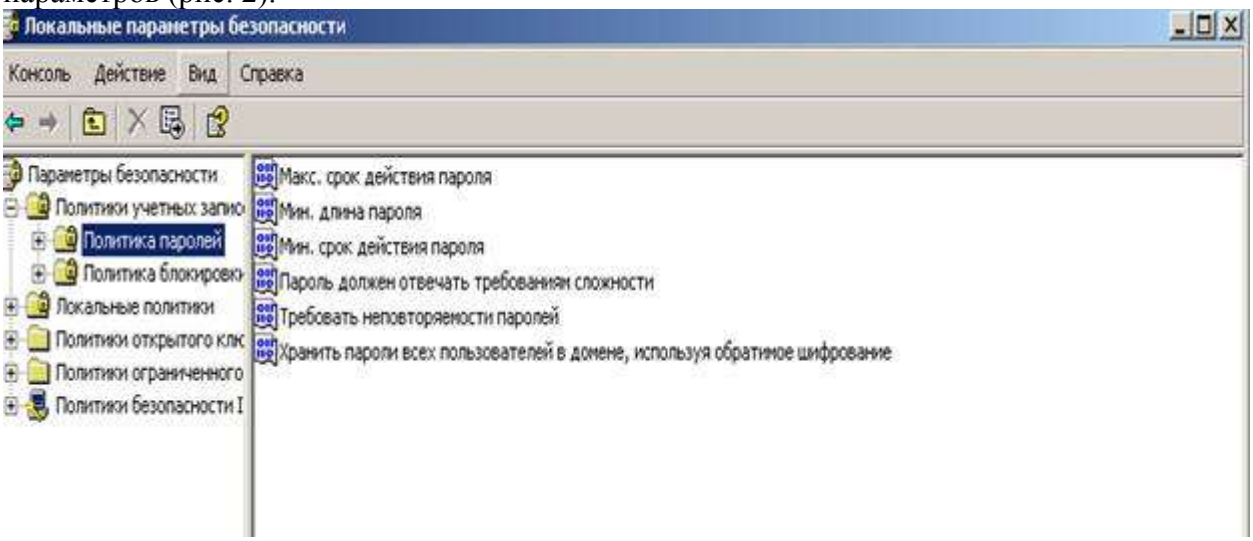


Рис. 2

6. В показанном примере политика паролей соответствует исходному состоянию системы безопасности после установки операционной системы, при этом ни один из параметров не настроен. Возможные значения параметров приведены в таблице №1.

Таблица №1

Значения параметров Политики паролей

Параметр	Значение
Требовать повторяемости паролей	Определяет число новых паролей, которые должны быть сопоставлены учетной записи пользователя, прежде чем можно будет снова использовать старый пароль. Это значение должно принадлежать диапазону от 0 до 24.
Максимальный срок действия пароля	Определяет период времени (в Днях), в течение которого можно использовать пароль, чем система потребует от пользователя заменить его. Можно задать значение в диапазоне от 1 до 999 дней или снять всякие ограничения срока действия, установив число дней равным 0.

Минимальный срок действия пароля.	Определяет период времени (в Днях), в течение которого можно использовать пароль, чем система потребует от пользователя заменить его. Можно задать значение в диапазоне от 1 до 999 дней или снять всякие ограничения срока действия, установив число дней равным 0.
Минимальная длина пароля.	Определяет наименьшее число символов, которые может содержать пароль учетной записи пользователя. Можно задать значение в диапазоне от 1 до 14 символов или отменить использование пароля, установив число символов равным 0
Пароль должен отвечать требованиям сложности	Определяет, должны ли отвечать пароли требованиям сложности. Если эта политика включена, пароли должны удовлетворять следующим минимальным требованиям. Ø Пароль не может содержать имя учетной записи пользователя или какую-либо его часть; Ø Пароль должен состоять не менее чем из 6 символов; Ø В пароле должны присутствовать символы трех категорий из числа следующих четырех: 1. Прописные буквы английского алфавита от A до Z; 2. Строчные буквы английского алфавита от A до Z; 3. Символы не принадлежащие алфавитно-цифровому набору (например, !,$,#,%). Проверка соблюдения этих требований выполняется при изменении или создании паролей.
Хранить пароли всех пользователей в домене, используя обратимое шифрование.	Определяет, следует ли в системах Windows 2000, Windows XP хранить пароли, используя обратимое шифрование. Эта политика обеспечивает поддержку приложений, использующих протоколы, которым для проверки подлинности нужно знать пароль пользователя. Хранить пароли, зашифрованные обратимыми методами, это всё равно, что хранить их открытым текстом. Поэтому данную политику следует использовать лишь в исключительных случаях, если потребности приложения оказываются важнее, чем защита пароля.

7. Ознакомитесь со свойствами всех параметров.
8. Для изменения требуемого параметра выделите его и вызовите его свойства из контекстного меню после нажатия правой кнопки мыши (или дважды щёлкните на изменяемом параметре).
9. В результате этого действия появится одно из окон, показанных на рис. 3.

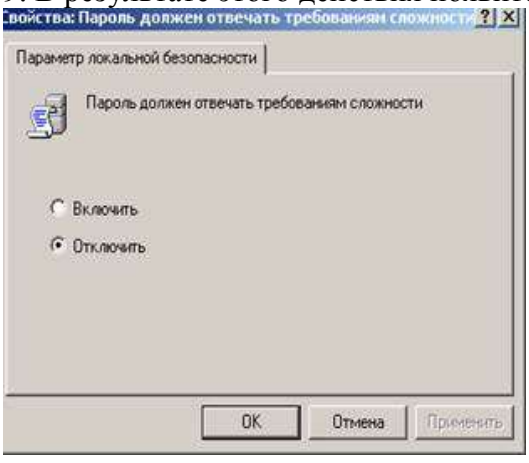


Рис. 3

10. Измените, значение параметра и нажмите Ок.
11. Например (обязательно выполнить и сохранить), выберите параметр Требовать неповторяемости паролей и измените его значение на 1.
12. Для настройки Политики блокировки учетной записи выберите этот подпункт и откройте его.
13. Значения параметров данного подпункта Политики учетной записи приведены в таблице №2.

Таблица №2

Параметр	Значение

Пороговое значение блокировки	Определяет число неудачных попыток входа в систему, после которых учетная запись пользователя блокируется. Блокированную учетную запись нельзя использовать до тех пор, пока не будет сброшена администратором или пока не истечёт её интервал блокировки. Можно задать значение в диапазоне от 1 до 999 или запретить блокировку данной учетной записи, установив значение 0.
Блокировка учетной записи на	Определяет число минут, в течении которых учетная запись остаётся блокированной, прежде чем будет автоматически разблокирована. Этот параметр может принимать значения от 1 до 99999 минут. Если установить Значение 0, учетная запись будет блокирована на всё время до тех пор, пока администратор не разблокирует её явным образом. Если пороговое значение блокировки определено, данный интервал блокировки должен быть больше или равен интервалу сброса.
Сброс счетчика блокировки через	Определяет число минут, которые должны пройти после неудачной попытки входа в систему, прежде чем счетчик неудачных попыток будет сброшен в 0. Этот параметр может принимать значения от 1 до 99999 минут. Если определено пороговое значение блокировки, данный интервал сброса не должен быть больше интервала Блокировка учетной записи на.

14. Ознакомитесь со свойствами всех параметров.
15. Для изменения параметров воспользуйтесь алгоритмом, описанным в пунктах 8-10.

Задания для самостоятельной работы:

1. Измените параметр «**Пароль должен отвечать требованиям сложности**» **Политики паролей** на «**Включен**» (рисунок 3) и после этого попробуйте изменить пароль своей учетной записи. Зафиксируйте все сообщения системы, проанализируйте и введите допустимый пароль. Этот пароль является результатом выполнения Вашего задания.
2. После успешного выполнения первого задания, измените пароль Вашей учетной записи, а в качестве нового пароля укажите прежний пароль. Все сообщения зафиксируйте, проанализируйте и объясните поведение системы безопасности.
3. Проведите эксперименты с другими параметрами **Политики учетных записей.**

Отчет

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

Контрольные вопросы

1. Что такое аутентификация и идентификация?
2. Для чего применяются эти механизмы?
3. Что можно настроить с помощью вкладки Локальные политики безопасности?

Практическая работа 23. Настройка параметров безопасности Интернет.

Цель работы произвести настройку параметров безопасности Internet Explorer.

Оборудование: учебный персональный компьютер.

Ход выполнения работы:

1. Откройте диалоговое окно **Свойства: Интернет (*Пуск/Панель управления/Свойства обозревателя*)**;

2. Перейдите на вкладку **Безопасность** и откройте параметры зоны Интернет с помощью кнопки ***Другой…***;
3. Установите ***Проверку имени пользователя*** в режим **Запрос имени пользователя и пароля**;
4. Разрешите в соответствующих полях указанные ниже действия:
    - Блокировать всплывающие окна;
    - Доступ к источникам данных за пределами домена;
    - Переход между кадрами через разные домены;
5. Установите **Разрешения канала программного обеспечения** на *Высокий уровень безопасности*;
6. Отключите *Использование элементов ActiveX не помеченных как безопасные*;
7. Отключите загрузку *Неподписанных элементов ActiveX*;
8. Примените параметры кнопкой ***ОК***;
9. Установите параметры конфиденциальности:
    - перейдите на вкладку **Конфиденциальность**;
    - установите регулятор на уровень *Умеренно высокий*;
    - разрешите загружать файлы ***cookie*** с узла **www.mail.ru**:
        - щелкните по кнопке ***Узлы***;
        - введите в поле *www.mail.ru* и щелкните по кнопке ***Разрешить***;
    - аналогично разрешите загружать cookie со следующих узлов: **www.yandex.ru, www.pochta.ru**;
    - примените параметры кнопкой ***ОК***;
10. Настройте ограничения на доступ к ресурсам по содержанию информации на них:
    - перейдите на вкладку **Содержание** и откройте окно **Ограничение доступа** кнопкой ***Включить*** в разделе **Ограничения доступа**;
    - установите пароль:
        - перейдите на вкладку **Общие**;
        - откройте окно создания пароля кнопкой ***Создать пароль***;
        - введите **пароль** - *user* и **подсказку** к нему - *user*;
        - примените параметры кнопкой ***ОК***.
    - перейдите на вкладку **Оценки** и установите уровни **Службы оценки Recreational Software Advisory Council** по своему усмотрению;
    - примените параметры кнопкой ***ОК***;
    - очистите пароли, которые браузер автоматически запоминает. Для этого на вкладке **Содержание**, щелкните по кнопке ***Автозаполнение***, а затем по кнопке ***Очистить пароли***;
    - удалите временные фалы Интернет и ***cookies*** на вкладке **Общие**.

Отчет

Отчет должен содержать:
1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

Контрольные вопросы

1. Какие параметры необходимо настраивать для обеспечения безопасности браузера Internet Explorer?
2. Для чего необходима проверка имени пользователя и пароля?
3. Зачем необходима настройка параметров конфиденциальности?