МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению практических занятий
по дисциплине «Основы информационной безопасности»
для студентов
Специальности 10.05.03 Информационная безопасность
автоматизированных систем
Специализация «Анализ безопасности информационных систем»

Ставрополь
2026

ВВЕДЕНИЕ

Цель и задачи освоения дисциплины

Целью освоения дисциплины «Основы информационной безопасности» является формирование у будущего специалиста по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация «Анализ безопасности информационных систем» понимания основных методов, средств и технологий эффективного взаимодействия и реализации успешной командной работы.

Задачи дисциплины:

– изучение теоретических основ формирования и развития навыков командной работы;

– формирование умений управления групповыми проектами;

– овладение навыками эффективного социального взаимодействия, создания благоприятной и конструктивной атмосферы в команде средствами доступных информационных технологий.

СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

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:

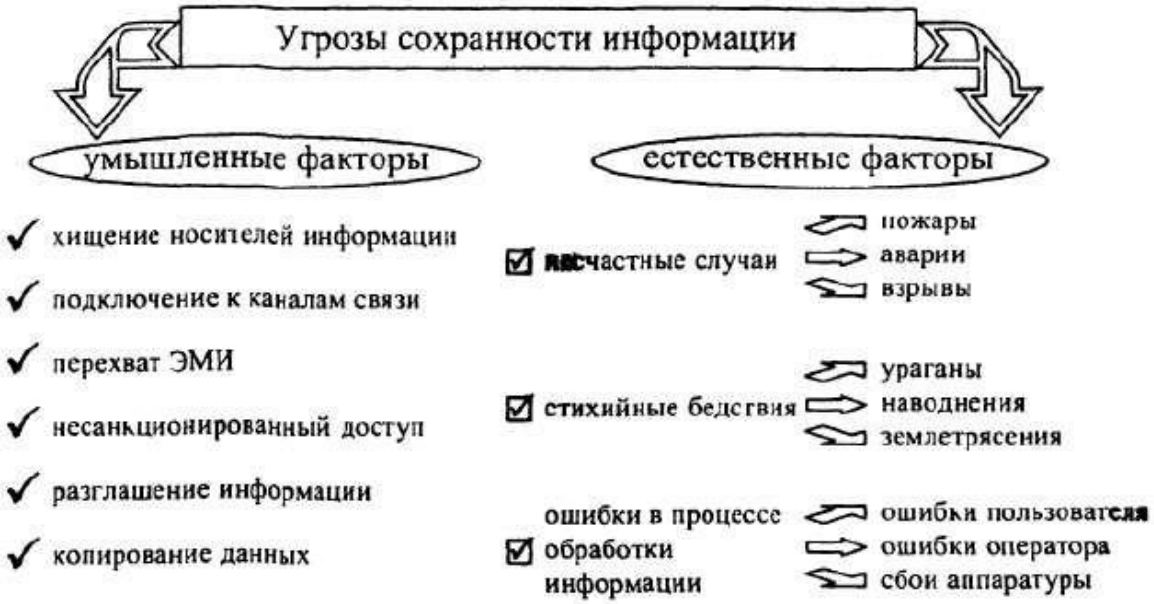
1) подверженность физическому искажению или уничтожению;

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

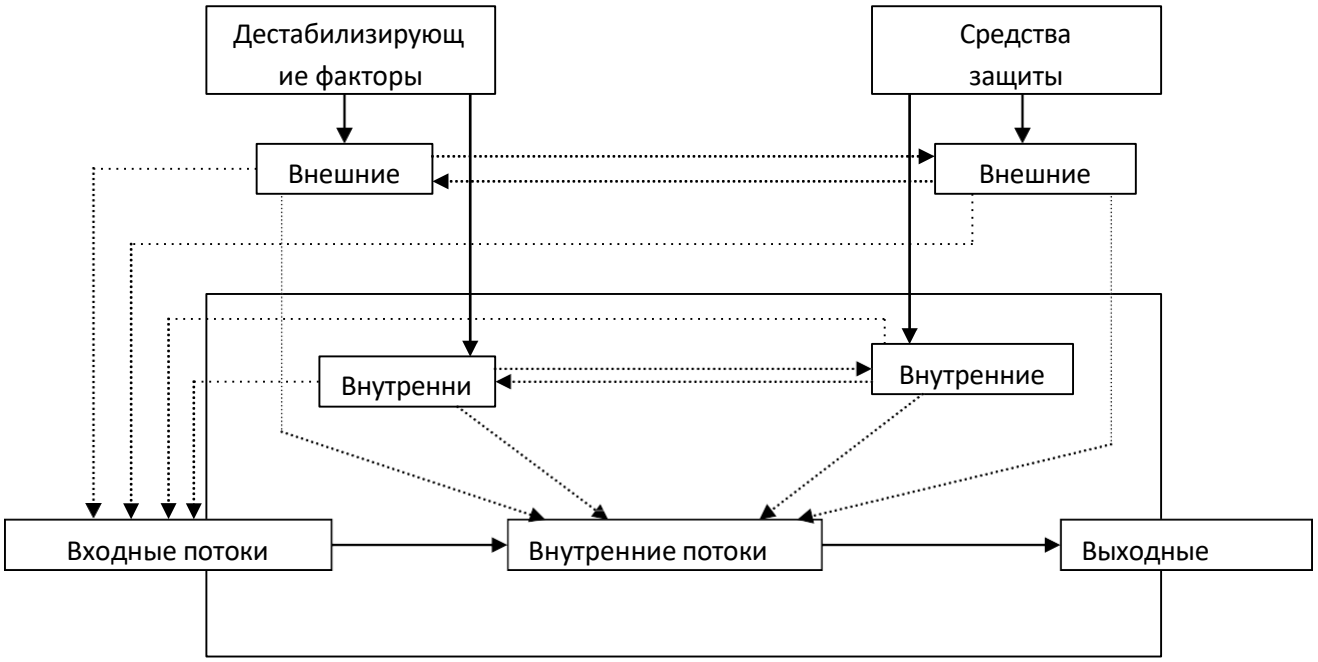
1. Что такое целостность информации?
2. Какие меры можно предпринять для защиты информации?

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.



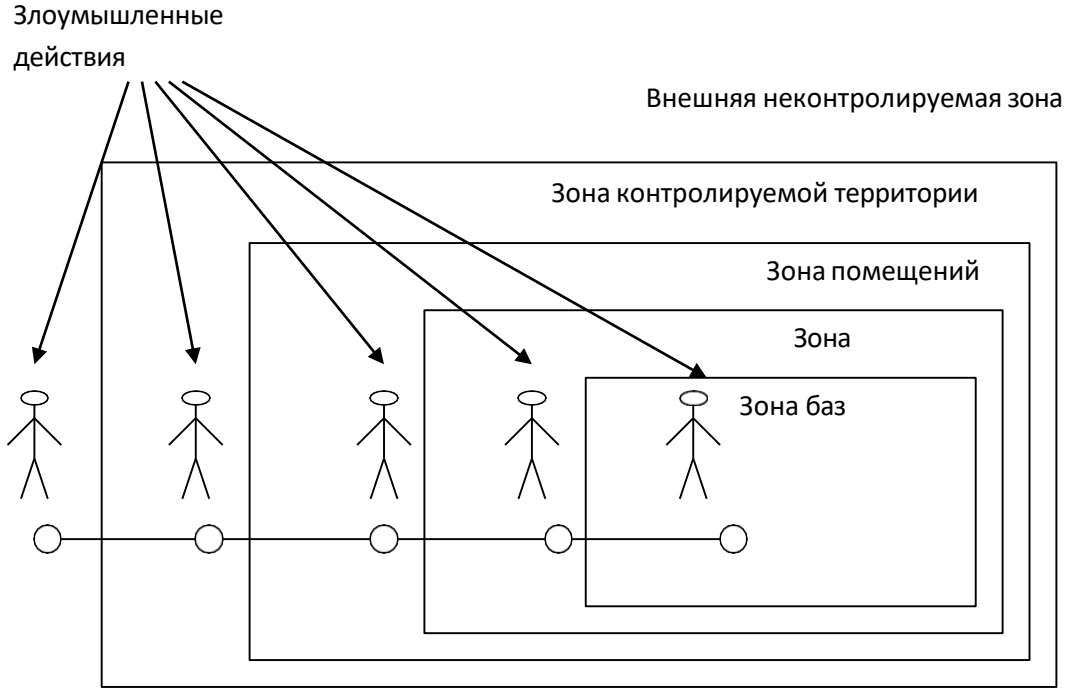
Данная детализируется при изучении конкретных видов уязвимости информации: нарушения физической или логической целостности, несанкционированной модификации, несанкционированного получения, несанкционированного размножения.

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 $С_{опт}$, 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

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

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?