Содержание:

Введение

Обеспечение информационной безопасности более чем необходимо, потому что сегодня множество данных передаются электронным образом. Проблема с обеспечением безопасности очень актуальна, потому что с развитием технологий все чаще возникают различные угрозы информационной безопасности и персональным данных.

Информационная безопасность - это общий термин для понятия защиты информации и чаще всего относится к защите информации, обрабатываемой и хранящейся в электронной форме с помощью компьютерных технологий. Термин «компьютерная безопасность» более точен, но термин «информационная безопасность» более распространен. Защита включает меры по защите от кражи данных, несанкционированного доступа, раскрытия, изменения или уничтожения данных, а также поддержанию их целостности и актуальности.

Цель данной курсовой работы - объяснить концепцию «информационной безопасности», ее содержания, вид и состав угроз информационной безопасностью

В связи с этим должны быть решены следующие задачи:

- Дать общее описание предметной области;
- Определить ключевые понятия информационной безопасности;
- Описать возможные типы уязвимостей;
- Описать виды и состав угроз информационной безопасности;
- Описать средства защиты от угроз.

Работа является актуальной по той причине, что знать основные типы и виды угроз информационной безопасности и их состав – необходимо каждому специалисту в области информатики, а особенно в области защиты информации.

1. Понятие информационной безопасности

1.2. Понятие информации и информационной безопасности

Информация всегда была и остается самым востребованным и дорогостоящим товаром, который особенно влияет на современное информационное общество. Проблемы компьютерной безопасности становятся все более серьезными с развитием информационных технологий и усилением атак на компьютерные системы. С точки зрения политики государственной безопасности защита информации является очень важной.

Одной из целей каждой информационной системы является предоставление полной, надежной и своевременной информации. Эта информация уязвима из-за случайных и злонамеренных дестабилизирующих факторов (угроз), которые требуют принятия мер для ее защиты.

Объектом защиты является структурный компонент информационной системы, в которой расположена информация. Такими объектами являются компьютеры (рабочие станции пользователей и системных администраторов, локально используемые настольные компьютеры, периферийные устройства), сетевые инструменты (модемы, оборудование для передачи данных, маршрутизаторы, сетевые серверы, каналы связи) и помещения. технической базы информационных систем. Компьютерная безопасность защищает информацию, хранящуюся в системе. Вот почему компьютерную безопасность часто называют информационной безопасностью.[1]

Цели информационной безопасности:

• Защита конфиденциальности: означает, что защищенная компьютерная система не должна допускать раскрытие информации пользователем, который не авторизован (нет аутентификации и несанкционированного доступа к нему).

• Защита целостности: компьютерная система должна поддерживать целостность сохраненной в ней информации. Точность или целостность означает, что система не должна компрометировать информацию или допускать несанкционированные преднамеренные или случайные изменения.

• Защита доступности: качество системы обеспечивает доступность информации в нужное время. Доступность - это качество компьютерной системы, которая обеспечивает доступность информации пользователю. Доступность означает, что

аппаратное и программное обеспечение компьютерной системы работает эффективно и что система может быстро и восстанавливаться, если происходит бедствие.

В конкретной среде один из аспектов безопасности может быть более важным, чем другие. При проектировании каждого отдельного информационного ресурса необходимо оценить общие требования безопасности, который также будет влиять на выбор специальных технических устройств и продуктов для удовлетворения этих требований.

Компьютерная и сетевая безопасность является свойством компьютерных систем и сетей для противодействия попыткам доступа к обрабатываемой и хранящейся информации, что приводит к разрушительным действиям и получению ложной информации. Она основывается на следующих концепциях:

- Идентификация. Пользователи входят в систему с помощью специальных приложений;
- Аутентификация - подтверждение личности пользователя.
- Авторизация. Назначение прав доступа для каждого пользователя (например, для записи, чтения или выполнения файла).
- Контроль доступа. Назначение прав доступа к сетевым ресурсам и защита ресурсов за счет ограниченного доступа (кому, как, когда и в каких условиях разрешен доступ).

Информационные системы нуждаются в безопасности информации при их обработке, хранении и переносе.

Для обеспечения конфиденциальности, целостности и доступности в качестве элементов информационной безопасности необходимо выполнить определенные меры безопасности. Более типичными из них являются политики и процедуры безопасности, технологии защиты и обучение для применения передового опыта в области безопасности.

Информационная безопасность - сложная концепция. Он включает административную и информационную безопасность:

Административная безопасность - обеспечение физической безопасности компьютерных сетей и систем, а также обеспечение непрерывности управления. Он разделен на два типа:

Непрерывность информации представляет собой систему правил и положений для регулируемых и нормативных актов, регулирующих защиту конфиденциальной информации, нарушение которой приводит к ответственности. [2]

Физическая безопасность связана с системой организационных, физических и технических мер по предотвращению несанкционированного доступа к важной (чувствительной) информации.

ИТ-безопасность - безопасность связана с безопасностью связи, а также с безопасностью данных. ИТ-безопасность защищает компьютер и все, что с ним связано - здание, комнаты, терминалы, принтеры, кабели, диски или что-то, что связано с защитой информации, поэтому часто это равенство между компьютерной и информационной безопасностью.

1.2. Ключевые понятия информационной безопасности

Три ключевых понятия, используемые в дискуссиях по информационной безопасности:

- Уязвимость
- Угроза
- Противодействие

Для каждой системы необходимо тщательно учитывать уязвимости и возможные угрозы, чтобы решить, как защитить систему и ее информацию.

Информационная безопасность заинтересована в выявлении уязвимостей в системах и защите от угроз для этих систем.

Уязвимость - это точка, в которой система подвержена атаке. Каждая компьютерная система уязвима для атаки. Политика безопасности и продукты могут снизить вероятность того, что атака сможет сломать защиту системы, заставив нарушителя тратить столько времени и ресурсов, что это не оправдывает затраты. Но один из основных принципов заключается в том, что нет полностью безопасной системы.

Ключевые факторы воздействия:

1. Резкое увеличение собираемой и обрабатываемой информации

2. Массовое использование компьютерных сетей и их интеграция.

3. Интеграция информации в различные базы данных.

4. Расширение круга пользователей, имеющих доступ к системным ресурсам и базам данных.

1.3. Типы уязвимостей

Типы уязвимости - в зависимости от того, где система подвержена атаке, уязвимости подразделяются на:

Физическая уязвимость - здания и компьютерные залы уязвимы. Злоумышленник может проникнуть в место хранения информации и повредить или уничтожить хранители информации. Замки и биометрические устройства (устройства, которые проверяют физические функции, такие как отпечатки пальцев, голос, подпись и сравнивают их, чтобы определить, являетесь ли вы тем, за кого себя выдаете) обеспечивают важную первичную защиту от взлома. Также эффективны аварийные сигналы и другие общие средства защиты. [10]

Природная уязвимость - компьютеры очень уязвимы для стихийных бедствий и экологических угроз. Катастрофы, такие как пожар, наводнение и землетрясение, могут разрушить компьютерные системы и данные. Пыль, влажность и высокие/низкие температуры также могут привести к повреждению.

Уязвимость оборудования и программного обеспечения. Некоторые типы аппаратных сбоев могут поставить под угрозу безопасность всей компьютерной системы. Например, многие системы обеспечивают аппаратную защиту путем структурирования памяти в привилегированных и несанкционированных областях. Если защита памяти не удалась, в системе происходит хаос, и безопасность нарушена. Программные сбои любого рода могут привести к сбою системы, сделать ее доступной для проникновения, или сделать ее настолько ненадежной, что она не гарантирует правильную и эффективную работу. Даже если аппаратные и программные компоненты защищены, вся система может быть скомпрометирована, если аппаратные компоненты неправильно подключены или если программное обеспечение установлено неправильно.

Уязвимости на периферии - дискеты, флеш-карты и принтеры могут быть украдены или повреждены такими различными опасностями, такими как пыль и химикаты. Большинство операций с носителями информации переписывают описания файлов, а не полностью очищать диск, поэтому важные данные могут быть восстановлены с носителя.

Уязвимости от прослушивания. Все электронное оборудование излучает электрическое и электромагнитное излучение. Электронные прослушивающие устройства могут обнаруживать сигналы, излучаемые компьютерными системами и сетями, а затем восстанавливать их. Информация, хранящаяся и передаваемая системами и сетями, становится уязвимой.

Уязвимости в области связи - если компьютер подключен к сети или даже если к нему обращаются по телефону, растет риск того, что кто-то сможет попасть в компьютерную систему. Сообщения могут быть обнаружены и изменены. Линии связи, соединяющие компьютеры друг с другом или соединительные терминалы с центральным компьютером, могут быть прерваны или физически повреждены.

Человеческий фактор - люди, которые управляют и используют компьютерную систему, являются самой большой из всех уязвимостей. Безопасность всей системы часто находится в руках системного администратора. Если этот администратор не имеет опыта или не принимает решения о совершении преступлений, система подвержена серьезной опасности. Обычные пользователи компьютеров, операторы, и другие люди также могут быть подкуплены или вынуждены передавать пароли, открывать двери или иным образом угрожать безопасности системы.

Операционные уязвимости. Существует множество вариантов легкого использования различных типов уязвимостей. Например, для прослушивания телефонного или сотового телефона требуется только один сканер. Включение системы, которая не имеет защиты паролем или имеет минимальный контроль, почти так же легко. С другой стороны, прослушивание зашифрованного волоконно-оптического канала связи или перехват передач из особо защищенного оборудования очень сложны. [8]

2. Виды и состав угроз информационной безопасности

2.1. Виды угроз информационной безопасности

Используя глобальные информационные технологии, мы также должны анализировать угрозы и риски этих технологий и то, что должно быть ответом на безопасность. Угроза может представлять опасность для системы; опасностью может быть человек (системный бандит или шпион), объект (дефектная часть оборудования) или событие (пожар или наводнение), которые могут использовать данную уязвимость в системе. Эти три компонента входят в систему безопасности. При построении политики безопасности подумайте о том, какие объекты и предметы.

Угрозы делятся на три основные категории:

Природными и физическими угрозами являются угрозы, которые угрожают любому человеку и части оборудования: пожары, наводнения, сбои питания и друге бедствия. Не всегда возможно предотвратить такие бедствия, но можно быстро реагировать, если возникнет какая-либо из них (с помощью пожарной сигнализации, например). Можно свести к минимуму вероятность серьезного ущерба. Системы защиты от стихийных бедствий могут быть защищены (путем резервного копирования важных данных в другом здании или путем организации резервной системы, которая будет использоваться в опасной ситуации).

Случайные угрозы - это те, которые вызваны незнанием - например, пользователь или системный администратор, который не прошел надлежащую подготовку, кто не прочитал документацию, и кто не понимает важность правильного применения процедур безопасности. Кто-то может сбросить диск или попытаться обновить базу данных некорректно и непреднамеренно удалить файл. Системный администратор может стать суперпользователем и изменить защиту файлов паролей или важное системное программное обеспечение. Гораздо больше информации скомпрометировано и потеряно из-за невежества, а не злого умысла.

Умышленные угрозы делятся на два типа: внутренние и внешние. Например, случайный нарушитель может не иметь возможности захватывать и расшифровывать электромагнитное излучение или выполнять определенный криптоанализ. [4]

Внутренние халатности - корпоративные нарушители (могут работать в вашей компании)

Внешние вредоносные:

Агенты иностранной разведки - они не встречаются повсюду, но они действительно существуют. Продукты, использующие технологию TEMPEST или устройства шифрования, лучше всего подходят для установки, где атаки на определенную информацию представляют собой реальную угрозу;

Террористы. Существуют также примеры целенаправленных нападений на университетские компьютерные центры, военные ремонтные центры, суда, и т.д.

Преступники - компьютерные преступления скрыты, в отличие от многих других видов преступлений. Целью может быть незаконная кража или другой вид вымогательства;

Корпоративные нарушители - все больше корпораций полагаются на компьютеры, сетевые коммуникации и электронную почту. Корпоративные записи и неофициальные сообщения иногда становятся более уязвимыми для атак;

Хакеры. Когда люди говорят о хакерах, они обычно означают злонамеренных людей, которые больше интересуются проблемой, чем результатами. Эти злонамеренные люди могут заглянуть в интересные данные и программы, но обычно они не делают это за деньги или за политические дивиденды.

2.2. Состав угроз информационной безопасности

Чем ценнее информация, тем труднее обеспечить ее безопасность, потому что многие злоумышленники хотят получить к ней доступ.

Основные риски и угрозы:

1. Вредоносное программное обеспечение

Это программное обеспечение работает без уведомления и информированного согласия пользователей компьютерной системы. Сюда входят компьютерные вирусы, черви, трояны, программы-шпионы и многое другое. Законное программное обеспечение, такое как архивные системы, удаленные системы технической поддержки и системы мониторинга персонала, также может использоваться в качестве вредоносного ПО, если они скрыты от пользователей. Компьютерная система может быть заражена вредоносным программным

обеспечением непреднамеренно, пользователь может получить его посещая веб-сайты, открывая почтовые вложения и чаты, используя портативные электронные носители (флэш-память), используя общие ресурсы (общие папки) в компьютерной сети, устанавливая зараженное законное программное обеспечение и т. д. Вредоносное программное обеспечение может быть установлено целенаправленно, через физический доступ к компьютерной системе или удаленно, с использованием пароля или уязвимостей в операционной системе, системном и прикладном программном обеспечении. Вредоносная программа может использоваться для чтения, изменения, записи или уничтожения информации (документов, почты, паролей и т. д.), обрабатываемых и хранящихся на локальном компьютере и доступных сетевых сервисах. Для программ-шпионов более свойственно совершение действий путем мониторинга экрана компьютера. Также они используются для прослушивания микрофона (ноутбуки имеют встроенные микрофоны), несанкционированного доступа к услугам и информации в локальных сетях, перехвата трафика и других методов заражения компьютерных систем в локальных сетях или Интернете и т. д. [10]

По данным за 2008 г., существует более миллиона активных разновидностей вредоносного программного обеспечения, каждый год увеличивается количество новых вредоносных программ.

При использовании антивирусного программного обеспечения защита не может быть гарантирована из-за того, что антивирусное программное обеспечение работает в основном с базами данных (определениями) уже распространенных вредоносных программ.

Для приемлемого уровня защиты от вредоносного программного обеспечения пользователь должен:

- устанавливать программное обеспечение, используемое для каждого отдельного компьютера, предопределенное и связанное только с обязанностями пользователя;

- использовать ограниченные права доступа к компьютеру, причем только определенные лица должны иметь доступ к учетным записям администратора, чтобы устанавливать системное программное обеспечение и изменять настройки системы;

- иметь правила (политика безопасности), т.е. кто, когда и с какой санкцией может установить новое программное обеспечение;

- иметь все исправления, связанные с безопасностью используемой системы и прикладного программного обеспечения;

- использовать антивирусное программное обеспечение с текущими обновлениями;

- обеспечить ведение централизованного и непрерывного мониторинга антивирусного программного обеспечения и другого программного обеспечения безопасности.

Могут также применяться дополнительные меры:

- один раз в месяц собственноручно проводить проверку всех или случайно выбранных компьютеров, на заранее подготовленной процедуре, установленном программном обеспечении, запущенных процессах и др.;

- технически запрещать запуск программного обеспечения, отличного от ранее утвержденного и уже установленного;

- контролировать трафик в локальных сетях.

Недобросовестные сотрудники

Сотрудник, который намеренно пытается причинить вред конкретному бизнесу или работодателю. Такой сотрудник может печатать или записывать и передавать конфиденциальную информацию, к которой сложно получить доступ. Это может быть организованно техническим (вредоносное программное обеспечение, перехват трафика) или иным образом для получения несанкционированного доступа к такой информации. Экспорт может осуществляться с помощью внешнего электронного устройства (флэш-памяти, портативного диска, мобильного телефона) или через Интернет (электронная почта, чат-клиенты, передача файлов). Данный сотрудник может предоставить информацию физически или удаленно, используя программное обеспечение (вредоносное ПО, программное обеспечение для удаленного обслуживания) и / или аппаратное обеспечение (беспроводное устройство, мобильный телефон) для компьютерных систем и сетей организации. [3]

Существенная опасность со стороны недобросовестных сотрудников, чьи обязанности включают защиту информации и техническую поддержку компьютерных систем, заключается в том, что они либо имеют, либо могут легко получить несанкционированный доступ ко всей информации.

Для приемлемого уровня защиты от недобросовестных сотрудников необходимо:

- хранить конфиденциальную информацию на серверах организации и / или на отдельных компьютерах, для которых применяются более строгие меры защиты;

- ограничить физический доступ к серверным / компьютерным комнатам;

- создать структуру папок с соответствующими элементами управления доступом (кто, к какому файлу / файлу обращается), с учетом принципа необходимости;

- ввести обязательное использование паролей для доступа к компьютерным системам и службам с соответствующими правилами (изложенными в Политике безопасности);

- определить правила для систем и служб, обрабатывающих конфиденциальную информацию, для непрерывной записи всех событий, связанных с доступом к этим системам, услугам и обрабатываемой ими информации;

- иметь правила (изложенные в политике безопасности) - кто, когда и с какой санкцией может выполнять технические действия, связанные с кабельной системой, оборудованием связи, серверами и компьютерами;

- обеспечить адекватную защиту от вредоносного программного обеспечения.

Могут также применяться дополнительные меры:

- внедрение программного обеспечения для мониторинга персонала;

- использование шифрования трафика в локальных сетях;

- использование смарт-карты вместо паролей для доступа к компьютерным системам и услугам;

- ограничение компьютеров, предназначенных для хранения конфиденциальной информации, в связи с Интернетом или другими общедоступными сетями;

- предупреждение ошибок пользователей.

Бессознательное действие или бездействие сотрудника, который наносит ущерб организации.

Эти действия или упущения могут быть вызваны обманом или небрежностью. Эти ошибки могут привести к заражению вредоносным программным обеспечением,

помогать действиям недобросовестных или посторонних людей в нанесении вреда организации, вызывать технические сбои или уничтожать информацию, раскрывать конфиденциальную информацию по доступу через Интернет или приводить к потере электронных носителей (флэш-память, портативный компьютер).

В данном случае наибольшей опасностью является угроза сотрудников, чьи обязанности включают защиту информации и техническую поддержку компьютерных систем. Их ошибки оказывают самое серьезное влияние на компьютерную безопасность и информацию, обрабатываемую и хранящуюся в компьютерных системах. Они или их права доступа могут дать возможность несанкционированного доступа ко всей информации или обхода и отключения системы безопасности. [11]

Для достижения приемлемого уровня защиты от пользовательских ошибок необходимо:

- обеспечить адекватную защиту от вредоносного программного обеспечения;

- обеспечить адекватную защиту от недобросовестных сотрудников;

- внедрить автоматизированную систему архивации;

- иметь правила для работы с системами безопасности (политика безопасности) и контролировать соблюдение этих правил.

Могут также использоваться дополнительные меры в виде ограничения использования или шифрования электронных носителей (флеш-накопителей, мобильных компьютеров), одобренных организацией.

Технический сбой

Техническая неисправность может возникнуть в результате ошибки программного обеспечения, сбоя оборудования, стихийного бедствия, человеческой ошибки, злонамеренных действий со стороны сотрудника или аутсайдера. Технические сбои обычно приводят к остановке обслуживания и прерыванию процессов в организации. Неисправность также может привести к потере информации. [8]

Для приемлемого уровня защиты от технического сбоя необходимо:

- обеспечить адекватную защиту от вредоносного программного обеспечения;

- внедрить автоматизированную систему архивации;

- резервировать и дублировать все важные компоненты компьютерных систем;

- подготовить план реагирования на инциденты / план восстановления после сбоя.

Внешние атаки

Внешние атаки - это действия программного обеспечения или третьих сторон, которые предназначены для нанесения вреда организации. Эти действия могут привести к утечке, уничтожению информации или приостановлению определенных услуг.

Подобная атака может быть проведена удаленно – методом использования уязвимостей в операционной системе, системном и прикладном программном обеспечении, перехватом незашифрованного трафика (паролей), использованием вредоносного ПО с помощью социальной инженерии (мошенничество).

Для приемлемого уровня защиты от внешних атак необходимо:

- использовать брандмауэры для подключения к Интернету;

- использовать адекватную защиту от вредоносного программного обеспечения.

Наиболее распространенными ошибками, которые непосредственно влияют на безопасность информации, в этом случае, являются:

1. При подключении к Интернету:

- аппаратные устройства принадлежат интернет-провайдерам:

- они обслуживаются провайдером и имеют подключение к локальной сети.

2. При создании кабельной системы и оборудования связи:

- отсутствие документации;

- использование сотрудниками переносных персональных устройств.

3. При покупке и установке оборудования:

- недостаточная проверка оборудования;

- отсутствие профилактики.

4. При покупке и установке программного обеспечения:

- установка программного обеспечения по личному усмотрению пользователя;

- установка внешними компаниями программного обеспечения для технической поддержки;

- использование различного программного обеспечения, часто пиратского, в отсутствие свободных аналогов;

- отсутствие обновления операционных систем, системного и прикладного программного обеспечения;

- использование антивирусного программного обеспечения, часто отличающегося на разных компьютерах, иногда без современных определений и без централизованного мониторинга;

- разделение папок независимо от информации в них;

- отсутствие на компьютерах паролей, системные учетные записи остаются без пароля;

- обход пароля с помощью загрузки операционной системы с внешнего носителя;

- отсутствие централизованного и автоматизированного архива;

- отсутствие записи контроля и распространения информации о личных компакт-дисках и мобильных компьютерах;

- отсутствие правил и общей концепции действий, включая безопасность.

Ведущие вопросы информационной безопасности:

- Нападения на финансовые системы;

- Дискредитование корпораций;

- Производственный саботаж;

- Раскрытие корпоративных секретов;

- Нарушение прав интеллектуальной собственности.

7, 8 и 9 февраля 2000 года состоялась массовая атака на одни из самых популярных интернет-серверов - Yahoo, eBay, Amazon, Buy, CNN, ZDNet, Datek и E * Trade. По некоторым данным, трехчасовое отсутствие этих серверов привело к убыткам, которые составляют 6 млрд. дол.

2.3. Средства защиты от угроз информационной безопасности

Угрозы растут и меняют свой облик каждый день, учитывая динамичное развитие компьютерных технологий и тенденцию к глобализации документооборота. Это требует улучшения мер безопасности и введения новых в случае необходимости.

Независимо от того, насколько улучшаются средства защиты информации, разрабатываются новые методы для их преодоления. Поэтому возрастающие требования предъявляются и к системам защиты информации, которые должны поддерживать интеграцию, соответствовать вложенным в них инвестициям, быть управляемыми и масштабируемыми.

Однако наиболее серьезная угроза безопасности исходит от самого человека.

Таким образом, наиболее неоспоримая угроза безопасности на сегодняшний день, как и ранее, человек – создающий сознательные целенаправленные действия по уничтожению и нанесению вреда другому человеку, обществу и миру.

Необходимо предвидеть и регулировать угрозы действий людей. Но прежде всего усилия должны быть направлены на то, чтобы избежать стимула, намерения таких действий, ограничить причины их возникновения.

Законом о секретной защите информации введены эффективные механизмы обеспечения информационной безопасности для организаций, которые создают, обрабатывают, хранят и передают секретную информацию в автоматизированных информационных системах и сетях.

Успешно создана государственная система защиты секретной информации и система сертификации ее фондов. Это создает новую нормативную базу для обеспечения информационной безопасности в управленческих, организационных и программных аспектах. Рассматривается вопрос о разработке эффективных политик, правил и процедур для обеспечения информационной безопасности и защиты секретной информации в автоматизированных информационных системах и сетях.

Политика защиты информации и секретной информации является активным компонентом защиты, включая результаты анализа возможных угроз, сценариев их реализации, оценки риска и выбора методов и средств противодействия.

Программно-технические аспекты защиты секретной информации в АИС и сетях являются наиболее важным аспектом защиты информации. Основная часть убытков связана с действиями юридических пользователей, в отношении которых управленческие и организационные меры неэффективны.

Программно-технические аспекты защиты включают:

- однозначную идентификацию и аутентификацию пользователей до совершения других действий;

- эффективный и надежный контроль доступа к ресурсам информационной системы, механизмы для которых должны позволять пользователям делиться на группы пользователей;

- доступ к информации в соответствии с принципом необходимости;

- непрерывная регистрация всех событий, связанных с безопасностью информационной системы;

- периодическая проверка и анализ аудиторских записей и идентификация действий, связанных с безопасностью отдельных лиц;

- строгий контроль конфигурации;

- сохранение целостности и достоверности информации;

- сохранение работоспособности системы;

- защита от вредоносного программного обеспечения.

Организационные меры по защите секретной информации в АИС и сетях ориентированы на человека.

Личная безопасность включает принципы и меры, применяемые компетентными органами в отношении системного и обслуживающего персонала, пользователей и лиц, участвующих в разработке и создании информационных систем, для обеспечения защиты секретной информации в соответствии с принципом «необходимо знать» и принцип «четырех глаз», чтобы предотвратить возможность

того, что человек знает и / или полностью контролирует важные функции безопасности.

Физическая безопасность достигается путем создания зон безопасности, в отношении которых внедряется система организационных, физико-технических мер для предотвращения несанкционированного доступа к материалам, документам, оборудованию и объектам, составляющим государственную или служебную тайну, для защиты от шпионажа, потери, кражи, модификации, повреждения или разрушения.

Документарная безопасность включает в себя систему мер и средств защиты секретной информации при создании, обработке и хранении документов, а также организацию, работу и безопасность регистров секретной информации.

Защита от электромагнитных излучений - меры по защите информации путем ограничения воздействия электромагнитных излучений, чтобы предотвратить перехват и анализ. Требуется для информационных систем, обрабатывающих секретную информацию, классифицированную как «конфиденциальная». Предметом защиты является не только компьютерное и коммуникационное оборудование, но также кабельные системы и маршруты, источники питания и т. д. [4]

Криптографическая безопасность связана с использованием криптографических методов и средств, проверяемых и утвержденных криптографическим органом безопасности, которые применяются для защиты секретной информации от несанкционированного доступа при ее создании, обработке, хранении и передаче.

Заключение.

Чем ценнее информация, тем сложнее ее защитить. Анализы и исследования показывают, что незаконное использование информации и личных данных достаточно распространено в 21 веке.

В последние годы большое внимание уделяется вопросам защиты информации, накапливаемой, хранимой и обрабатываемой как в отдельных компьютерах, так и построенных на их основе вычислительных системах. При этом под защитой информации понимается создание совокупности средств, методов и мероприятий, предназначенных для предупреждения искажения, уничтожения и

несанкционированного использования защищаемой информации.

Основными факторами, способствующими повышению уязвимости информации, являются:

- постоянно возрастающие объемы обрабатываемых данных;

- сосредоточение в единых базах данных информации различного назначения и принадлежности;

- резкое расширение круга пользователей, имеющих непосредственный доступ к ресурсам вычислительной системы;

- расширение использования компьютерных сетей, в частности глобальной сети Интернет, по которым передаются большие объемы информации государственного, военного, коммерческого и частного характера и т.д.

Учитывая эти факты, защита информации в процессе ее сбора, хранения, обработки и передачи приобретает исключительно важное значение.

Список использованных источников

1. Арсентьев М. В. К вопросу о понятии «информационная безопасность» //Информационное общество. – 1997. – №. 4-6. – С. 48-50.
2. Вихорев С. В. Классификация угроз информационной безопасности //URL: http://www. cnews. ru/reviews/free/oldcom/security/elvis_class. shtml. – 2001..
3. Владимирова Т. В. Сетевые коммуникации как источник информационных угроз //Социологические исследования. – 2011. – №. 5. – С. 123-129.
4. Гаврилов А. Д., Волосенков В. О. Угрозы информационной безопасности автоматизированной системы обработки данных //Проблемы безопасности российского общества. – 2013. – №. 4. – С. 85-92.
5. Гафнер В. В. Информационная безопасность: учеб. пособие. – 2009.
6. Девянин П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие. – Горячая линия-Телеком, 2012..
7. Жидко Е. А. Научно-обоснованный подход к классификации угроз информационной безопасности //Информационные системы и технологии. – 2015. – Т. 87. – №. 1. – С. 132.

8. Жидко Е. А. Методология формирования единого алгоритма исследований информационной безопасности //Вестник Воронежского института МВД России. – 2015. – №. 1
9. Курушин В. Д., Минаев В. А. Компьютерные преступления и информационная безопасность. – 1998.
10. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации //М.: Горячая линия-телеком. – 2004. – Т. 16.
11. Мещеряков Р. В. и др. Основы информационной безопасности //М.: Горячая линия-телеком. – 2006.
12. Юруйло А. В. Аудит информационной безопасности. – 2015.
13. Ярочкин В. Информационная безопасность. – Международные отношения, 2000