1 . Что понимается под защитой информации в системах и сетях?

Информационная безопасность (англ. Information Security, а также — англ. InfoSec) — практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные (электронная или, например, физическая). Основная задача информационной безопасности — сбалансированная защита конфиденциальности, целостности и доступности данных, с учётом целесообразности применения и без какого-либо ущерба производительности организации. Это достигается, в основном, посредством многоэтапного процесса управления рисками, который позволяет идентифицировать основные средства и нематериальные активы, источники угроз, уязвимости, потенциальную степень воздействия и возможности управления рисками. Этот процесс сопровождается оценкой эффективности плана по управлению рисками.

Для того, чтобы стандартизовать эту деятельность, научное и профессиональное сообщества находятся в постоянном сотрудничестве, направленном на выработку базовой методологии, политик и индустриальных стандартов в области технических мер защиты информации, юридической ответственности, а также стандартов обучения пользователей и администраторов. Эта стандартизация в значительной мере развивается под влиянием широкого спектра законодательных и нормативных актов, которые регулируют способы доступа, обработки, хранения и передачи данных. Однако внедрение любых стандартов и методологий в организации может иметь лишь поверхностный эффект, если культура непрерывного совершенствования не привита должным образом.

Общие сведения

В основе информационной безопасности лежит деятельность по защите информации — обеспечению её конфиденциальности, доступности и целостности, а также недопущению какой-либо компрометации в критической ситуации. К таким ситуациям относятся природные, техногенные и социальные катастрофы, компьютерные сбои, физическое похищение и тому подобные явления. В то время, как делопроизводство большинства организаций в мире до сих пор основано на бумажных документах, требующих соответствующих мер обеспечения информационной безопасности, наблюдается неуклонный рост числа инициатив по внедрению цифровых технологий на предприятиях, что влечёт за собой привлечение специалистов по безопасности информационных технологий (ИТ) для защиты информации. Эти специалисты обеспечивают информационную безопасность технологии (в большинстве случаев — какой-либо разновидности компьютерных систем). Под компьютером в данном контексте подразумевается не только бытовой персональный компьютер, а цифровые устройства любой сложности и назначения, начиная от примитивных и изолированных, наподобие электронных калькуляторов и бытовых приборов, вплоть до индустриальных систем управления и суперкомпьютеров, объединённых компьютерными сетями. Крупнейшие предприятия и организации, в силу жизненной важности и ценности информации для их бизнеса, нанимают специалистов по информационной безопасности, как правило, себе в штат. В их задачи входит обезопасить все технологии от вредоносных кибератак, зачастую нацеленных на похищение важной конфиденциальной информации или на перехват управления внутренними системами организации.

Информационная безопасность, как сфера занятости, значительно развилась и выросла в последние годы. В ней возникло множество профессиональных специализаций, например, таких, как безопасность сетей и связанной инфраструктуры, защиты программного обеспечения и баз данных, аудит информационных систем, планирование непрерывности бизнеса, выявление электронных записей и компьютерная криминалистика. Профессионалы информационной безопасности имеют весьма стабильную занятость и высокий спрос на рынке труда. Масштабные исследования, проведённые организацией (ISC)² показали, что на 2017 год 66 % руководителей информационной безопасности признали острую нехватку рабочей силы в своих подразделениях, а по прогнозам к 2022 году недостаток специалистов в этой области составит по всему миру 1 800 000 человек.

Угрозы и меры противодействия

Угрозы информационной безопасности могут принимать весьма разнообразные формы. На 2018 год наиболее серьёзными считаются угрозы связанные с «преступлением как услугой» (англ. Crime-as-a-Service), Интернетом вещей, цепями поставок и усложнением требований регуляторов. «Преступление как услуга» представляет собой модель предоставления зрелыми преступными сообществами пакетов криминальных услуг на даркнет-рынке по доступным ценам начинающим киберпреступникам. Это позволяет последним совершать хакерские атаки, ранее недоступные из-за высокой технической сложности или дороговизны, делая киберпреступность массовым явлением. Организации активно внедряют Интернет вещей, устройства которого зачастую спроектированы без учёта требований безопасности, что открывает дополнительные возможности для атаки. К тому же, быстрое развитие и усложнение Интернета вещей снижает его прозрачность, что в сочетании с нечётко определёнными правовыми нормами и условиями позволяет организациям использовать собранные устройствами персональные данные своих клиентов по собственному усмотрению без их ведома. Кроме того, для самих организаций проблематично отслеживать, какие из собранных устройствами Интернета вещей данных передаются во вне. Угроза цепей поставок состоит в том, что организации, как правило, передают своим поставщикам разнообразную ценную и конфиденциальную информацию, в результате чего теряют непосредственный контроль над ней. Таким образом, значительно возрастает риск нарушения конфиденциальности, целостности или доступности этой информации. Всё новые и новые требования регуляторов значительно осложняют управление жизненно-важными информационными активами организаций. Например, введённый в действие в 2018 году в Евросоюзе Общий регламент защиты персональных данных (англ. General Data Protection Regulation, GDPR), требует от любой организации в любой момент времени на любом участке собственной деятельности или цепи поставок, продемонстрировать, какие персональные данные и для каких целей имеются там в наличии, как они обрабатываются, хранятся и защищаются. Причём эта информация должна быть предоставлена не только в ходе проверок уполномоченными органами, но и по первому требованию частного лица — владельца этих данных. Соблюдение такого комплаенса требует отвлечения значительных бюджетных средств и ресурсов от других задач информационной безопасности организации. И хотя упорядочение обработки персональных данных предполагает в долгосрочной перспективе улучшение информационной безопасности, в краткосрочном плане риски организации заметно возрастают.

Большинство людей так, или иначе испытывают на себе воздействие угроз информационной безопасности. Например, становятся жертвами вредоносных программ (вирусов и червей, троянских программ, программ-вымогателей), фишинга или кражи личности. Фишинг (англ. Phishing) представляет собой мошенническую попытку завладения конфиденциальной информацией (например, учётной записью, паролем или данными кредитной карты). Обычно пользователя Интернета стараются заманить на мошеннический веб-сайт, неотличимый от оригинального сайта какой-либо организации (банка, интернет-магазина, социальной сети и т. п.). Как правило, такие попытки совершаются с помощью массовых рассылок поддельных электронных писем якобы от имени самой организации, содержащих ссылки на мошеннические сайты. Открыв такую ссылку в браузере, ничего не подозревающий пользователь вводит свои учётные данные, которые становятся достоянием мошенников. Термин Identity Theft с англ. — «кража личности» появился в английском языке в 1964 году для обозначения действий, в которых чьи-либо персональные данные (например, имя, учётная запись в банковской системе или номер кредитной карты, часто добытые с помощью фишинга) используются для мошенничества и совершения иных преступлений. Тот, от чьего имени преступники получают незаконные финансовые преимущества, кредиты или совершают иные преступления, зачастую сам становится обвиняемым, что может иметь для него далеко идущие тяжёлые финансовые и юридические последствия. Информационная безопасность оказывает непосредственное влияние на неприкосновенность частной жизни, определение которой в различных культурах может весьма разниться.

Органы государственной власти, вооружённые силы, корпорации, финансовые институты, медицинские учреждения и частные предприниматели постоянно накапливают значительные объёмы конфиденциальной информации о своих сотрудниках, клиентах, продуктах, научных исследованиях и финансовых результатах. Попадание такой информации в руки конкурентов или киберпреступников может повлечь для организации и её клиентов далеко идущие юридические последствия, невосполнимые финансовые и репутационные потери. С точки зрения бизнеса информационная безопасность должна быть сбалансирована относительно затрат; экономическая модель Гордона-Лоба описывает математический аппарат для решения этой задачи. Основными способами противодействия угрозам информационной безопасности или информационным рискам являются:

снижение — внедрение мер безопасности и противодействия для устранения уязвимостей и предотвращения угроз;

передача — перенос затрат, связанных с реализацией угроз на третьих лиц: страховые или аутсорсинговые компании;

принятие — формирование финансовых резервов в случае, если стоимость реализации мер безопасности превышает потенциальный ущерб от реализации угрозы;

отказ — отказ от чрезмерно рисковой деятельности.

2 . Дайте определения ИБ КИС

Информационная безопасность – это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением...

Корпоративная информационная система (КИС) — управленческая идеология, объединяющая бизнес стратегию и информационные технологии. Корпоративная информационная система — это масштабируемая система, предназначенная для комплексной автоматизации всех видов хозяйственной деятельности небольших и средних предприятий, в том числе корпораций, состоящих из группы компаний, требующих единого управления. Корпоративной Информационной Системой может считаться система, автоматизирующая более 80 % подразделений предприятия. Корпоративные информационные системы являются развитием систем для рабочих групп, они ориентированы на крупные компании и могут поддерживать территориально разнесенные узлы или сети. В основном они имеют иерархическую структуру из нескольких уровней. Для таких систем характерна архитектура клиент-сервер со специализацией серверов или же многоуровневая архитектура. При разработке таких систем могут использоваться те же серверы баз данных, что и при разработке групповых информационных систем. Однако в крупных информационных системах наибольшее распространение получили серверы Oracle, DB2 и Microsoft SQL Server.

3 . Приведите классификацию угроз информации

Угрозы информационной безопасности Угрозы информационной (компьютерной) безопасности — это различные действия, которые могут привести к нарушениям состояния защиты информации. Другими словами, это — потенциально возможные события, процессы или действия, которые могут нанести ущерб информационным и компьютерным системам. Угрозы ИБ можно разделить на два типа: естественные и искусственные. К естественным относятся природные явления, которые не зависят от человека, например ураганы, наводнения, пожары и т.д. Искусственные угрозы зависят непосредственно от человека и могут быть преднамеренными и непреднамеренными. Непреднамеренные угрозы возникают из-за неосторожности, невнимательности и незнания. Примером таких угроз может быть установка программ, не входящих в число необходимых для работы и в дальнейшем нарушающих работу системы, что и приводит к потере информации. Преднамеренные угрозы, в отличие от предыдущих, создаются специально. К ним можно отнести атаки злоумышленников как извне, так и изнутри компании. Результат реализации этого вида угроз — потери денежных средств и интеллектуальной собственности организации. Классификация угроз информационной безопасности В зависимости от различных способов классификации все возможные угрозы информационной безопасности можно разделить на следующие основные подгруппы. Нежелательный контент. Несанкционированный доступ. Утечки информации. Потеря данных. Мошенничество. Кибервойны. Кибертерроризм.

4. Какие основные направления и методы реализации угроз Вам известны?

• типов и параметров носителей информации;

• архитектуры, типов и параметров технических средств КС, версии операционной системы, состава прикладного программного обеспечения;

• основных функций, выполняемых КС;

• средств и способов защиты;

• способов представления и кодирования информации.

После решения задач определения параметров системы злоумышленник переходит к этапу получения сведений о режимах доступа, паролях и сведений о пользователях системы. Для этого он пытается получить доступ к использованным расходным материалам и сменным носителям:

• съемные носители информации, содержащие секретную информацию;

• визуальное наблюдение или съемка экранов терминалов, анализ распечаток и отходов работы графопостроителей и т.д.;

• перехват побочных электромагнитных и звуковых излучений и наводок по цепям питания.

Получив доступ к КС или возможность входа в систему, злоумышленник, в зависимости от преследуемых целей, среди которых можно выделить получение секретной информации, искажение секретных данных, нарушение работы системы, предпринимает следующие действия:

• несанкционированный доступ к информации;

• перехват данных по каналам связи;

• изменение архитектуры КС, путем установки дополнительных перехватывающих устройств или замены отдельных узлов на специальные, содержащие возможность проводить несанкционированные действия в КС, например, установка клавиатурных шпионов, перепрограммирование ПЗУ, установка сетевых карт, способных фиксировать и сохранять или искажать проходящие через них пакеты;

• уничтожение машинных носителей информации;

• внесение искажений в программные компоненты КС;

• внедрение дезинформации;

• раскрытие способов представления информации и ключей шифрования;

• изменение доступа к информации.

5. Что понимают под информационной системой?

Информационная система (ИС) — система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию (ISO/IEC 2382:2015).

ИС предназначена для своевременного обеспечения надлежащих людей надлежащей информацией, то есть для удовлетворения конкретных информационных потребностей в рамках определённой предметной области, при этом результатом функционирования информационных систем является информационная продукция — документы, информационные массивы, базы данных и информационные услуги.

Понятие информационной системы

Понятие информационной системы интерпретируют по-разному, в зависимости от контекста.

Достаточно широкое понимание информационной системы подразумевает, что её неотъемлемыми компонентами являются данные, техническое и программное обеспечение, а также персонал и организационное обеспечение. Широко трактует понятие «информационной системы» федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации», подразумевая под информационной системой совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств.

Среди российских ученых в области информатики наиболее широкое определение ИС дает М. Р. Когаловский, по мнению которого в понятие информационной системы помимо данных, программ, аппаратного обеспечения и людских ресурсов следует также включать коммуникационное оборудование, лингвистические средства и информационные ресурсы, которые в совокупности образуют систему, обеспечивающую «поддержку динамической информационной модели некоторой части реального мира для удовлетворения информационных потребностей пользователей».

Более узкое понимание информационной системы ограничивает её состав данными, программами и аппаратным обеспечением. Интеграция этих компонентов позволяет автоматизировать процессы управления информацией и целенаправленной деятельности конечных пользователей, направленной на получение, модификацию и хранение информации. Так, российский стандарт ГОСТ РВ 51987 подразумевает под ИС «автоматизированную систему, результатом функционирования которой является представление выходной информации для последующего использования». ГОСТ Р 53622-2009 использует термин информационно-вычислительная система для обозначения совокупности данных (или баз данных), систем управления базами данных и прикладных программ, функционирующих на вычислительных средствах как единое целое для решения определённых задач.

ИС в деятельности организации рассматривается как программное обеспечение, реализующее её деловую стратегию и бизнес-процессы. Желательной целью является создание и развертывание единой корпоративной информационной системы, удовлетворяющей информационные потребности всех сотрудников, служб и подразделений организации. На практике создание такой системы слишком затруднено или даже невозможно, а иногда и нецелесообразно, вследствие чего на предприятии обычно функционируют несколько различных систем, решающих отдельные группы задач: управление производством, финансово-хозяйственная деятельность, электронный документооборот и т. д. Часть задач бывает «покрыта» одновременно несколькими информационными системами, часть задач — вовсе не автоматизирована. Такая ситуация получила название «лоскутной автоматизации» и является довольно типичной для многих предприятий.

6. Что называют информационными ресурсами?

Информационные ресурсы - это совокупность данных, организованных для получения достоверной информации в самых разных областях знаний и практической деятельности. Законодательство Российской Федерации под информационными ресурсами подразумевает отдельные документы и отдельные массивы документов в информационных системах.

Ресурсы определяют как запасы, источники чего-либо.

В современном мире объем информации увеличивается лавинообразно. Все труднее становится выбрать из нее ту, которая более всего отвечает существующему запросу. Различают пертинентную (подробней >>) и релевантную (подробней >>) информацию. В конце ХХ века возникает понятие "информационные ресурсы".

Сегодня понятие "информационные ресурсы" достаточно многопланово и включает в себя все многообразие документов на традиционных и нетрадиционных носителях. В данном пособии мы расскажем о наиболее полных из них, содержащих информацию по профилю Российской экономической академии им. Г.В. Плеханова.

Информационные ресурсы подразделяются по классам собираемой информации.

К первично собираемой информации, т.е. той, которая отражает специфику ее источника, области или сферы создания, возникновения, относится информация, образующаяся самостоятельно в природных условиях (например, количество колец на спиле дерева, свидетельствует о его возрасте). Информация о количественных и качественных характеристиках разных социальных процессов образуют класс "снимаемой информации". Выделенные по этому признаку информационные ресурсы можно классифицировать как естественные, производственные, социально-экономические. Например, информация о росте населения.

Другой класс информационного ресурса образуют сведения, данные, получаемые искусственно в процессе научно-исследовательской деятельности, а также любой творческой работы. Она базируется на обработке уже имеющейся информации по специальным параметрам и моделям (математическая обработка, логическая, семантическая и т.д.). К этому же классу относятся и объекты, создаваемые как авторские произведения в области литературы, искусства. Важным компонентом этих ресурсов является информация, получаемая в результате интеллектуальной деятельности человека. Выделяется вторичная информация, возникающая на основе переработки уже имеющейся информации, и новая, фиксирующая то, что человечество до сих пор не знало. Сюда относятся открытия, прогнозы в области различных социальных и природных процессов.

К информационным ресурсам относятся: библиотеки, архивы, базы данных, СМИ и т.п.) и информационные сервисы (Информационные сервисы - это группа сайтов, на которых можно воспользоваться разнообразными сервисными услугами: электронной почтой, блогом (подробней >>), а также познакомиться с механизмом его ведения, поиском, различными каталогами, словарями, справочниками, прогнозом погоды, телепрограммой, курсами валют и т.д.

По существующей классификации, информационные ресурсы могут быть государственными и негосударственными и как элемент состава имущества находятся в собственности граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений.

7. Что составляет основу политики безопасности?

Основу политики безопасности составляет способ управления доступом, определяющий порядок доступа субъектов системы к объектам системы. Название этого способа, как правило, определяет название политики безопасности.

В настоящее время лучше всего изучены два вида политики безопасности: избирательная и полномочная (мандатная), основанные соответственно на избирательном и полномочном способах управления доступом.

Избирательное управление доступом – метод управления доступом субъектов системы к объектам, основанный на идентификации и опознавании пользователя, процесса и/или группы, к которой он принадлежит. Мандатное управление доступом – концепция доступа субъектов к информационным ресурсам по грифу секретности разрешенной к пользованию информации, определяемому меткой секретности. Кроме того, существует набор требований, усиливающий действие этих политик и предназначенный для управления информационными потоками в системе.

Избирательная политика безопасности наиболее широко применяется в коммерческом секторе, так как ее реализация на практике отвечает требованиям коммерческих организаций по разграничению доступа и подотчетности, а также имеет приемлемую стоимость и небольшие накладные расходы.

8. Проанализируйте механизмы и свойства защиты информации?

1. Формирование и опознание подписи. Ее механизм основывается на алгоритмах асимметричного шифрования и включает две процедуры: формирование подписи отправителем и ее опознание (верификацию) получателем. Первая процедура обеспечивает шифрование блока данных или его дополнение криптографической контрольной суммой, причем в обоих случаях используется секретный ключ отправителя. Вторая процедура основывается на использовании общедоступного ключа, знание которого достаточно для опознавания отправителя.

2. Контроль и разграничение доступа. Осуществляет проверку полномочий объектов (программ и пользователей) на доступ к ресурсам сети. В основе контроля доступа к данным лежит система разграничения доступа специалистов информационной технологии к защищаемой информации.

3. Система регистрации и учета информации. Отвечает за ведение регистрационного журнала, позволяет проследить за тем, что происходило в прошлом, и соответственно перекрыть каналы утечки информации. В регистрационном журнале фиксируются все осуществленные или неосуществленные попытки доступа к данным или программам. Содержание регистрационного журнала может анализироваться как периодически, так и непрерывно. В регистрационном журнале ведется список всех контролируемых запросов, осуществляемых специалистами, а также учет всех защищаемых носителей информации с помощью их маркировки, с регистрацией их выдачи и приема.

Система регистрации и учета является одним из эффективных методов увеличения безопасности в информационных системах и технологиях.

4. Обеспечение целостности данных. Применяется как к отдельному блоку, так и к потоку данных. Целостность блока является необходимым, но не достаточным условием целостности потока. Целостность блока обеспечивается выполнением взаимосвязанных процедур шифрования и дешифрования отправителем и получателем. Отправитель дополняет передаваемый блок криптографической суммой, а получатель сравнивает ее с криптографическим значением, соответствующим принятому блоку. Несовпадение свидетельствует об искажении информации в блоке. Однако описанный механизм не позволяет вскрыть подмену блока в целом. Поэтому необходим контроль целостности потока данных, который реализуется посредством шифрования с использованием ключей, изменяемых в зависимости от предшествующих блоков.

5. Обеспечение аутентификации. Это механизм установления подлинности, т.е. проверка, является ли объект (субъект) действительно тем, за кого себя выдает. Механизмы аутентификации подразделяются на одностороннюю и взаимную аутентификацию. При использовании односторонней аутентификации один из взаимодействующих объектов проверяет подлинность другого. Во втором случае – проверка является взаимной.

6. Подстановка трафика (подстановка текста). Используются для реализации службы засекречивания потока данных. Они основываются на генерации объектами информационной системы фиктивных блоков, их шифровании и организации передачи по каналам связи. Тем самым нейтрализуется возможность получения информации об информационной технологии и обслуживаемых ее пользователей посредством наблюдения за внешними характеристиками потоков информации, циркулирующих по каналам связи.

7. Управление маршрутизацией. Обеспечивают выбор маршрутов движения информации по коммуникационной сети таким образом, чтобы исключить передачу секретных сведений по скомпрометированным (небезопасным), физически ненадежным каналам.

8. Арбитраж. Обеспечивает подтверждение характеристик данных, передаваемых между объектами информационной системы, третьей стороной (арбитром). Для этого вся информация, отправляемая или получаемая объектами, проходит и через арбитра, что позволяет ему впоследствии подтверждать упомянутые характеристики.

9. Дайте понятие объекта защиты информации?

Объект защиты информации - информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации.

10. Что относят к информационным процессам?

Процессы, связанные с поиском, хранением, передачей, обработкой и использованием информации, называются информационными процессами.

Теперь остановимся на основных информационных процессах.

1. Поиск.

Поиск информации - это извлечение хранимой информации.

Методы поиска информации:

непосредственное наблюдение;

общение со специалистами по интересующему вас вопросу;

чтение соответствующей литературы;

просмотр видео, телепрограмм;

прослушивание радиопередач, аудиокассет;

работа в библиотеках и архивах;

запрос к информационным системам, базам и банкам компьютерных данных;

другие методы.

Понять, что искать, столкнувшись с той или иной жизненной ситуацией, осуществить процесс поиска - вот умения, которые становятся решающими на пороге третьего тысячелетия.

2. Сбор и хранение.

Сбор информации не является самоцелью. Чтобы полученная информация могла использоваться, причем многократно, необходимо ее хранить.

Хранение информации - это способ распространения информации в пространстве и времени.

Способ хранения информации зависит от ее носителя (книга- библиотека, картина- музей, фотография- альбом).

ЭВМ предназначен для компактного хранения информации с возможностью быстрого доступа к ней.

Информационная система - это хранилище информации, снабженное процедурами ввода, поиска и размещения и выдачи информации. Наличие таких процедур- главная особенность информационных систем, отличающих их от простых скоплений информационных материалов. Например, личная библиотека, в которой может ориентироваться только ее владелец, информационной системой не является. В публичных же библиотеках порядок размещения книг всегда строго определенный. Благодаря ему поиск и выдача книг, а также размещение новых поступлений представляет собой стандартные, формализованные процедуры.

3. Передача.

В процессе передачи информации обязательно участвуют источник и приемник информации: первый передает информацию, второй ее получает. Между ними действует канал передачи информации - канал связи.

Канал связи - совокупность технических устройств, обеспечивающих передачу сигнала от источника к получателю.

Кодирующее устройство - устройство, предназначенное для преобразования исходного сообщения источника к виду, удобному для передачи.

Декодирующее устройство - устройство для преобразования кодированного сообщения в исходное.

Деятельность людей всегда связана с передачей информации.

В процессе передачи информация может теряться и искажаться: искажение звука в телефоне, атмосферные помехи в радио, искажение или затемнение изображения в телевидении, ошибки при передачи в телеграфе. Эти помехи, или, как их называют специалисты, шумы, искажают информацию. К счастью, существует наука, разрабатывающая способы защиты информации - криптология.

Каналы передачи сообщений характеризуются пропускной способностью и помехозащищенностью.

Каналы передачи данных делятся на симплексные (с передачей информации только в одну сторону (телевидение)) и дуплексные (по которым возможно передавать информацию в оба направления (телефон, телеграф)). По каналу могут одновременно передаваться несколько сообщений. Каждое из этих сообщений выделяется (отделяется от других) с помощью специальных фильтров. Например, возможна фильтрация по частоте передаваемых сообщений, как это делается в радиоканалах.

Пропускная способность канала определяется максимальным количеством символов, передаваемых ему в отсутствии помех. Эта характеристика зависит от физических свойств канала.

Для повышения помехозащищенности канала используются специальные методы передачи сообщений, уменьшающие влияние шумов. Например, вводят лишние символы. Эти символы не несут действительного содержания, но используются для контроля правильности сообщения при получении.

С точки зрения теории информации все то, что делает литературный язык красочным, гибким, богатым оттенками, многоплановым, многозначным,- избыточность. Например, как избыточно с таких позиций письмо Татьяны к Онегину. Сколько в нем информационных излишеств для краткого и всем понятного сообщения "Я Вас люблю!"

4. Обработка.

Обработка информации - преобразование информации из одного вида в другой, осуществляемое по строгим формальным правилам.

Примеры обработки информации

Примеры Входная информация Выходная информация Правило

Таблица умножения Множители Произведение Правила арифметики

Определение времени полета рейса "Москва-Ялта" Время вылета из Москвы и время прилета в Ялту Время в пути Математическая формула

Отгадывание слова в игре "Поле чудес" Количество букв в слове и тема Отгаданное слово Формально не определено

Получение секретных сведений Шифровка от резидента Дешифрованный текст Свое в каждом конкретном случае

Постановка диагноза болезни Жалобы пациента + результаты анализов Диагноз Знание + опыт врача

Обработка информации по принципу "черного ящика" - процесс, в котором пользователю важна и необходима лишь входная и выходная информация, но правила, по которым происходит преобразование, его не интересуют и не принимаются во внимание.

"Черный ящик" - это система, в которой внешнему наблюдателю доступны лишь информация на входе и на выходе этой системы, а строение и внутренние процессы неизвестны.

5. Использование.

Информация используется при принятии решений.

Достоверность, полнота, объективность полученной информации обеспечат вам возможность принять правильное решение.

Ваша способность ясно и доступно излагать информацию пригодится в общении с окружающими.

Умение общаться, то есть обмениваться информацией, становится одним главных умений человека в современном мире.

Компьютерная грамотность предполагает:

знание назначения и пользовательских характеристик основных устройств компьютера;

Знание основных видов программного обеспечения и типов пользовательских интерфейсов;

умение производить поиск, хранение, обработку текстовой, графической, числовой информации с помощью соответствующего программного обеспечения.

Информационная культура пользователя включает в себя:

понимание закономерностей информационных процессов;

знание основ компьютерной грамотности;

технические навыки взаимодействия с компьютером;

эффективное применение компьютера как инструмента;

привычку своевременно обращаться к компьютеру при решении задач из любой области, основанную на владении компьютерными технологиями;

применение полученной информации в практической деятельности.

6. Защита.

Защитой информации называется предотвращение:

доступа к информации лицам, не имеющим соответствующего разрешения (несанкционированный, нелегальный доступ);

непредумышленного или недозволенного использования, изменения или разрушения информации.

Более подробно о защите информации мы остановимся далее.

Под защитой информации, в более широком смысле, понимают комплекс организационных, правовых и технических мер по предотвращению угроз информационной безопасности и устранению их последствий.

11. Что понимают под информационной системой?

Информационная система (ИС) — система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию (ISO/IEC 2382:2015)

ИС предназначена для своевременного обеспечения надлежащих людей надлежащей информацией[2], то есть для удовлетворения конкретных информационных потребностей в рамках определённой предметной области, при этом результатом функционирования информационных систем является информационная продукция — документы, информационные массивы, базы данных и информационные услуги

Понятие информационной системы.

Понятие информационной системы интерпретируют по-разному, в зависимости от контекста.

Достаточно широкое понимание информационной системы подразумевает, что её неотъемлемыми компонентами являются данные, техническое и программное обеспечение, а также персонал и организационное обеспечение[4]. Широко[5] трактует понятие «информационной системы» федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации», подразумевая под информационной системой совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств

Среди российских ученых в области информатики наиболее широкое определение ИС дает М. Р. Когаловский, по мнению которого в понятие информационной системы помимо данных, программ, аппаратного обеспечения и людских ресурсов следует также включать коммуникационное оборудование, лингвистические средства и информационные ресурсы, которые в совокупности образуют систему, обеспечивающую «поддержку динамической информационной модели некоторой части реального мира для удовлетворения информационных потребностей пользователей

Более узкое понимание информационной системы ограничивает её состав данными, программами и аппаратным обеспечением. Интеграция этих компонентов позволяет автоматизировать процессы управления информацией и целенаправленной деятельности конечных пользователей, направленной на получение, модификацию и хранение информации[9]. Так, российский стандарт ГОСТ РВ 51987 подразумевает под ИС «автоматизированную систему, результатом функционирования которой является представление выходной информации для последующего использования». ГОСТ Р 53622-2009 использует термин информационно-вычислительная система для обозначения совокупности данных (или баз данных), систем управления базами данных и прикладных программ, функционирующих на вычислительных средствах как единое целое для решения определённых задач.

ИС в деятельности организации рассматривается как программное обеспечение, реализующее её деловую стратегию и бизнес-процессы. Желательной целью является создание и развертывание единой корпоративной информационной системы, удовлетворяющей информационные потребности всех сотрудников, служб и подразделений организации. На практике создание такой системы слишком затруднено или даже невозможно, а иногда и нецелесообразно[11], вследствие чего на предприятии обычно функционируют несколько различных систем, решающих отдельные группы задач: управление производством, финансово-хозяйственная деятельность, электронный документооборот и т. д. Часть задач бывает «покрыта» одновременно несколькими информационными системами, часть задач — вовсе не автоматизирована. Такая ситуация получила название «лоскутной автоматизации» и является довольно типичной для многих предприятий.

12. Что называют информационными ресурсами?

Информационные ресурсы — документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, депозитариях, музейных хранилищах и т. п.)

Термин-Информационные ресурсы являются одним из видов общественных/экономических ресурсов — факторов производства.

Со временем значимость информационных ресурсов возрастает; одно из свидетельств этого заключается в том, что они становятся товаром, совокупная стоимостью которого на рынке сопоставима со стоимостью традиционных дел.

Любая классификация информационных ресурсов общества оказывается неполной. Внутри каждого класса можно проводить дополнительно, более детальное разделение. Например, ресурсы Интернета можно разделять по их назначению и по формам представления: сервисная информация, библиографическая информация, материалы телеконференции, видео и т. д.

Важной особенностью информационных ресурсов является их «неуничтожаемость» — они не исчезают после использования и ими можно пользоваться многократно, копируя без ограничений.

В соответствии с Федеральным законом РФ от 20 февраля 1995 г. № 24-ФЗ "Об информации, информатизации и защите информации" (Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" признан утратившим силу) — информационные ресурсы — отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах)

13. Примеры комплексов программно-аппаратных средств и преимущества использования.

Программно-аппаратный комплекс — это набор технических и программных средств, работающих совместно для выполнения одной или нескольких сходных задач.

Аппаратно-программный комплекс — техническое решение концепции алгоритма работы сложной системы, управление которой осуществляется, как правило, исполнением кода из определённого базового набора команд (системы команд)

Состоит, соответственно, из двух основных частей:

Аппаратная часть (англ. hardware) — устройство сбора и обработки информации например компьютер, плата видеозахвата, биометрический детектор, калибратор и т. п.

Программная часть (англ. software) — специализированное программное обеспечение (как правило, написанное компанией-производителем аппаратной части), обрабатывающее и интерпретирующее данные, собранные аппаратной частью. Например: встроенное программное обеспечение, операционная система.

Программно-аппаратный комплекс представляет собой набор технических и программных средств, работающих совместно для выполнения одной или нескольких однородных задач. Позволяют оперативно развертывать определенные системы, связанные с ИТ-инфраструктурой, без привлечения квалифицированного персонала. Это помогает существенно снизить расходы на внедрение определенных элементов инфраструктуры.

Область применения разрабатываемых нами комплексов охватывает широкий спектр деятельности, как социальную сферу, так и объекты предпринимательства:

оптовая и розничная торговля;

информационно-библиотечные ресурсы;

кредитные организации;

образовательные учреждения;

производственная сфера;

логистические предприятия;

предприятия коммуникаций и связи;

организации здравоохранения;

туристическая деятельность и т.д.

Для решения конкретных задач вышеперечисленных отраслей мы предлагаем разработку программно-аппаратных комплексов:

• автоматизированное рабочие место;

• электронная очередь;

• видеонаблюдения и контроля доступа;

• системы распознавания образов;

• медицинской диагностики;

• защиты конфиденциальной информации;

• автоматической книговыдачи;

• имитационное моделирование и постановка эксперимента;

• решение управленческих задач;

• системы видеоанализа;

• системы маскировки передачи защищаемой информации и т.д.

Специалисты отдела системной интеграции помогут вам выбрать решения максимально соответствующие специфике вашей деятельности и подберут оптимальные - по цене, качеству, производительности и функциональности.

Программно-аппаратные комплексы позволяют увеличить показатели эффективности живого и овеществленного труда, сократить объемы оборотных средств, повысить показатели рентабельности.

Программно-аппаратные комплексы это:

простота администрирования и минимальные затраты на обслуживание за счет интуитивно понятного интерфейса процесс администрирования устройства прост и может осуществляться с помощью любого интернет-браузера;

максимально быстрое развертывание за счет использования оптимизированного программного обеспечения;

контроль работоспособности позволяет автоматически восстанавливать работоспособность устройства в случае возникновения каких-либо проблем;

минимизация количества внеплановых остановок,

активное противодействие позволяет максимально оперативно реагировать на вирусные угрозы.

При создании программно-аппаратных комплексов специалисты компании Технологии Репликации руководствуются принципами:

• соблюдение авторского права;

• вариативность при выборе способа объединения комплектующих в единый комплекс ПАК для решение какой-то конкретной задачи. Знать и устранять типичные ошибки при сборке ПАК;

• выявление и устранение ошибок при установке программного обеспечения;

• интеграция существующего программного обеспечения с вновь устанавливаемым;

• проектирование и внедрение ПАК необходимого для решения конкретной задачи;

• доступное обучение пользователя ПАК.

Освоение новых предметных областей и инновационных технологий, исследования в информационной области являются неотъемлемой частью создания программно-аппаратных комплексов компании Технологии Репликации.