РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

Митюшин Дмитрий Алексеевич

Информационные технологии. Администрирование подсистем защиты информации

Тема 1. Место и роль подсистемы защиты информации в современных информационных системах

Вопросы:

1. *Структура автоматизированной информационной системы*
2. *Жизненный цикл подсистем защиты информации*
3. *Правила, регламенты и стратегия администрирования в АИС*

Литература

1. Румянцева Е.Л., Слюсарь В.В. Информационные технологии. Учебное пособие / Е.Л. Румянцева, В.В. Слюсарь; Под ред. Л.Г. Гагариной. – М.: ИД ФОРУМ: НИЦ Инфра-М, 2013. – 256 с.: ил. ЭБС. http://znanium.com/bookread2.php?book=392410&spec=1
2. Гатчин Ю.А., Климова Е.В. Введение в комплексную защиту объектов информатизации: учебное пособие. – СПб: НИУ ИТМО, 2011. – 112 с.
3. Гришина Н. В. Организация комплексной системы защиты информации. – М.: Гелиос АРВ, 2007. – 256 с, ил.

1. Структура автоматизированной информационной системы

1.1. Определение системы и виды информационных систем

Выделим закономерность, характеризующие любую систему:

- ***отграниченность от среды***, ***интегративность*** – система есть абстрактная сущность, обладающая целостностью и определённая в своих границах, при этом в некотором существенном для наблюдателя аспекте «сила» или «ценность» связей элементов внутри системы выше, чем сила или ценность связей элементов системы с элементами внешних систем или среды. Системообразующие, системосохраняющие факторы при этом называют интегративными.
- ***синергичность***, ***эмерджентность***, ***холизм***, ***системный эффект***, ***сверхаддитивный эффект***, ***целостность*** – появление у системы свойств, не присущих элементам системы; принципиальная несводимость свойств системы к сумме свойств составляющих её компонентов. Возможности системы превосходят сумму возможностей составляющих её частей; общая производительность или функциональность системы лучше, чем у простой суммы элементов.
- ***иерархичность*** – каждый элемент системы может рассматриваться как система; сама система также может рассматриваться как элемент некоторой надсистемы (суперсистемы). Более высокий иерархический уровень оказывает воздействие на нижележащий уровень и наоборот: подчинённые члены иерархии приобретают новые свойства, отсутствовавшие у них в изолированном состоянии (влияние целого на элементы), а в результате появления этих свойств формируется новый, другой «облик целого» (влияние

1. Структура автоматизированной информационной системы

1.1. Определение системы и виды информационных систем

В таблице приведены примеры нескольких систем, состоящих из разных элементов и направленных на реализацию разных целей.

Система	Элементы системы	Главная цель системы
Фирма	Люди, оборудование, материалы, здания и др.	Производство товаров или услуг
Компьютер	Электронные и электромеханические элементы, шины связи и др.	Обработка данных
Телекоммуникационная система	Компьютеры, модемы, маршрутизаторы, кабели, сетевое ПО и др.	Передача информации
Информационная система	Компьютеры, компьютерные сети, люди, информационное и программное обеспечение	Производство профессиональной информации

1. Структура автоматизированной информационной системы

1.1. Определение системы и виды информационных систем

Применительно к информационным системам чаще всего имеется в виду набор технических средств и программ. Системой может называться не только аппаратная часть компьютера. Системой может также считаться множество программ для решения конкретных прикладных задач, дополненных процедурами ведения документации и управления расчётами.

ГОСТ 34.321-96 даёт такое определение:

Информационная система (information system): система, которая организует хранение и манипулирование информацией о предметной области.

Информационная система – взаимосвязанная совокупность средств, методов и персонала, используемых для хранения, обработки и выдачи информации в интересах достижения поставленной цели.

Информационная система имеет цель – производство профессиональной информации, связанной с определённой профессиональной деятельностью. Информационные системы обеспечивают сбор, хранение, обработку, поиск, выдачу информации, необходимой в процессе принятия решений задач из любой области. Их задача помочь в анализе проблем и создавать новые продукты.

1. Структура автоматизированной информационной системы

1.1. Определение системы и виды информационных систем

Современное понимание информационной системы предполагает использование в качестве основного технического средства переработки информации персонального компьютера. В крупных организациях наряду с персональным компьютером в состав технической базы информационной системы может входить мэйнфрейм или суперЭВМ.

Кроме того, техническое воплощение информационной системы само по себе ничего не будет значить, если не учтена роль человека, для которого предназначена производимая информация и без которого невозможно её получение и представление.

Обязательной компонентой любой информационной системы, как и любой искусственно созданной системы, является человек. В нашем случае – персонал, взаимодействующий с компьютерами и телекоммуникациями.

Среди множества факторов, определяющих совокупность свойств конкретной информационной системы, можно выделить три основных:

- технический уровень;
- характер обрабатываемой информации;
- целевые функции, т.е. круг задач, для решения которых данная система предназначена.

1. Структура автоматизированной информационной системы

1.1. Определение системы и виды информационных систем

Перечисленные факторы определяют форму представления информации как в системе, так и для пользователя, характер процессов обработки информации и взаимодействия системы с внешней средой, состав алгоритмического и программного обеспечения системы.

По техническому уровню информационные системы разделяют на:

- ручные,
- механизированные,
- автоматизированные и
- автоматические.

Порядок перечисления систем отражает историческую последовательность их создания.

1. Структура автоматизированной информационной системы

1.1. Определение системы и виды информационных систем

В ***ручных информационных системах*** все процессы обработки информации осуществляются вручную. Информационные массивы ручных систем имеют небольшой объём, данные хранятся на носителях различных типов. Для поиска информации в таких системах используются простые селектирующие приспособления. Фактически ручные информационные системы являются не системами, а устройствами, облегчающими поиск нужной информации по определённой совокупности признаков. Эти устройства дешёвые, простые в обращении, для их эксплуатации не требуется высококвалифицированный обслуживающий персонал.

В ***механизированных информационных системах*** для обработки и поиска информации использовались различные средства механизации, среди которых наибольшее распространение получили счётно-перфорационные машины. Носителями информации в механизированных системах являлись перфокарты. В комплект технических средств такой механизированной системы входит набор перфорационных машин, каждая из которых выполняет определённые функции. С помощью перфоратора информация переносится с первичных документов на перфокарты. Перфокарты, имеющие общие признаки, раскладывает по отдельным группам сортировщик.

1. Структура автоматизированной информационной системы

1.1. Определение системы и виды информационных систем

В ***автоматизированных*** и ***автоматических информационных системах*** для хранения, обработки и поиска информации используются компьютеры. Эти системы обладают широкими функциональными возможностями и способны хранить и обрабатывать большие массивы информации. Носители информации здесь – запоминающие устройства компьютеров.

Средства вычислительной техники (СВТ) в автоматических и автоматизированных информационных системах используются не только для хранения и поиска информации, но и для выполнения операций, связанных со сбором, подготовкой и передачей информации в компьютеры, а также с выдачей информации пользователю.

В функционировании ***автоматизированных информационных систем*** (АИС), являющихся наиболее распространёнными, на различных этапах технологического процесса обработки информации принимает участие человек (при сборе информации и подготовке её к вводу в компьютер, в процессе поиска). Человек является партнёром АИС со стороны внешней среды, поэтому именно на него ориентирована выходная информация системы.

1. Структура автоматизированной информационной системы

1.1. Определение системы и виды информационных систем

В ***автоматических информационных системах*** все процессы протекают без участия человека. Обычно автоматические системы используются в составе более крупных систем, например в автоматизированных системах управления технологическими процессами и объектами.

«Партнёрами» автоматических систем являются роботы, станки с программным управлением, технологические процессы, производственные объекты и т.п.

Входная информация в таких системах представляется в форме сигналов или каких-либо физических величин, выходная информация используется для управления и регулирования.

Основная цель автоматизации управления связана с рядом общих идей, обусловленных желанием сформировать своеобразную электронную «нервную систему» организации.

1. Структура автоматизированной информационной системы

1.1. Определение системы и виды информационных систем

Принципы, на которых базируются электронные «нервные системы» любого уровня, являются общими для всех подобных систем:

- стандартизация аппаратных средств, наличие «линейки» вычислительных систем разных возможностей, обеспечивающих требуемую гибкость и производительность за приемлемую стоимость;
- работа с любым видом информации, представление всей информации в цифровой форме;
- создание всепроникающей коммуникационной инфраструктуры; построение и использование сети, объединяющей отдельные части вычислительных систем и обеспечивающей постоянную связь, и том числе в рамках универсальной системы электронной почты;
- стандартизация рабочих инструментов и вычислительных ресурсов конечных пользователей и организаций;
- применение интегрированных приложений, специфических для конкретного вида и уровня деятельности.

1. Структура автоматизированной информационной системы

1.1. Определение системы и виды информационных систем

Общие фундаментальные принципы построения и функционирования ИС – принцип первого лица, системного подхода, надёжности, непрерывного развития, экономичности, совместимости:

- принцип первого лица определяет право принятия окончательного решения и порядок ответственности на различных уровнях управления;
- принцип системного подхода предполагает в процессе проектирования ИС проведение анализа объекта управления в целом и системы управления им, а также выработку общих целей и критериев функционирования объекта в условиях его автоматизации. Данный принцип предусматривает однократный ввод информации в систему и многократное её использование; единство информационной базы; комплексное программное обеспечение;
- принцип надёжности характеризует надёжность работы ИС, которая обеспечивается с помощью различных способов. Например, дублирование структурных элементов системы или их избыточность;
- принцип непрерывного развития системы требует от системы возможности расширяться без проведения серьёзных организационных изменений;
- принцип экономичности заключается в том, что выгоды от новой ИС не должны превышать расходы на неё;
- принцип совместимости предполагает, что проектируемая ИС будет учитывать организационную структуру предприятия, а также интересы, квалификацию людей, осуществляющих работу с ИС.

1. Структура автоматизированной информационной системы

1.1. Определение системы и виды информационных систем

Они должны быть подготовлены к работе в этой системе.

Обмен информацией начинается и заканчивается речью, данными или изображением, воспринимаемыми органами восприятия человека: слухом, зрением и осязанием. А между этими входными и выходными элементами в компьютеризованной информационной системе находится электронный продукт различных уровней – операционные системы, системы управления базами данных, прикладное обеспечение и сама информация.

1. Структура автоматизированной информационной системы

1.2. Структура автоматизированных информационных систем

В АИС появляется возможность отображения на информационную плоскость всего, что происходит с организацией. Все экономические факторы и ресурсы выступают в единой информационной форме, в виде данных, что позволяет рассматривать процесс принятия решений как ***информационную технологию***.

Таким образом, АИС может стать средой информационной поддержки целенаправленной коллективной деятельности всей организации, т.е. ***корпоративной информационной системой***. Такая система включает в себя совокупность различных программно-аппаратных платформ, универсальных и специализированных приложений различных разработчиков, интегрированных в единую информационно-однородную систему, которая наилучшим образом решает задачи каждого конкретного предприятия.

Корпоративная ИС решает одну единственную задачу – эффективное управление всеми ресурсами предприятия (материально-техническими, финансовыми, технологическими и интеллектуальными) для получения максимальной прибыли и удовлетворения материальных и профессиональных потребностей всех сотрудников предприятия.

1. Структура автоматизированной информационной системы

1.2. Структура автоматизированных информационных систем

Корпоративная информационная система – это человеко-машинная система и инструмент поддержки интеллектуальной деятельности человека, которая, в частности, под его воздействием должна:

- накапливать определённый опыт и формализованные знания;
- постоянно совершенствоваться и развиваться;
- быстро адаптироваться к изменяющимся условиям внешней среды и новым потребностям предприятия.

Обычно в ***структуру*** корпоративной АИС можно выделить:

- персонал;
- единую базу данных хранения информации, формируемую различными и не связанными между собой программами и прикладными системами;
- программы, обеспечивающие функционирование информационной системы (операционные системы, служебные программы и т.п.);
- технические устройства;
- множество прикладных систем, созданных разными фирмами и по разным технологиям (финансы, материально-технический учёт, конструкторско-технологическая подготовка производства, документооборот, аналитика и т. п.).

1. Структура автоматизированной информационной системы

1.2. Структура автоматизированных информационных систем

В плане функционирования корпоративная АИС имеет функциональную и обеспечивающую части (рис. 1).

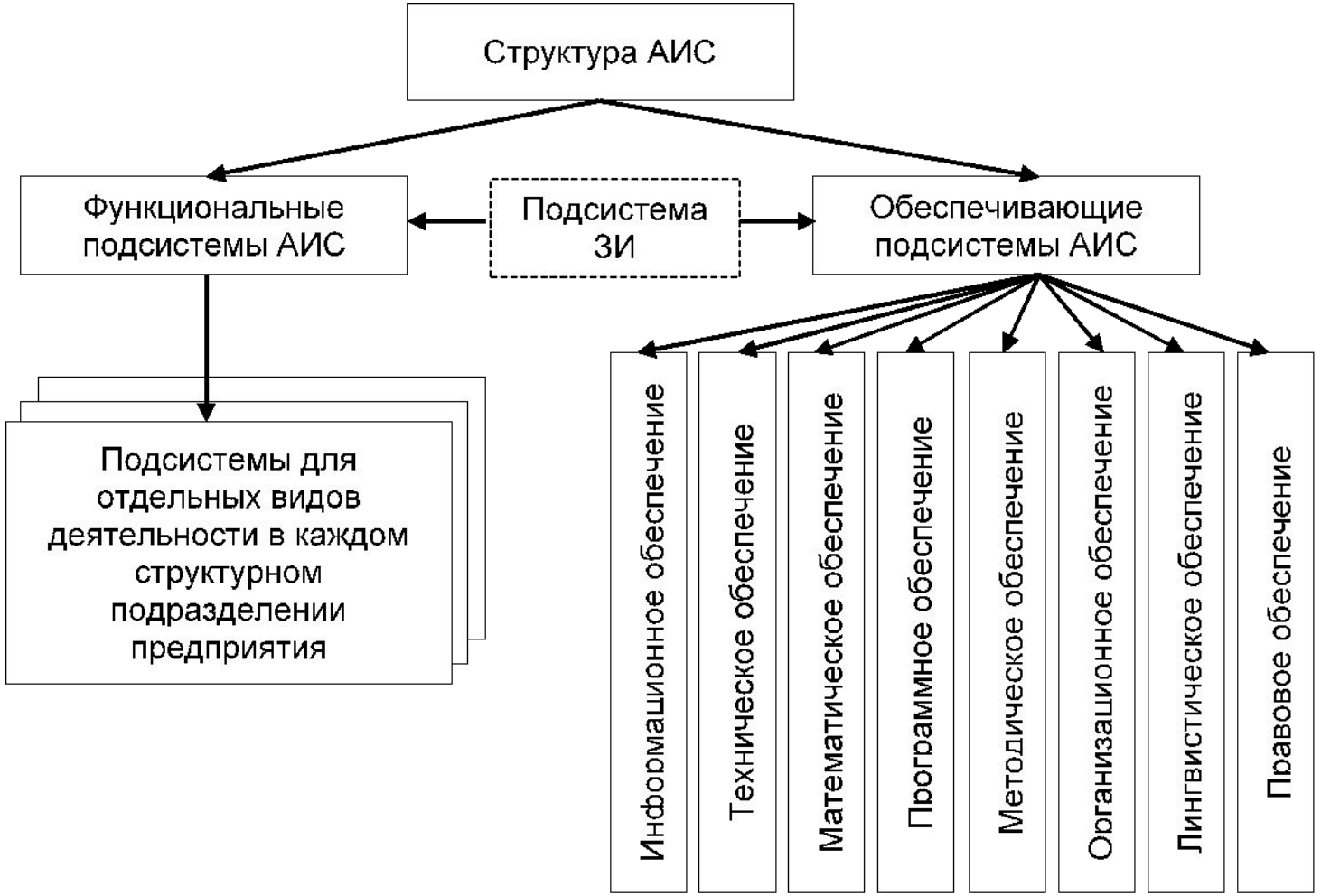

Рис. 1. Структура АИС

1. Структура автоматизированной информационной системы

1.2. Структура автоматизированных информационных систем

Функциональная часть АИС обеспечивает выполнение задач, для которых и предназначена информационная система. Фактически здесь содержится модель системы управления организацией. В рамках этой части происходит трансформация целей управления в функции, функций – в подсистемы АИС.

Подсистема – это часть системы, выделенная по какому-либо признаку, реализующая определённые задачи.

Обычно в информационной системе функциональная часть разбивается на подсистемы по функциональным признакам:

- уровень управления (высший, средний, низший);
- вид управляемого ресурса (материальный, трудовой, финансовый и т.п.);
- сфера применения (банковская, фондового рынка и т. п.);
- функции управления и период управления.

Обеспечивающая часть состоит из информационного, технического, математического, программного, методического, организационного, лингвистического и правового обеспечений.

1. Структура автоматизированной информационной системы

1.2. Структура автоматизированных информационных систем

Информационное обеспечение АИС – совокупность проектных решений по объёмам, размещению, формам организации информации (единой системы классификации и кодирования информации, унифицированных систем документации, схем информационных потоков), циркулирующей в организации, а также методология построения баз данных.

Информационное обеспечение включает в себя показатели, справочные данные, классификаторы и кодификаторы информации, унифицированные системы документации, информацию на носителях и т.д., которые могут быть представлены как в виде входных, так и выходных документов.

В зависимости от организации работы с документами можно выделить внемашинное и внутримашинное информационное обеспечение.

Основная часть внемашинного информационного обеспечения – это система документации, которая воспринимается человеком без технических средств (наряды, акты, накладные и т.п.).

1. Структура автоматизированной информационной системы

1.2. Структура автоматизированных информационных систем

Внутримашинное информационное обеспечение представляет собой информационную базу, которая содержится на носителях и может быть создана как совокупность отдельных файлов, каждый из которых отражает некоторое множество однородных управленческих документов, или как интегрированная база данных. В последнем случае файлы будут зависимыми по структуре, а структуры файлов информационной базы не будут соответствовать структуре используемых документов.

Техническое обеспечение АИС – комплекс технических средств, предназначенных для работы информационной системы, а также соответствующая документация на эти средства и технологические процессы.

В целом рассматриваемые технические средства можно разбить на следующие группы:

- технические средства сбора и регистрации, накопления, обработки, передачи, отображения, вывода, размножения информации;
- средства компьютерной техники – компьютеры любых моделей (персональные и высокопроизводительные), которые могут объединяться в вычислительные сети;
- средства организационной техники.

1. Структура автоматизированной информационной системы

1.2. Структура автоматизированных информационных систем

К техническому обеспечению относят также эксплуатационные материалы.

Предварительный выбор технических средств, организация их эксплуатации, технологический процесс обработки данных, технологическое оснащение оформляются документацией. Документацию можно условно разделить на три группы:

1) общесистемную, включающую в себя государственные и отраслевые стандарты по техническому обеспечению;
2) специализированную, содержащую комплекс методик по всем этапам разработки технического обеспечения;
3) нормативно-справочную, используемую при выполнении расчётов по техническому обеспечению.

Математическое обеспечение АИС – совокупность математических методов, моделей, алгоритмов обработки информации, используемых при решении задач в АИС (функциональных и автоматизации проектирования информационных систем). К средствам математического обеспечения относятся:

- средства моделирования процессов управления;
- типовые задачи управления;
- методы математического программирования, математической статистики, теории массового обслуживания и др.

1. Структура автоматизированной информационной системы

1.2. Структура автоматизированных информационных систем

Программное обеспечение АИС – совокупность программ для реализации целей и задач информационной системы, а также *нормального функционирования* комплекса технических средств.

В состав ПО входят системные и специальные программные продукты, прикладное ПО, а также техническая документация. Системные программные средства предназначены для обеспечения деятельности компьютерных систем как таковых и включают в себя:

- операционные системы;
- командно-файловые процессоры;
- системные утилиты;
- *антивирусные* программы.

Специальное ПО представляет собой совокупность программ, разработанных при создании конкретной АИС. В его состав входят пакеты прикладных программ, реализующие разработанные модели и отражающие функционирование реального объекта, а также программы, ориентированные на пользователей и предназначенные для решения типовых задач обработки информации. Они позволяют расширить функциональные возможности компьютеров, контроля и управления процессом обработки данных.

1. Структура автоматизированной информационной системы

1.2. Структура автоматизированных информационных систем

Прикладное ПО обеспечения деятельности предприятий классифицируются следующим образом:

- системы подготовки текстовых документов;
- системы обработки финансово-экономической информации;
- системы управления базами данных;
- личные информационные системы;
- системы подготовки презентаций;
- системы управления проектами;
- экспертные системы и системы поддержки принятия решений;
- системы интеллектуального проектирования и совершенствования систем управления;
- *прочие* системы.

Техническая документация на разработку ПО должна содержать описание задач, задание на алгоритмизацию, экономико-математическую модель задачи, контрольные примеры.

1. Структура автоматизированной информационной системы

1.2. Структура автоматизированных информационных систем

Методическое и организационное обеспечение АИС – совокупность методов, средств и документов, регламентирующих взаимодействие персонала системы с техническими средствами и между собой в процессе разработки и эксплуатации информационной системы.

В методическое и организационное обеспечение входят различные методические и руководящие материалы по стадиям разработки, внедрения и эксплуатации информационной системы (предпроектного обследования, технического задания, технико-экономического обоснования, разработки проектных решений, выбора автоматизируемых задач, типовых проектных решений пакетов прикладных программ, внедрения и эксплуатации информационной системы).

Организационное обеспечение реализует следующие функции:

- анализ существующей системы управления организацией, где будет использоваться ИС, и выявление задач, подлежащих автоматизации;
- подготовку задач к решению на компьютере, включая ТЗ на проектирование ИС и ТЭО её эффективности;
- разработку управленческих решений по составу и структуре организации, а также методологии решения задач, направленных на повышение эффективности системы управления;

1. Структура автоматизированной информационной системы

1.2. Структура автоматизированных информационных систем

- разработку документации, содержащей различные эргономические требования к рабочим местам, информационным моделям, условиям деятельности персонала, набор способов их реализации для обеспечения высокой эффективности работы персонала;
- обучение и сертификацию персонала – учебно-методическая документация и набор требований к уровню подготовки персонала, формирование системы отбора и подготовки персонала.

Правовое обеспечение АИС – совокупность правовых норм, регламентирующих создание, юридический статус и эксплуатацию ИС. В первую очередь, с помощью правового обеспечения регламентируется порядок получения, преобразования и использования информации для укрепления законности работы предприятия.

В состав правового обеспечения входят законы, указы, постановления государственных органов власти, приказы, инструкции и другие нормативные документы министерств, ведомств, организаций, местных органов власти.

В правовом обеспечении можно выделить общую часть, регулирующую функционирование любой информационной системы, и локальную, относящуюся к конкретной системе.

1. Структура автоматизированной информационной системы

1.2. Структура автоматизированных информационных систем

Правовое обеспечение этапов разработки информационной системы включает в себя нормативные акты, связанные с договорными отношениями разработчика и заказчика и правовым регулированием отклонений от договора.

Правовое обеспечение на этапе функционирования информационной системы определяет:

- статус ИС;
- права, обязанности и ответственность персонала;
- правовые положения отдельных видов процесса управления;
- порядок создания и использования информации и др.

Лингвистическое обеспечение АИС – совокупность языков общения (языковых средств) персонала информационной системы и пользователей с программным, математическим и информационным обеспечением, а также совокупность терминов, используемых в информационной системе.

1. Структура автоматизированной информационной системы

1.2. Структура автоматизированных информационных систем

Лингвистическое обеспечение включает:

- информационные языки для описания структурных единиц информационной базы;
- языки управления и манипулирования данными;
- языковые средства информационно-поисковых систем, систем автоматизации проектирования;
- систему терминов и определений, используемых в процессе разработки и функционирования информационной системы, и т.п.

Как видно, нигде не упоминается подсистема защиты информации. Только местами можно догадываться, что там она может подразумеваться.

С другой стороны, достижения последних лет в области компьютерных и информационных технологий обусловили возможность создания распределённых АИС практически во всех областях человеческой деятельности, как в коммерческом использовании, так и в деятельности силовых структур.

Использование АИС характеризуется огромными потоками информации, в т.ч. конфиденциальной. Разумеется, встаёт вопрос о защите данной информации. В рассмотренной выше структуре АИС элементы подсистемы защиты присутствуют во всех указанных подсистемах, поэтому есть смысл выделить

В то же время создание системы защиты информации не является главной задачей предприятия, как, например, производство продукции и получение прибыли. Поэтому создаваемая СЗИ не должна приводить к ощутимым трудностям в работе предприятия, а создание СЗИ должно быть экономически оправданным. Тем не менее, она должна обеспечивать защиту важных информационных ресурсов предприятия от всех реальных угроз.

2. Жизненный цикл подсистем защиты информации

Подсистема защиты информации, как и АИС, относится к сложным системам. Поэтому при их построении могут использоваться основные типовые этапы построения сложных систем с учётом специфики решаемых задач.

В зависимости от особенностей защищаемой АИС системы, условий её эксплуатации и требований к защите информации процесс создания подсистемы ЗИ может не содержать отдельных этапов, или их содержание может несколько отличаться от общепринятых норм при разработке сложных аппаратно-программных систем.

Разработка конкретной ПЗИ может включать следующие этапы:

1. Проведение предварительного обследования состояния объекта и организации защиты информации. Определение факторов, анализ условий и осуществление выбора и обоснования требований по защите информации на заданном объекте.

На стадии обследования организации:

- изучается состав защищаемой информации и объекты защиты;
- устанавливается наличие секретной (конфиденциальной) информации в разрабатываемой ПЗИ, оценивается уровень конфиденциальности и объёмы;
- определяются режимы обработки информации (диалоговый, телеобработки и

2. Жизненный цикл подсистем защиты информации

- анализируется возможность использования имеющихся на рынке сертифицированных средств защиты информации;
- определяется степень участия персонала, функциональных служб, специалистов и вспомогательных работников объекта автоматизации в обработке информации, характер их взаимодействия между собой и со службой безопасности;
- определяются мероприятия по обеспечению режима секретности на стадии разработки.

2. Определение функций защиты, обеспечивающих требуемый уровень в потенциально возможных условиях функционирования объекта.

3. Выявление потенциально возможных угроз информации и вероятностей их появления. Формирование на их основе модели угроз и определение уровня возможного ущерба (незначительный, малый, средний, большой, очень большой и т.п.) и соответствующего уровня требований к защищённости.

При определении уровня наносимого ущерба необходимо учитывать:

- стоимость возможных потерь при получении информации конкурентом;
- стоимость восстановления информации при её утрате;
- затраты на восстановление нормального процесса функционирования АС и т. д.

2. Жизненный цикл подсистем защиты информации

4. Составление модели потенциально возможных нарушителей. Потенциальными правонарушителями прежде всего могут быть сотрудники организации, имеющие значительные материальные затруднения; склонные к азартным играм, к пьянству, наркотической зависимости; имеющие тяжело больных близких родственников; часто меняющие место работы; психически неуравновешенные.

5. Выявление каналов утечки защищаемой информации и определение возможностей и основных каналов НСД к защищаемой информации.

6. Формулирование стратегии ПЗИ (оборонительная, наступательная, упреждающая).

7. Разработка политики безопасности, организационно-распорядительных документов и мероприятий по обеспечению ИБ. Обоснование перечня задач защиты информации, их классификации и эффективности их реализации с точки зрения предотвращения возможных сбоев АС.

8. Обоснование структуры и технологии функционирования ПЗИ. Определение состава технического, математического, программного, информационного и лингвистического обеспечения, нормативно-методических документов и организационно-технических мероприятий по защите информации.

2. Жизненный цикл подсистем защиты информации

9. Моделирование ПЗИ.

10. Проектирование ПЗИ.

11. Тестирование ПЗИ. Проверяется реакция системы в целом и отдельных её компонентов на возможные отказы:

- отдельного компонента;
- группы компонентов;
- основных модулей;
- «жёсткий» сбой (отказ питания).

12. Внедрение ПЗИ. Определение эффективности защиты информации с помощью оценки степени её защищённости. Сравнение полученных результатов с их требуемыми значениями и анализ стоимостных затрат на обеспечение защиты.

13. Корректировка, уточнение, внесение необходимых изменений.

14. Подготовка и передача технической и эксплуатационной документации. Обучение пользователей правилам работы с ПЗИ.

2. Жизненный цикл подсистем защиты информации

15. Эксплуатация ПЗИ и сопровождение. Постоянный мониторинг состояния защищённости информационных ресурсов и выработка предложений по её совершенствованию. Периодический пересмотр следующих положений политики безопасности:

- эффективность политики, определяемая по характеру, числу и воздействию зарегистрированных инцидентов, касающихся безопасности;
- стоимости средств обеспечения безопасности на показатели эффективности функционирования КС;
- влияние изменений на безопасность технологии.

В настоящее время наибольший эффект от внедрения подсистемы защиты информации может быть достигнут только в том случае, когда все используемые средства, методы и меры объединяются в единый целостный механизм – комплексную систему защиты информации. При этом функционирование системы должно контролироваться, обновляться и дополняться в зависимости от изменения внешних и внутренних условий.

Комплексная система защиты информации (КСЗИ) – это совокупность организационно-правовых и инженерно-технических мероприятий, направленных на обеспечение защиты информации от разглашения, утечки и несанкционированного доступа.

2. Жизненный цикл подсистем защиты информации

Как и любой изготовленный продукт, информационная система имеет свой жизненный цикл, т.е. промежуток времени от начала создания до момента прекращения эксплуатации. АИС является особым продуктом, без которого организация существовать не в состоянии, поэтому можно говорить лишь о прекращении эксплуатации данного поколения информационной системы, отдельных её подсистем и элементов.

Жизненный цикл заканчивается, как правило, не в результате физического износа АИС, а из-за её морального устаревания. ***Моральный износ***, ***моральное старение*** – прекращение соответствия информационной системы предъявляемым к ней требованиям.

При моральном износе возможные модификации информационной системы являются экономически невыгодными или невозможными, что влечёт за собой необходимость разработки новой информационной системы. Устаревание и замена новым – вполне естественный процесс для информационных технологий.

Жизненный цикл – период создания и использования информационной системы, охватывающий её различные состояния, начиная с момента возникновения необходимости в данной информационной системе и заканчивая моментом её полного выхода из эксплуатации.

2. Жизненный цикл подсистем защиты информации

В жизненном цикле выделяют следующие стадии:

1) разработка требований;
2) проектирование;
3) реализация и тестирование;
4) внедрение;
5) сопровождение.

Жизненный цикл носит итеративный характер: реализованные этапы ЖЦ, начиная с самих ранних, циклически повторяются в соответствии с новыми требованиями и изменениями внешних условий.

На каждом этапе ЖЦ формируется набор документов и технических решений, которые являются исходными для последующих решений.

2. Жизненный цикл подсистем защиты информации

Наибольшее распространение получили три ***модели ЖЦ***:

- ***каскадная модель***, в которой переход на следующий этап означает полное завершение работ на предыдущем этапе. Основным недостатком этого подхода является существенное запаздывание с получением результата;
- ***поэтапная модель*** с промежуточным контролем – итерационная модель разработки системы с циклами обратных связей между этапами, допускающие возвраты к предыдущему этапу. В результате каждый из этапов может растянуться на весь период разработки;
- ***спиральная модель***, в которой каждый виток спирали соответствует созданию работоспособного фрагмента или версии системы. Это позволяет уточнить требования, цели и характеристики проекта, определить качество разработки, спланировать работы следующего витка спирали и в результате выбрать оптимальный вариант системы, удовлетворяющий требованиям заказчика, и довести его до реализации. Основная проблема – определение момента перехода на следующий этап.

3. Правила, регламенты и стратегия администрирования в АИС

3.1. Основные положения стратегии администрирования

Администрирование системы – это комплекс мероприятий по созданию, настройке и поддержанию нормальной и стабильной работоспособности АИС, а также техническая поддержка всех пользователей системы.

Для реализации основных задач АИС администрирование обязано организовать, структурировать и систематизировать обслуживание пользователей, и вся стратегия администрирования должна быть первоначально построена на основе правил и регламентов.

Документально оформленные, доведённые до сведения всех сотрудников правила и регламенты необходимы для нормального функционирования любой организации.

Они должны быть соответствующим образом оформлены, утверждены руководством и проверены юристами. Лучше это сделать до того, как возникнет необходимость обращения к подобным документам для решения какой-нибудь острой проблемы.

Желательно, чтобы в каждой организации были следующие документы:

- правила административного обслуживания;
- регламенты прав и обязанностей пользователей;
- правила для администраторов (пользователей с особыми привилегиями);

3. Правила, регламенты и стратегия администрирования в АИС

3.1. Основные положения стратегии администрирования

Для систематизации практического опыта можно использовать различные регламенты, оформленные в виде контрольных списков и инструкций. Эти документы полезны как для новых администраторов, так и для ветеранов.

Преимущества, получаемые при использовании регламентов:

- рутинные задачи всегда выполняются одинаково;
- уменьшается вероятность появления ошибок;
- работа по инструкциям выполняется администратором гораздо быстрее;
- изменения самодокументируются;
- корректность действий администратора можно соизмерять с неким эталоном.

В перечень таких регламентов входят:

- подключения компьютера;
- подключения пользователя;
- настройки и конфигурирования компьютера;
- установки библиотеки TCP-оболочек на компьютер;
- настройки резервного копирования для нового компьютера;
- защита нового компьютера;
- перезапуск сложного программного обеспечения;
- восстановления Web-серверов, которые не отвечают на запросы или не предоставляют данных;

3. Правила, регламенты и стратегия администрирования в АИС

3.1. Основные положения стратегии администрирования

- разгрузки очереди и перезагрузки принтера;
- модернизации операционной системы;
- инсталляции пакета прикладных программ;
- инсталляции программного обеспечения по сети;
- модернизации наиболее важных программ (sendmail, gcc, named и т.д.);
- резервные копирования и восстановления файлов;
- выполнение аварийной остановки системы (всех компьютеров; всех, кроме наиболее важных, компьютеров и т.д.).

Некоторые положения инструкций диктуются особенностями ПО, с которым вы работаете, либо правилами, принятыми в тех или иных сторонних группах, например у поставщиков услуг Интернета.

Соблюдение некоторых положений является обязательным, особенно если вы должны обеспечить секретность данных пользователей. В частности, управление интернет-адресами, именами компьютеров, идентификаторами пользователей и групп, регистрационными именами должно осуществляться единообразно для всех компьютеров организации. Для больших структур (в частности, транснациональных корпораций) такой подход реализовать не просто, но если удастся это сделать, управление значительно упростится.

3. Правила, регламенты и стратегия администрирования в АИС

3.2. Правила и регламенты администрирования

В правилах для администраторов (и других лиц с особым статусом) должны быть сформулированы руководящие принципы использования предоставленных привилегий и соблюдения секретности пользовательских данных. Трудно, конечно, ответить на жалобу пользователя о том, что почта не работает, не видя «отскочивших» сообщений, но копии заголовка в большинстве случаев хватает для определения сути проблемы и способа её устранения.

В системе Unix, например, применяют следующие правила.

Если для доступа в систему с правами *root* применяется программа типа *sudo*, то администраторам следует выбирать надёжные пароли и не делить учётные записи с кем попало. Регулярно проверяйте пароли системных администраторов при помощи программы *crack*. Кроме того, важно, чтобы они не использовали команду *sudo tcsh*, поскольку нарушится способность *sudo* регистрировать события и выполняемые команды.

В ряде организаций обладание паролем *root* является символом занимаемого положения. Иногда этот пароль есть у инженеров, которым он не нужен или не должен выдаваться.

3. Правила, регламенты и стратегия администрирования в АИС

3.2. Правила и регламенты администрирования

Другой проверенный метод – поместить пароль *root* в конверт и спрятать его в известном месте. Администраторы обычно пользуются в своей работе программой *sudo*; если по какой-либо причине им понадобится пароль *root*, то они вскроют конверт. После этого пароль *root* меняется и прячется в новый конверт. Конечно, вскрыть конверт ничего не стоит, но доступ к тому месту, где он хранится, имеют только администраторы.

Большое значение имеют правила и регламенты, которые необходимы в экстренных случаях. Для этого необходимо заблаговременно решить вопрос о том, кто будет руководить работой в случае нарушения защиты. Заранее определяется субординация; имена и телефоны должностных лиц держатся вне системы. Может оказаться так, что лучшим руководителем в подобной ситуации будет администратор сети, а не директор.

Правила работы по администрированию в аварийных ситуациях требуют чёткого планирования действий всего персонала организации. Действия персонала в случае аварии нужно планировать заранее. Наиболее сложные аварии случаются на ноутбуках руководителей.

3. Правила, регламенты и стратегия администрирования в АИС

3.2. Правила и регламенты администрирования

При составлении плана аварийных мероприятий обычно предполагается, что административный персонал будет на месте, и он в состоянии справиться с ситуацией. Однако в реальности люди болеют, переходят на другие должности, уходят в отпуск и увольняются. Поэтому стоит заранее продумать, где можно быстро найти дополнительный персонал. (Если система не очень устойчива, а персонал неопытен, то недостаточное количество администраторов уже само по себе рискованно.)

Функции администрирования включают в себя:

1) Обеспечение работоспособности: поиск и устранение любых проблем, мешающих стабильной работоспособности АИС.
2) Управление конфигурацией: настройка параметров ОС и техническая модернизация компонентов системы.
3) Аналитика функционирования системы: непрерывный контроль за использованием сетевых ресурсов.
4) Управление производительностью: сбор статистики о функционировании сетей и АИС за определённый временной интервал с целью рационализации использования сетевых ресурсов, а также снижения сопутствующих затрат.
5) Обеспечение безопасности: организация доступа к АИС и обеспечение надёжного хранения всех данных.

3. Правила, регламенты и стратегия администрирования в АИС

3.2. Правила и регламенты администрирования

Администрирование АИС включает в себя следующие задачи:

- поддержка нормального функционирования электронных баз данных;
- обеспечение стабильной работы АИС;
- предотвращение проникновения в АИС злоумышленников;
- организация прав доступа пользователей к использованию ресурсов системы;
- создание резервных копий информации; организация и ведение учёта по работе АИС;
- оптимизация рабочих процессов с целью повышения уровня производительности;
- обучение пользователей работе в системе;
- осуществление контроля за использованием ПО и препятствие его незаконной модификации;
- контроль модернизации АИС или её компонентов.